Binding corporate rules

Moerel, E.M.L.

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

BINDING CORPORATE RULES

FIXING THE REGULATORY PATCHWORK OF DATA PROTECTION

Lokke Moerel

ISBN/EAN 978-90-817726-0-0

A sensible approach to paper consumption, procurement and recycling is a vital part of our care for the environment. That is why this edition is printed on Forest Stewardship Council (FSC) certified paper with inks on vegetable base and without any damaging solvent ingredients.

Binding Corporate Rules
Fixing the Regulatory Patchwork of Data Protection

Proefschrift ter verkrijging van de graad van doctor aan de universiteit van Tilburg, op gezag van de rector magnificus, prof. Dr. Ph. Eijlander, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in de aula van de Universiteit

op maandag 19 september 2011 om 16.15 uur

door

Elise Marie Leonore Moerel
geboren op 23 september 1965 te Zwolle

Promotor:

Prof. mr. J.E.J. Prins

Promotie commissie:

Prof. Ch. Millard
Prof. mr. M.V. Polak
Prof. C.D. Scott
Prof. dr. L.A.J. Senden

Acknowledgements

In performing my research I have had help in many forms. I obviously benefited from all discussions on Binding Corporate Rules with the Dutch Data Protection Authority and the members of the BCR working group, the advice and input we received from their foreign group companies as well as US and other external foreign counsel. My thanks further go to my firm De Brauw Blackstone Westbroek for again granting me the space to pursue my academic interests and facilitated practical support, provided by Stephen Machon, who edited my English and Mieke Merkelijn, who provided research assistance and edited many footnotes. I am further indebted to The Hague Institute for International Law for launching the HiiL Research Program 'Private Actors and Self-regulation', into the legitimacy, effectiveness, enforcement and quality of different forms of transnational private regulation. My participation in the HiiL program brought me in contact with the European experts on transnational private regulation and their invaluable work products as part of this program, from which I greatly benefited. My thanks finally go to my mentor and PhD supervisor Corien Prins, for being such a generous person, from which all other things follow. I would also like to thank the members of my Review Committee, Christopher Millard, Martijn Polak, Linda Senden and Colin Scott, for reading the manuscript so carefully and for sharing their constructive comments. Finally, I would like to express my love for my husband Jaap and our children Julius, August and Fien, who make everything in life worthwhile pursuing.

Table of contents

ABBREVIATIONS

ADR	Alternative Dispute Resolution
A-G	Advocate General
APEC	Asia-Pacific Economic Cooperation
APPI	Act on the Protection of Personal Information
BEREC	Body of European Regulators for Electronic Communication
BCR	Binding Corporate Rules
BGC	Binding Global Codes
BRIC	Brazil, Russia, India and China
CIPL	Centre for Information Policy Leadership
CNIL	La Commission nationale de l'informatique et des libertés
COPPA	Children's Online Privacy Protection Act
CRM	Customer Relationship Management
CSR	Corporate Social Responsibility
CTLR	Computer Technology Law Report
DCFR	Draft Common Frames of Reference
DG	Directorate-General
DPA	Data Protection Authority
DPD	Data Protection Directive
EC	European Community
EC	European Commission
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECJ	European Court of Justice
ECR	European Court Report
ECSC	European Community of Coal and Steel
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
ESAs	European Supervisory Authorities
etc.	etcetera
EU	European Union
EWC	European Works Council
FAQ	Frequently Asked Questions
FEDMA	Federation of European and Interactive Marketing
FSA	Financial Services Authority
FTC Act	Federal Trade Commission Act
FTSE	Financial Times Stock Exchange
GAAP	Generally Accepted Accounting Principles
GLBA	Gramm-Leach-Bliley Act
HiiL	The Hague Institute for the Internationalisation of Law
HIPPAA	Health Insurance Portability and Accountability Act

HITECH	Health Information Technology for Economic and Clinical Health Act
HR	Human Resources
ICC	International Chamber of Commerce
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
i.e.	id est
IFRS	International Financial Reporting Standards
ILO	International Labour Organisation
IOSCO	International Organisation of Securities Commission
ISAs	Independent Supervisory Authorities
IT	Information Technologies
ITU	International Telecommunication Union
LSE	London School of Economics
MNC(s)	Multinational Corporation(s)
MNE(s)	Multinational Enterprise(s)
MRP	Mutual Recognition Procedure
n	(foot)note
NYSE	New York Stock Exchange
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Controls
OJ	Official Journal of the European Union
OPTA	Onafhankelijke Post en Telecommunicatie Authoriteit (Dutch supervisory authority on telecom operators)
P&I	Privacy & Informatie
para(s).	paragraph(s)
PIAs	Privacy Impact Assessments
PIL	private international law
PIPEDA	Canadian Personal Information Protection and Electronic Document Act
PNR	passenger name records
Pub.L.	Public Law
RSCAS	Robert Schuman Centre for Advanced Studies
SAS 70	Statement on Auditing Standards No 70
SBN	Security Breach Notification
SCC	Specialist Computer Centres
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TNC(s)	Transnational Corporation(s)
TPR	Transnational Private Regulation
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations

US	United States
USC	United States Code
v.	versus
Vol.	Volume
WP 29	Art. 29 Data Protection Working Party
WPNR	Weekblad voor Privaatrecht, Notariaat en Registratie
WPPJ	Working Party on Police and Justice
WSIS	World Summit on the Information Society

1 Introduction

1.1 Background

In 1999, a major US bank implemented an IT system in the US, in which it centralised its processing of employee and customer data (including data of consumers) of all its establishments around the world. The group companies obtained access on a remote basis to the data in the central IT system. This access was not limited to a group company's own employee and customer data, but also to certain data from other group companies for purposes of management information. As the US bank had establishments in most EU Member States, the transfer of the employee and customer data of these EU establishments to the US and other non-EU countries triggered the EU data protection laws of these Member States. The law firm in London I worked for at the time was tasked with ensuring that these data transfers were in compliance with the EU data transfer rules. At that time this required coordination of (i) entering into the EC Standard Contractual Clauses between each of the EU data exporters (i.e. the EU group companies) and each of the non-EU data importers (i.e. the US group company that centrally processed the data as well as all other group companies established in non-EU countries that were not considered by the European Commission as providing an adequate level of data protection), and (ii) meeting all formal permit and notification requirements in these Member States. After four years we had to conclude that despite our efforts, at major cost to the client, we had not succeeded in our mission to meet all formalities in the Member States. In certain Member States, the data protection authorities, in spite of many reminders, never issued the required permits, and some never replied at all. Even worse, after four years, we had to establish that the central data processing operation had substantially changed over time, additional data categories had been added, additional central applications had been implemented (such as online performance evaluation), security measures had changed, and more. As a result, the myriad of EC Standard Contractual Clauses entered into between all group companies had become outdated, and a repeat exercise was indicated. I remember telling the client at the time, as well as my own thoughts that if I were the client, I would not repeat the exercise. Despite major efforts and costs, the compliance effort had not resulted in the desired formal compliance. But more importantly, the exercise had not brought any material data protection in practice to the employees and customers. The exercise had been performed by a network of external counsel, completely without the involvement of the company itself. If anything, it just constituted paper compliance, shuffling contracts and permits, put in a drawer never to be looked at again. Though the contracts contained broad third-party beneficiary rights and remedies of employees

and customers, the chances that these third parties would be aware of these rights and remedies were minimal (there being no requirement to publish such contracts), and if aware, the chances that employees or customers would act on these rights against the company in a foreign jurisdiction were even less.

In the same years, we regularly received instructions of multinationals, especially from outside the EU, to review their global privacy policies for compliance with EU data protection laws. These policies contained processing instructions to employees on how to process personal data of employees and customers in the performance of their tasks, and also provided for a complaints procedure if things went amiss. These reviews led to many changes in these policies, especially regarding the purposes allowed for data processing, requirements for consent and data retention, etc. These reviews did lead to actual changes in the data processing practices of the relevant multinational, and on a global basis. Further, enquiries taught us that introduction of the internal complaints procedures led to an increase in complaints, which I took as a positive sign rather than negative, it being likely that prior to introduction of these codes, complaints were not being pursued at all rather than their not being there. My conclusion at the time was that introduction of these global privacy policies brought substantial additional material data protection to employees and customers in practice, while the administrative burden on the companies to comply with formal requirements was minimal. Money spent on external counsel was a fraction, as this concerned marking up companies' data protection policies rather than coordinating the entering into a network of formal contracts and notification and permit procedures.

Combining the two experiences led to the thought that implementation of a global privacy policy would actually prove a better tool to regulate the inter-company data transfers of multinationals than ever to be achieved by the entering into a contractual network of EC Standard Contractual Clauses. I floated the idea at some international conferences, and finally in a more public manner in the Dutch Financial Times of 3 April 2003:

> "**Boundless Privacy**
>
> The Dutch Data Protection Act requires that for any exchange of personal data between group companies outside the EU, contracts need to be in place between all the group companies concerned. With a company that is even slightly multinational, this can quickly lead to hundreds of contracts. Madness.

A few examples. A company implements a human resources system which contains the data of employees worldwide and which is accessible to the management of all group companies. A car manufacturer with offices over the entire world exchanges customer data with its subsidiaries in order to coordinate which clients will receive Wimbledon tickets.

They should be able to do that, or so you think. All regular acts performed in the normal course of business should be acceptable and permissible. Who thinks that is thinking outside the Personal Data Protection Act. Transferring personal data, such as employee data and data of customers of the car manufacturer, is prohibited to those countries outside the European Economic Area (EEA) that do not offer an adequate level of protection of personal data. Transferring personal data to an own group company in these countries also falls under this prohibition.

Should you forget to notify this transfer to the Dutch Data Protection Authority, then you yourself – without the approval of the customer – hang a criminal law sanction above your head. Intentional violation – you are now warned! – can lead to your doing time for six months.

Thankfully there are a few exceptions to the prohibition on transfers. But not to the duty to notify the Authority. Data transfers to group companies via a central HR system is in certain instances permissible, the most important of which are if (1) the employees concerned have provided their informed consent for the transfer, or (2) the Minister of Justice has granted a permit. Consent may be refused, and via this route it is practically not viable to transfer the complete employee processing to the group company operating the central database.

If the centralisation of the database is for management information purposes, this is only worthwhile when indeed all employee data are included. The most practical solution is to request a permit. The permit can be granted when “adequate safeguards” to protect personal data are offered. What are adequate safeguards?

The European Commission has drafted model contracts. When the exporter of the data has concluded such model contract with the importer of the data outside the EEA, the company will receive a permit on this basis. That sounds reasonable. But how does this work out in the example of the worldwide accessible HR database? The Dutch group company then exchanges data with all its establishments outside the EEA, the French company with all establishments outside the EEA, and so on. This leads to hundreds of inter-company contracts.

> It is a good thing that personal data are not, just like that, transferred to countries where there is no control over the further processing of the data. But influencing such further processing is certainly possible within a group of companies. Instead of concluding hundreds of contracts between group companies, an internal code of conduct, which all group companies adhere to, imposing strict rules for the processing of personal data, would lead to the same result. This code of conduct could provide, among other things, that the individual employees and customers involved will obtain the legal rights and remedies against the foreign group companies that they would have under their own national law.
>
> Many companies have already implemented this type of worldwide code of conduct. Not because this was legally required, but because in a global company, all concerned have an interest in streamlining the internal procedures for data exchange. Pushing back frontiers. And now to await a model code of conduct from the European Commission."

The day after this publication, the Dutch Data Protection Commissioner (at the time Peter Hustinx), invited my (by that time Dutch) law firm and five of our multinational clients[1] to a meeting to discuss the possibility of a corporate privacy code as an alternative to the EC Standard Contractual Clauses. A working group was established which met regularly for the next year. In June of that year the advisory committee to the European Commission on data protection in which the (**Working Party 29**)[2] issued the first (of a series of 6) opinions on corporate privacy codes as an alternative tool for data transfers, which corporate codes it labelled "Binding

---

1 The initial working group consisted of Philips, Shell, AkzoNobel, Sara Lee and Heineken, at a later stage other multinationals joined such as ING, Schlumberger, DSM and AEGON.

2 The Working Party 29 was established as an advisory body to the European Commission under Article 29 of the Data Protection Directive. The Working Party 29 has advisory status only and acts independently, see Article 29(2) Data Protection Directive. Members are representatives of each of the DPAs, the European Data Protection Supervisor and the European Commission. The tasks of the Working Party 29 are clearly formulated and are publicly available. It issues opinions to "contribute to the uniform application of the Data Protection Directive and advises on proposals for EU legislation having an impact of data protection. See the Document "Tasks of the Working Party 29", as published at <www.ec.europa.eu>. Though the opinions of the Working Party 29 are non-binding, they are often followed in practice by the DPAs and, as such, often set the rules *de facto* for application of the Data Protection Directive. The DPAs are, however, not obliged to do so and on specific topics (in particular on BCR) some DPAs follow their own course. See in more detail Chapter 10.2, in particular n 38. See on the Working Party 29, its tasks and procedural rules in more detail para. 14.7.2 - 14.7.4.

Corporate Rules" (**BCR**). Though the first opinion discussed the possibility of BCR in very general terms only, the fact that also the Working Party 29 thought the concept possible was helpful in moving the discussions forward. In June 2004, the meetings and discussions resulted in a template form of BCR for employee data, which could be subsequently adapted by multinationals to their specific requirements. The discussions were based on the understanding between the Dutch data protection authority (**Dutch DPA**) and the multinationals that while the working group was in the process of discussing how to translate the data protection requirements under the Data Protection Directive into a practical data protection compliance program to be embodied in BCR, the Dutch DPA would not pursue these multinationals based on non-compliance in respect of their inter-company data transfers. This enabled the multinationals to spend their time and efforts on developing the compliance tools required for a data protection compliance program, such as development of an audit program, training modules for employees and the privacy officers, and privacy impact assessment tools. The experiences of the multinationals when developing these compliance tools, the feedback they received on the draft template BCR from their group companies around the world and review of the draft BCR by external US and other non-EU counsel, led in their turn to changes in the template BCR. Experiences were also shared with DPAs of other Member States receptive to the concept of BCR, most notably in the so-called Berlin meeting[3], where the DPAs of a limited number of countries and a representative of the European Commission, together with three multinationals (and their outside counsel) shared experiences in a closed meeting. The results of these discussions were fed back to the Working Party 29 and led, in turn, to the the Working Party 29's five subsequent opinions on BCR. The crystallisation of the BCR regime further led to the introduction of the mutual recognition procedure, whereby a number of DPAs agreed to mutually recognise each other's BCR authorisations.

As such, the joint development of the BCR template by the Dutch DPA and the working group of multinationals showed some similarities with what my research later demonstrated to be "learning-based meta-regulation", where legislators that aim to regulate self-regulation do so in cooperation with the companies that wish (or have to) introduce the self-regulation, based on a number of learning cycles.

---

3 The meeting took place on 27 and 28 May 2004. Participants were representatives of the DPAs of Austria, Germany, Hungary, Poland, the UK and the Netherlands, the European Commission and further GE, Philips and Daimler Chrysler (the multinationals at that time being most advanced in their BCR project).

My research made me realise that the development of the BCR regime constitutes a remarkable example of the emergence of a form of transnational meta-regulation (i.e. "regulation of self-regulation"), whereby transnational effect is achieved not so much by transnational public regulation and transnational approvals, but by mutual recognition among national regulators of their respective publicly recognised private codes.

Another topic which attracted my attention in that period was the scope of the applicability regime of the Data Protection Directive. When advising on cross-border data processing operations, the first question to be answered is whether, and if so which of, the data protection laws of the Member States are applicable. Two trends became visible in the opinions of the Working Party 29 on the applicability regime, which from a practical perspective were each understandable and even desirable, but which were incompatible with each other and both contrary to the (legislative history of the) Data Protection Directive.

The applicability regime of the Data Protection Directive is based on the principle of cumulation of applicable laws. In the highly visible SWIFT case, SWIFT was headquartered in Belgium and had a number of establishments in the EU. Based on the cumulation principle, the central data processing operations of SWIFT in principle attract the laws of all Member States where SWIFT has an establishment. As this apparently (also in the eyes of the Working Party 29) was not desirable, the Working Party 29 applied only the law of SWIFT's headquarters (i.e. Belgian law) to all data processing operations of SWIFT in the EU.

On the other hand, with the increased access of EU citizens to the Internet, there was an increasing number of foreign-based websites that processed data of EU citizens by means of cookies. As these foreign websites often have no establishments in the EU and do not otherwise use equipment in the EU, the protection of the Data Protection Directive does not, in principle, extend to the processing of EU data via these websites. The Working Party 29, however, qualified the computers of the users on which the cookies were placed as the "use of equipment" in the EU and thus applied EU data protection law.

These opinions led in practice to companies filing notifications and requesting permits for data transfers which were returned by DPAs since in their opinion the laws of their respective Member State did not apply, or conversely to a lack of compliance with EU data protection requirements as companies operating foreign websites never even thought of the possibility that the Data Protection Directive could be applicable. This widespread

confusion was the trigger for my research into the applicability regime of the Data Protection Directive, which led to a number of publications and papers with recommendations for changes to the applicability regime, which became part of the discussions of the Working Party 29 on the topic. The papers were subsequently published and constitute Chapters 2 and 3 of this dissertation. In 2010, the Working Party 29 subsequently acknowledged for the first time that the scope of applicability of the Directive was indeed confusing, and announced it would issue a further opinion on the topic. Shortly thereafter, the European Commission issued its Communication on the revision of the Data Protection Directive and announced it would indeed revise the applicability regime thereof. In December 2010, the Working Party 29 issued its further opinion on the applicability regime, which deviates in many instances from its earlier opinions and recommends amending the applicability regime very much along the lines as suggested in my publications.

Though much has been achieved on the topics of BCR and the applicability regime of the Directive since 2003, this is not the end of it, though. If anything it became clear in my research into the applicability regime, that the EU (like all legislators in the area of data protection) try to use the scope of their laws to keep a grip on data when transferred across borders. By applying their law also when data are transferred abroad, the data remains protected. It also became clear to me that this is an attempt which is doomed to fail from the start. Territoriality is, and will remain, a key factor for jurisdiction and applicable law regimes. The concepts of applicable law, jurisdiction and enforcement are embedded in a long tradition of Private International Law, where laws that overextend their jurisdictional reach, are considered to be an unacceptable form of 'hyper-regulation' if they apply so indiscriminately that there is no hope of enforcement. Enforcement powers of states and the jurisdiction of their courts are subject to similar limitations. Applicability and enforcement regimes are therefore inherently delineated and cannot be instrumental in filling the gaps in the protection of personal data and subsequent enforcement. This automatically also applies to the data transfer regimes in these laws, as these are only triggered if the relevant data protection law is applicable in the first place.

This would not pose a problem if all countries in the world were to have adequate data protection laws and enforcement. Cross-border cooperation would then be a solution to achieving protection of EU originated data. The current data protection landscape is, however, still a far cry from a proper global network of data protection laws and a global data protection standard is generally not considered achievable in the coming ten years. This is not meant to say that we then just have to accept that control is inevitably lost

over data after they have been transferred (or made part of the cloud). To the contrary, it is meant to say that we have to be more creative in trying to achieve the desired cross-border protection.

When discussing and negotiating the template BCR in the BCR working group with the Dutch DPA, it became clear to me that a possible alternative for the cross-border enforcement issues inherent to the patchwork of national legislation is a choice of law and forum in BCR. Such choice of law and forum may drastically improve the data protection and the access to remedies for the individuals covered by the BCR. If a breach occurs, rather than pursuing rights through traditional judicial means, the individual affected will be able to file a complaint with the group company with which s/he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The individual will, therefore, not have to prove which of the group companies was at fault, which is one of the obstacles in practice to bringing and succeeding in a claim. There is also no issue as to which law applies and whether the relevant law provides for data protection since the breach is governed by the BCR. Also, if the country of the individual has no privacy protection at all, the BCR apply. The complaint may be filed by the individual in her/his own language. The group company that received the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and will ensure provision of the required translations. If the complaints procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the Lead DPA or the courts of the Lead DPA. This procedure will lead to enforceable rights even in jurisdictions where no (adequate) data protection laws are in place or where insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimises cost.

During the process of the BCR working group developing a template form of BCR jointly with the Dutch DPA, many questions came up which were jointly solved and led to changes in the template BCR, including how to ensure that unilateral undertakings in BCR can be enforced by the beneficiaries of BCR. However, other questions also came up which were not easily solved and obviously required further research. One of them is whether indeed a choice of law and forum in BCR is possible or whether this contravenes the mandatory applicability and jurisdiction regime of the Data Protection Directive and/or the employee and consumer protection regimes under Private International Law. Further, since multinationals are not necessarily limited to the EU, recognition of BCR in the EU is not sufficient. For BCR to operate on a global basis, recognition of BCR is required also in non-EU

countries for outbound data transfers from their respective countries. This requires further research whether, and if so, under which conditions, a private law instrument like BCR may be acceptable also by such non-EU countries. This is in the belief that in the present age of 'big data', cross-border solutions will not be achieved by national legislation while it is in the interest of governments, multinationals and individuals alike to protect personal data ubiquitously.

1.2 Research objectives and hypotheses

The digital era is characterised by an unprecedented continuous worldwide flow of data both within multinational companies as well as with their external service providers. While large corporations operate internationally, state governments legislate nationally. Besides leaving gaps in the patchwork of national data protection regulations, this situation also leads to overlaps in applicable national rules that often deviate or outright conflict. These conflicts make it impossible for multinational corporations to comply fully and consistently as to their many forms of cross-border data processing. Further, the traditional territory-based enforcement tools are not adequate for states to force compliance. This legal landscape provides a challenging background to test whether transnational private regulation[4] of data protection can provide solutions where legislation fails to.

1.2.1 Background

In the digital age, data protection is of increasing concern for governments, individuals and companies alike. While many multinational companies fully act on a seamless worldwide basis, states remain bound to their respective territories. The maturing of the internet especially led to a vast increase in cross-border flows of personal data both within and between groups of companies. Though all countries face essentially the same dilemma of how to regulate these vast flows of personal information, their governments have chosen substantially different solutions to do so. Within the European Union (**EU**) the protection of individuals prevailed and the rights of individuals in respect of the processing of their personal data became a fundamental right and freedom. The desire to avoid gaps in the protection of personal data and to prevent circumvention of the Data Protection Directive led EU legislators to provide for a very broad scope of applicability of the Data Protection Directive ("long arm reach"). The wish to regulate the outbound transnational data streams from Europe resulted in another "long arm"

4 The term 'private regulation' is used here in the broad sense, covering both pure self-regulation and regulated self-regulation. Pure self-regulation refers to regulation processes where the state has no involvement. To describe self-regulation when it is combined with laws enacted by the state, various terms are used, such as regulated self-regulation, co-regulation, enforced self-regulation, and audited self-regulation. For a discussion on these various types, see Wolfgang Schulz and Thorsten Held, *Regulated self-regulation as a form of modern government. An analysis of case studies from media and telecommunications law* (University of Luton Press 2004), at 7.

provision in the Data Protection Directive, where it prohibited data transfers to countries outside the EU without an adequate level of protection (**EU data transfer rules**). This extraterritorial provision prompted many countries outside the EU to follow suit in adopting comprehensive data protection legislation to facilitate ongoing access by multinational companies to the EU market. These states also struggled to regulate their outbound transnational data streams which resulted in many states adopting equally "long arm reach" data protection laws and multiple instances of "overregulation" (i.e. where rules are made so generally applicable that they apply prima facie to processing of personal data of their nationals wherever processed around the world). In addition, many of these countries have imposed restrictions on the outbound transfer of personal data from their respective countries. Such outbound data transfer requirements are considered necessary by most countries as there are still many countries with no data protection laws at al,l as well as countries (most notably the US) with a limited regime, where public regulation is targeted at certain sensitive industries and data categories only. As a consequence the worldwide data protection regulatory landscape therefore at present consists of at best a patchwork of very diverse national data protection laws, which laws often deviate or even outright conflict.

A specific challenge for data protection regulators across the world is posed by the fact that enforcement of data protection legislation is based on a jurisdictional approach. In the international environment this leads to many long arm reach data protection laws having no hope of enforcement in practice if the relevant company is not established in the relevant jurisdiction also. Further, the concepts of applicable law and jurisdiction are embedded in a long tradition of international private law, where laws that over-extend their jurisdictional reach are considered an unacceptable form of 'hyper-regulation' if they apply so indiscriminately that there is no hope of enforcement. Applicability regimes are therefore inherently delineated and cannot be instrumental in solving the present gaps in the protection of personal data and the enforcement thereof.

At present the data protection regulators aim to solve the cross-border enforcement issues by a "network approach", where data protection regulators of different jurisdictions cooperate in the event of cross-border violations. Until the time all jurisdictions have adequate data protection laws and supervision thereof, this network approach cannot adequately solve the enforcement issues presently faced by data protection regulators. Though there is a persistent call for such a legally binding global standard for data protection and there are some concrete initiatives in this respect, it is not expected, however, that a global standard will indeed be realised

within the coming 10 years. The present regulatory landscape is still too diverse for such a standard to be acceptable for adoption on a global level. In any event the adoption of a global standard should not be taken as the holy grail for all international jurisdiction and enforcement issues as presently seen in the data protection field. Even if global standards exist, differences in enforcement between countries will remain as in practice regulatory enforcement at the national level proves patchy, whether this is due to lack of resources or the prioritisation by national governments of national commercial or other interests above regulatory enforcement. Solutions may therefore only be forthcoming if some form of central enforcement could be implemented by, for instance, the data protection authority and courts of the jurisdiction where the company has its headquarters.

The regulatory environment described above and deficiencies in protection and enforcement make a challenging background to evaluate whether the fundamentals of the present applicability and jurisdiction regime of the Data Protection Directive are still appropriate in light of the present seamless technical landscape and the worldwide data protection regulatory landscape as it emerges today. This research question will be addressed in Part I.

The existing overlap and conflicts in applicable data protection laws makes a 100% worldwide compliance for multinational companies a practical impossibility. Compliance would require multinational companies not only to track and comply with the material data protection rules of each jurisdiction but also to track and comply with all requirements relating to data transfers between specific countries. Further, multinational companies largely ignore the EU data transfer rules as these lead to impossible administrative burdens and provide little additional material protection for individuals. Rather than strive for compliance with the national laws on a country-by-country basis, many multinational companies implement worldwide self-regulation (by introducing corporate privacy policies). These company-wide data protection rules provide for an adequate level of data protection, and ignore possible stricter national provisions. The foregoing significantly affects the capacity of EU DPAs to enforce compliance by multinational companies in the area of data protection. The introduction of corporate privacy policies by multinational companies has created a bottom-up pressure on national legal orders. This is reflected in how third-party beneficiaries of such policies invoke them before national courts (so far mainly in the US), and the pressure exerted on the EU DPAs to recognise these corporate privacy policies as instruments to ensure an adequate level of data protection throughout these multinational groups of companies, justifying the international transfers of data between these group

companies, wherever located. The Working Party 29[5] recognises the added value of transnational private regulation (**TPR**) in the data protection area in light of the gaps and deficiencies of the present EU data transfer regime. The Working Party 29 set criteria for this TPR to provide for a minimum level of protection for the processing of data by a multinational on a worldwide basis. To express the binding character of these corporate privacy codes, the Working Party 29 calls these "Binding Corporate Rules" (**BCR**). With BCR, the Working Party 29 introduced a complex hybrid system of self-regulation (corporate privacy policies) with public arrangements (the DPAs validating such corporate privacy policies and providing support in the area of enforcement). The BCR regime established by the Working Party 29 introduces the possibility of worldwide central enforcement of such BCR by the DPA and courts of the EU headquarters of the multinational.

The regulatory environment described above, and the deficiencies in protection and enforcement make a challenging background to research whether any gaps and deficiencies in the present applicability and jurisdiction regime of the Data Protection Directive may be addressed by transnational self-regulation, rather than by long arm jurisdiction-based legislation and jurisdiction-based enforcement. Of special interest in that context are the relative merits of central enforcement of BCR through one lead DPA (this lead DPA taking over the enforcement from other DPAs) over the present reliance on enforcement on a network basis (whereby DPAs cooperate in the enforcement in order to enable each DPA to enforce on its own territory). This research question will be addressed in Part II.

1.2.2 Research Objectives and hypotheses

Part I: Assessment of the EU applicability and jurisdiction regime

Research Objective Part I

Within the EU, there is much debate as to how EU national data protection laws apply in an international situation. The applicability rule of the Data Protection Directive has not been implemented by the Member States in a uniform manner. As a consequence, the national DPAs are left to their own devices as to when to apply their data protection law and in practice do so in a highly divergent manner. None of the existing publications[6] evaluates the full scope of application of the Data Protection Directive, its long arm reach,

5 See on the Working Party 29 n 2.

6 See for an overview of publications in respect of the applicability and jurisdiction regime of the Data Protection Directive the Bibliography Part I.

instances of overregulation, possible gaps in the protection and unnecessary cumulation of applicable laws. The applicable law and jurisdiction rules of the Data Protection Directive require independent research as these rules consist (mainly) of specific connecting factors unique to the data protection field, as a consequence of which research into the general applicable law and jurisdiction rules under international private law as well as other specific areas of EU law presenting similar transnational issues, are of limited relevance only.

Also, within the EU the enforcement of data protection legislation is based on a jurisdictional approach with different regulators cooperating in the event of cross-border issues. None of the existing publications evaluates the possible deficiencies and gaps in enforceability in practice. Research is indicated on the jurisdiction system under the Data Protection Directive and the gaps in enforcement as they present themselves in practice, whether by lack of cooperation between states, lack of enforcement tools, lack of resources or the sheer scale of non-compliance. In this context there is a need for evaluation whether the fundamentals of the present applicability and jurisdiction regime of the Data Protection Directive are still appropriate in light of the present seamless technical landscape and the worldwide data protection regulatory landscape as it emerges today. The research will lead to proposals for a new or improved applicability and jurisdiction system.

Research Hypotheses Part I

(1) The present applicability regime of the Data Protection Directive is not adequately harmonised and on the one hand leads to gaps in the protection of personal data (Article 4(1)(a) Data Protection Directive) and on the other hand to an arm's length scope which has little hope of enforcement (Article 4(1)(c) Data Protection Directive).
(2) The present jurisdiction regime is adequately harmonised, does not lead to gaps in enforcement or “exorbitant” jurisdiction, but does not provide for meaningful redress in practice.

Part II: Assessment of the suitability and relative merits of transnational self-regulation of data protection as an instrument to regulate global corporate conduct

Research Objective Part II
In the recent past a vast body of research has been conducted into:

(i) the legitimacy of TPR to regulate corporate conduct in a globalised society;
(ii) how TPR can be aligned with principles of private international law (**PIL**)
(iii) how TPR can be used to implement the "principle of accountability" in respect of compliance with the relevant legal requirements; and
(iv) the area of Corporate Social Responsibility (**CSR**), where multinationals also implement TPR to overcome differences in regulations and regulatory approaches between countries and as part of their global reputation management.

None of the research above addresses specifically that of TPR regulating data protection in an international environment. Also, the Working Party 29 and the DPAs have little experience with TPR as a tool to regulate cross-border data compliance. Though the Working Party 29 has recently approved the concept of BCR, some DPAs still struggle with the requirements under which these BCR can be recognised and enforced. Similar uncertainty exists as how to fit the BCR concept with the regulatory data protection regimes of other countries or regions like the APEC Privacy Framework. Given this lack of experience, I assess the BCR regime in light of the findings of existing general research into the legal arenas above. Two main topics I address are to what extent data protection may be regulated by TPR and whether any choice of law and forum is allowed under PIL so that indeed central enforcement of BCR is possible. The research results in proposals for improvement of the BCR regime as well as proposals how to fit this hybrid system with other existing data protection regimes across the world (especially in the US) and new regulatory regimes in development today (especially by the APEC countries). The objective is to investigate how to further the acceptance of BCR as a mainstream global solution to regulate global corporate conduct in the area of data protection. BCR may then indeed provide a private solution to solve the gaps in protection and enforcement as presented by the current patchwork of national data protection laws and jurisdiction based enforcement thereof.

Research Hypotheses Part II

(3) BCR as an instance of TPR can do better than the present territory-based state regulation of data protection in terms of:
  (a) avoiding gaps in protection and enforcement as presented by the current patchwork of national data protection laws and state based enforcement; and
  (b) regulating transborder data flows.

(4) The BCR regime as currently developed by the Working Party 29 does not sufficiently incorporate or is not sufficiently aligned with principles of international private law, best practices when implementing the principle of accountability, generally accepted legitimacy demands made of TPR, and best practices as to CSR, in order for BCR to be acceptable on a global basis as a form of TPR to regulate global corporate conduct in the area of data protection.

1.2.3 Structure, Relevance and Recommendations

This dissertation is divided into 2 parts.

Part I discusses and evaluates the applicability and jurisdiction regime of the Data Protection Directive and is dedicated to Research Objective 1. My conclusions in respect of Research Objective 1 and an evaluation of Research Hypotheses 1 & 2 can be found at the end of Part I (Chapter 5).

Part II discusses and evaluates the BCR regime and is dedicated to Research Objective 2. My conclusions in respect of Research Objective 2 and an evaluation of Research Hypotheses 3 & 4 can be found at the end of Part II (Chapter 16). In this conclusion I have also incorporated my findings in respect of Part I and to that extent Chapter 16 provides my overall conclusions of this study.

With this study, I intend to (i) contribute to the academic debate on these topics; (ii) achieve more clarity and uniformity on how these concepts should be applied in practice; (iii) further the acceptance of BCR as a mainstream global solution to regulate global corporate conduct in the area of data protection; and (iv) provide concrete suggestions to EU legislators on how to improve these regimes.

Re (i) Academic relevance

The academic relevance of my research has already been addressed in the previous paragraphs. In addition, I would also mention that the assessment of the BCR concept in particular in light of the findings of the existing research into the legitimacy of TPR to regulate corporate conduct in a globalised society, adds an interesting concrete example in practice to test the merits of these findings. This is particularly relevant as under EU law data protection qualifies as a human right[7], and the existing literature is divided on the issue whether human rights are indeed fit to be regulated by

[7] See in detail Chapter 7, n3.

TPR (and in particular CSR codes) and the existing research has until now not been extended to the role of self-regulation in the data protection field.[8]

Re (ii) Clarity and uniformity and (iii) Further acceptance of BCR as mainstream solution - societal relevance

Data protection being a human right, the present debate (and uncertainty) on how the applicability and jurisdiction regime of the Privacy Directive should be applied has serious consequences in practice. From the perspective of companies, there is no greater uncertainty than not knowing to which data protection laws your data processing is subject and which DPAs and courts have jurisdiction in this respect. Research on the applicability and jurisdiction regime under the Privacy Directive may lead to a uniform EU-wide interpretation which will enhance compliance by multinationals and therewith enhance data protection afforded to individuals. Reassessment of the applicability regime of the Data Protection Directive may well lead to introduction in the EU of a country-of-origin principle which may lead to a reduction in the administrative burden for companies. The same applies to a reassessment of the enforcement system of the Data Protection Directive, which may lead to an improved enforcement system, which in its turn will lead to enhanced data protection afforded to individuals.

Further, the substantial efforts and cost for multinationals to embark on a worldwide BCR programme without having certainty (i) whether the BCR concept will work on an EU-wide basis; and (ii) about the timeframe within which EU-wide approval of BCR may ultimately be achieved, prove an obstacle in practice for multinationals to decide on the adoption of BCR within their group of companies. Multinationals will benefit if the uncertainties as to the validity and enforcement of BCR are solved and the BCR authorisation procedure is streamlined. Given the present non-compliance by multinationals with the EU data transfer rules and the cross-border enforcement issues encountered by individuals in the enforcement of their rights, individuals may equally benefit.

The assessment of the BCR regime in light of the findings of existing research on TPR, PIL, CSR, and the accountability principle, will accelerate the acceptance and credibility of BCR as the mainstream global solution. This is not only beneficial to multinationals, but at the same time will also enhance the protection afforded to individuals of one of their fundamental rights and freedoms.

---

8 Several case studies in respect of TPR of human rights (including BCR) are presently performed as part of the HiiL Program (see on the HiiL Program para. 1.2.4).

Re (iv) Recommendations to EU legislators

My suggestions to EU legislators for improvement are not made collectively at the end, but rather throughout the text where indicated and are placed in a framework. An overview of my recommendations in Part I can be found in Chapter 5. An overview of my recommendations in Part II can be found in Chapter 16. In Annex I, a full overview of my recommendations can be found, as well as a matrix listing for each recommendation which of the disciplines led to such recommendation, as well as whether such recommendation overlaps with those made for revision of the Data Protection Directive by the Rand Report, the Working Party 29, the European Data Protection Supervisor, the Centre for Information Policy Leadership or the European Commission.

1.2.4 Prior research and publications

Chapters 2 and 3 on the delineation of the present applicability regime of the Data Protection Directive have already been published in two separate publications.[9/10] Changes to the text have been limited to attune the texts of the two earlier publications now that they are published in reversed order and some new developments have been included. Further, additional footnotes have been inserted in red to show the opinion of the Working Party 29 on the respective issues, which it issued in its 2011 Opinion on applicable law.[11] My publications were available to the Working Party 29 when deliberating and drafting this opinion, and I have inserted additional footnotes in these Chapters in red to reflect the position of the Working Party 29 on the respective issues, which in many instances deviates from earlier its opinions.

---

9 Lokke Moerel, "The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", [2011] 1 International Data Privacy Law, at 23 - 41. This publication at its turn was based on a paper presented at the 2009 ESIL-ASIL Research Forum 'Changing Futures? Science and International Law', held in Helsinki, Finland, October 2009.

10 Lokke Moerel, "Back to basics: when does EU data protection law apply?", [2011] 2 International Data Privacy Law at 92-110 This publication in its turn draws on two earlier publications in Dutch on the interpretation by the Dutch DPA of Article 4 of the Dutch Data Protection Act, 'Back to Basics: wanneer is de Wet bescherming Persoonsgegevens van toepassing'?', 2008/ Computerrecht, at 81 and 'Art. 4 Wbp revisited'; naschrift De nieuwe WP Opinie inzake Search Engines', 2008/6 Computerrecht, at 290.

11 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836/10/EN WP (**WP Opinion on applicable law**).

For this dissertation I have further made use of my desk research[12] performed as part of the HiiL Research Program 'Private Actors and Self-Regulation', into the legitimacy, effectiveness, enforcement and quality of different forms of TPR (**HiiL Program**).[13] As part of the HiiL Program, I carry out a case study into the legitimacy, effectiveness, enforcement and quality of BCR, as a form of TPR of data protection. The empirical research in respect of the effectiveness of BCR in providing material data protection to individuals is outside the scope of this publication, but is currently being conducted as part of the HiiL Program, and will be published at a later stage.[14] The point of departure for this dissertation is that data protection

---

[12] In particular my paper "Transnational Private Regulation of Data Protection" prepared for the 2010 HiiL Annual Conference on Transnational Private Regulation, June 2010, Dublin, to be found at <www.privateregulation.eu>.

[13] For the scope of the HiiL Program's research, see HiiL 2008, "The Added Value of Private Regulation in an International world? Towards a Model of the Legitimacy, Effectiveness, Enforcement and Quality of Private Regulation" and the "Draft Inventory Report", both dated May 2008 and to be found at <www.hiil.org>. The central research questions of the HiiL program are set out in the Draft Inventory Report at para. 2.5:

1. Is regulation with a transnational dimension, drafted by private actors, more successful than formal, state-regulation in regulating the conduct of corporations active in the global market?
2. If so, to what extent, under what conditions and with respect to which areas does private regulation have a – positive or negative – impact upon the effective and efficient functioning of national legal orders?
3. The main objective of the research is to formulate a model (or a number of models), which could be of use to governments and to private actors, in which these questions come together and be answered.

The HiiL Program will, on a theoretical level, research the following topics:

- What are the transnational constitutional foundations of private regulation;
- What are the differences between private regulation at national and transnational level: what contrasting modes of acquiring legitimacy and effectiveness are adopted;
- What is the role of private regulation as an alternative or a complement to public regulation (are there common principles that can be identified?);
- What factors or principles are – or should be – relevant/decisive in making regulatory choices from the point of view of effectiveness (including learning), enforcement, legitimacy and quality? (normative determinants);
- What are the unintended (and potentially counterproductive) effects associated with the emergence of a plurality of legal regimes at transnational level in terms both of effectiveness and legitimacy;
- What is the role of regulatory impact assessment concerning the choice between public and private regulation and the principle of proportionality?

[14] The final report of the HiiL Program is expected in December 2012.

regulation should be designed and evaluated based on whether rules provide for material data protection for individuals in practice rather than whether they provide for rights and remedies in theory.[15]

1.2.5 Scope of Research

This dissertation does not concern itself with the desirability of data protection legislation per se or the relative merits of the different regulatory systems set up by legislators across the world. Multinationals have to operate in the present regulatory landscape and for this dissertation this is taken as a given.

I further concentrate on the topic of cross-border data protection and enforcement in the private sector. This concerns cross-border flows of personal data both within groups of companies and between groups of companies. Though many types of cross-border data flows are carried out between public authorities and further between companies and public authorities (especially for law enforcement purposes), these types of data flows give rise to special issues and are outside the scope of this research.

The study is current up to 1 May 2011, and all hyperlinks were valid on that date.

1.3 Outline

Chapter 2 discusses the key concepts of Article 4(1)(a) Data Protection Directive which contains the main default rule for applicability of EU data protection law. A uniform interpretation of this rule is provided based on the legislative history of the Data Protection Directive. Discussed are the differences in the national implementations and the resulting divergent interpretations by the DPAs. The position of the Working Party 29 in the SWIFT Opinion is evaluated (which seems contrary to the legislative history of the Directive). The chapter concludes with recommending EU legislators how best to revise this applicability rule of the Data Protection Directive.

---

[15] In July 2010, the Working Party 29 explicitly embraced this perspective of 'law in action' as opposed to 'law in theory': see WP 173, Opinion 3/2010 on the principle of accountability adopted on 13 July 2010 (**WP Opinion on the principle of accountability**) at 3: "Data protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures. (…) In its document on The Future of Privacy (WP 168) of December 2009, the Article 29 Working Party expressed the view that the present legal framework has not been successful in ensuring that data protection requirements translate into effective mechanisms that deliver real protection."

Chapter 3 discusses the key concepts of Article 4(1)(c) Data protection Directive, which contains the rule for applicability of EU data protection law to non-EU websites. A uniform interpretation of this rule is provided based on the legislative history of the Directive. Discussed are the differences in national implementations and the resulting divergent interpretations by the DPAs. The present means used by websites worldwide to collect personal data of their visitors, like cookies, JavaScript, ad banners and spyware are analysed and it is evaluated whether the applicability rule should indeed lead to application of the EU data protection rules to the processing of personal data of EU citizens by non-EU websites. The position of the Working Party 29 is evaluated (which seems contrary to the legislative history of the Directive). The chapter concludes with recommending EU legislators how to revise this applicability rule to make the Directive fit for application in the digital era.

Chapter 4 discusses the jurisdiction regime of the Data Protection Directive: when are the DPAs competent to take enforcement action and when can individuals address the DPAs or the courts of a Member State with a complaint or claim that their data protection rights have been violated? A uniform interpretation of these jurisdiction rules is provided based on the legislative history of the Directive. Discussed are the differences in the national implementations. An evaluation is given of the jurisdiction regime for the DPAs against international jurisdiction principles under public international law. The chapter concludes with recommending to EU legislators to harmonise the jurisdiction regime and how to align this with the applicability regime as improved per my recommendations.

Chapter 5 presents my conclusions and recommendations in respect of the research objective and hypotheses of Part I.

Chapter 6 contains an introduction to Part II.

Chapter 7 gives an introduction to the worldwide data protection regulatory landscape and the different types of regulatory systems. An overview is given of the basic principles of the Data Protection Directive, as knowledge of these principles is required for a proper understanding of the BCR regime. The APEC Privacy Framework is also discussed as a representative of a data protection system based on an organisational approach rather than a territorial approach.

Chapter 8 discusses some trends and developments in the regulatory landscape, such as the increasing tensions between the different regulatory systems, the prospects of the growing call for a global data protection

standard, and the cross-border enforcement issues presently encountered by DPAs and individuals alike. The chapter concludes with a discussion of possible alternative solutions to improve the position of individuals in case of cross-border data protection violations. One of these solutions requires the introduction by multinationals of global corporate self-regulation backed up by government enforcement. By introducing the possibility for multinationals to make a choice of law and forum in these self-regulatory codes, it would be possible to have these codes supervised and enforced on a worldwide basis by one "lead" DPA only, preferably the authority of the place of establishment of the headquarters of such multinational.

Chapter 9 discusses a number of practical developments encountered by multinationals, which result in the data processing operations of multinationals being governed by a myriad of national data protection laws. It is subsequently discussed why and how multinationals mitigate their global data protection risks by means of a global corporate privacy code.

Chapter 10 introduces the BCR regime as developed by the Working Party 29, recognising corporate self-regulation as an alternative method for multinationals to comply with the EU data transfer rules. The European BCR approval procedure is discussed as well as its shortcomings. It is further discussed in which non-EU countries BCR are (potentially) recognised as a valid data transfer tool also for data transfers from these non-EU countries. Recommendations are made to recognise BCR as a valid tool for data transfers in the revised Directive and to streamline the BCR authorisation procedure.

Chapter 11 discusses some contractual issues in light of the requirement that BCR should be internally binding on the group companies and employees of the multinational and externally binding for the benefit of the beneficiaries of BCR. The latter requires discussion of the enforceability of unilateral undertakings by the beneficiaries of BCR. TPR is further often effectuated through contractual "supply chain management", a solution which is also part of the BCR regime. Also supply chain management raises issues of enforceability by the beneficiaries of these contracts, which are of equal relevance to BCR. How the various supply chain issues can be best addressed in BCR is also discussed.

Chapter 12 discusses the interaction of BCR with rules of Private International Law (**PIL**), which is twofold. First there is the traditional function of PIL, where for instance a choice of law and forum made in BCR has to comply with rules of PIL. This requires answering the questions of (i) which instruments of PIL are in scope?; do the rules of PIL take precedence

over the applicability and jurisdiction regime of the Directive; and (iii) is a choice of law possible under the Directive? It is further discussed how the BCR applicability and enforcement regime can be best set up to avoid the current pitfalls under the employee and consumer protection regimes of PIL. The second function of PIL is as a potential source of "meta-norms" for BCR. It is discussed how the BCR applicability and enforcement regime can be best aligned with the underlying policy choices behind PIL instruments and doctrines in order to be able to achieve universal acceptance of BCR.

Chapter 13 discusses BCR in the wider context of the introduction of the "accountability principle" in the area of data protection and in other fields of law.
Specific attention is devoted as to how regulators can provide companies with incentives and tools to use their own inherent "regulatory capacities". Separately discussed are the merits and the relevance for BCR of the proposal by the Working Party 29 to introduce in the revised Data Protection Directive a provision that controllers will remain accountable for the protection of their data also after these data have been transferred to a third party.

Chapter 14 evaluates BCR as a form of TPR. This concerns the issue of what the optimal form of meta-regulation is when choosing TPR. The discipline of how best to regulate (the rules for rule making, the search for meta-norms) has in the EU become known under the label "Better Regulation" (**BR**). In this chapter BCR are evaluated from the perspective of BR as to whether (i) the norm-setting as to BCR meets the basic requirements for EU law-making, for instance as to requirements of participation and transparency; and (ii) BCR (qualifying as co-regulation) concern an area of law for which European institutions consider co- or self-regulation appropriate. Proposals are made to bring the BCR norm-setting, evaluation / monitoring and enforcement in line with the body of thought on BR.

Chapter 15 addresses BCR as a form of Corporate Social Responsibility (**CSR**). It is discussed to what extent data protection is covered by international soft law instruments setting guidelines for CSR, and if so, whether this has any repercussions for the BCR regime. This requires (again) a discussion of regulating human rights, not so much in the context of whether these may be regulated by self-regulation, but whether the international instruments on CSR require that fundamental rights held by individuals should be viewed as imposing duties directly on multinationals, even for activities of these multinationals in countries that do not recognise such human rights.

Chapter 16 presents my overall conclusions and recommendations and gives an evaluation of the research objectives and hypotheses of combined Parts I and II.

PART I THE APPLICABILITY AND JURISDICTION REGIME OF THE DATA PROTECTION DIRECTIVE

2 When does EU data protection law apply?

2.1 Introduction

It is much debated when the data protection laws of the EU Member States apply in international situations. The rules of applicability of the EU Data Protection Directive[1] (**Data Protection Directive**) are extraordinarily complex. The lack of guidance in the Data Protection Directive on key concepts of applicable law and jurisdiction (and the absence of case law of the European Court of Justice) has led to unacceptable differences in the manner in which this provision is implemented in the Member States. Also, the opinions of the Working Party 29[2] have adopted conflicting interpretations of the law. As a consequence, the national data protection authorities (**DPAs**) are very much left to their own devices as to when to apply their data protection law, and in practice do so in a divergent manner, which causes widespread confusion within the international business community. Given the substantial obligations of controllers under the Data Protection Directive, there is no greater uncertainty than not knowing to which data protection laws your data processing is subject. The Data Protection Directive thus fails to meet its broader legal purpose to operate as a single market measure.[3] In this Chapter, an attempt is made to provide a uniform interpretation of the main applicability rule based on the legislative history of the Data Protection Directive. Suggestions are also made as to which key concepts require further guidance from the Working Party 29 and what amendments to the Data Protection Directive should be considered.

The Data Protection Directive applies 'to the processing of personal data in the context of the activities of an establishment of the controller on the territory of the Member State'.[4] This provision has been implemented by some Member States by providing that their national data protection law applies only if the data controller is established on their territory. Also, some DPAs and authors apply the provision in this manner. At first glance this

---

1 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

2 See on the Working Party 29 Chapter 1, n 2.

3 The legal basis for the Data Protection Directive is Article 95 (formerly 100a) of the Consolidated Version of the Treaty establishing the European Community, [2002] OJ C325/1 (**EC Treaty**). See further Recitals 1 – 9 of the Data Protection Directive. The EC Treaty has been replaced by the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**). Article 95 EC Treaty is now Article 114 TFEU.

4 Article 4(1)(a) Directive.

appears to be a perfectly legitimate interpretation of the Data Protection Directive, but it creates a gap in the legal protection of personal data. As is often the case, it is necessary to review the full legislative history of a Data Protection Directive in order to determine the correct application. In this case, the outcome is surprising. The Data Protection Directive seems to declare a national data protection law already applicable if the data processing takes place in the context of the activities of an establishment of a controller that is located on its territory. The controller itself does not have to be established in the Member State in question. This leads to a much wider scope of application of the national data protection laws. Further, in its SWIFT Opinion[5], the Working Party 29 also applied the national data protection law of the Member State of the controller to data processing by establishments of such controller in other Member States (thereby sidelining the national data protection law of the establishments in the other Member States). This position of the Working Party 29 is probably designed to preclude an unnecessary cumulative application of the national EU data protection laws. However, it will become apparent that this interpretation by the Working Party 29 does not solve the problem of the cumulative application of national data protection laws, but rather creates gaps in the legal protection of personal data. Although the attempt of the Working Party 29 to avoid cumulative application of the EU data protection laws is very commendable, this result will only be achieved if the 'country of origin' principle is also introduced into EU data protection law, which should be done by European legislation and not via the short-cut of opinions of the Working Party 29. In its first evaluation of the Data Protection Directive in 2003,[6] the European Commission recognised the lack of clarity of Article 4 of the Data Protection Directive, but announced that it would first take as its priority ensuring the correct implementation of Article 4 of the Data Protection Directive in all Member States, before considering amendments. In December 2009, the Working Party 29 also acknowledged the problem of the lack of clarity of Article 4 and the many different interpretations of it,

5 Working Party 29, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006) (**SWIFT Opinion**).

6 See Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final, at 17 (**First Report on the Directive**). Similarly, a study sponsored by the European Commission highlights the ambiguity and divergent implementation of the applicable law rules in the Directive and recommends that "better, clearer and unambiguous rules are desperately needed on applicable law". See "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments", January 2010, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

and announced that it was writing a further opinion on the concept of applicable law, which would include recommendations for revisions for the future legal framework, this in response to the revision of the Data Protection Directive launched by the Commission on 1 July 2009.[7] The Commission seemed to have moved on as well and announced in November 2010[8] that it would indeed revise and clarify the applicability rule. In this dissertation an attempt is made to provide a uniform interpretation of the applicability rule based on the legislative history of the Data Protection Directive and the suggestion is made to introduce a 'true' country-of-origin principle for data protection. In December 2010, the Working Party 29 issued its further WP Opinion on applicable law.[9] The text of my publication on which this Chapter 2 is based, was available to the Working Party 29 when drafting its opinion. I have inserted additional footnotes in red to reflect the position of the Working Party 29 on the respective issues, which in many instances deviates from its earlier opinions.

2.2 Article 4(1)(a) of the Data Protection Directive

Article 4(1)(a) of the Data Protection Directive contains the key provision for the application of EU data protection law:

> '1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.'

---

7 See Working Party 29, 'The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168, 1 December 2009), at para. 26 – 28. (**WP Contribution on The Future of Privacy**).

8 See European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union', COM(2010) 609/3 (4 November 2010), at para. 2.2.1 and 2.2.3 (**EC Communication on revision of the Directive**).

9 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836/10/EN WP (**WP Opinion on applicable law**).

2.3 The legislative history

2.3.1 The country-of-origin principle

In order to understand the legislative history of the Data Protection Directive knowledge of the 'country-of-origin principle' is required. Around the time the Data Protection Directive was adopted, European legislators introduced the country-of-origin principle for various areas of law, most notably for cross-border television broadcasting services[10] and for e-commerce services.[11] According to the country-of-origin principle, the Member States each apply their own law to the services provided by service providers established on their territory (i.e. these services are governed by the law of their 'country of origin'). The other Member States must allow these services and may not apply further regulations.[12] This prevents the cumulative application of the different national laws to cross-border services within the EU. Application of the country-of-origin principle is considered justified in a European context if a certain area of law has been extensively harmonised within the EU.[13] Given the purpose of the Data Protection Directive (full harmonisation of data protection law within the EU),[14] introduction of the country-of-origin principle also for data protection law would have been the obvious choice. We will see that this was indeed the

---

10 Directive 89/552/EEC of the European Parliament and of the Council of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, [1989] OJ L 298/ 23 (**Television without Frontiers Directive**) as recently amended by Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 (renaming the Television without Frontiers Directive as the) (**Audiovisual Media Services Directive**). The implementation date of the Audiovisual Media Services Directive expired on 19 December 2009.

11 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] OJ L 178/1 (**E-commerce Directive**). See E.M.L. Moerel, 'The country of origin principle in the E-commerce Directive: the expected "one stop shop"?' [2001] CTLR, at 184.

12 See Article 2 and 2a and Recitals 10-14 Television without Frontiers Directive (n 10) and Article 3 and Recital 5 E-commerce Directive (n 11).

13 Note however that the E-commerce Directive itself harmonised no more than five selected topics and this also in a very limited way. This means that Member States are forced to allow certain information society services which comply with the applicable rules in the country-of-origin, even though those rules have not been harmonised.

14 See Recital 8 of the Data Protection Directive, indicating that the purpose of the Directive was full harmonisation with the exception of specific discretionary powers in a limited number of areas. See also Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, paras. 95-96.

original proposal of European legislators, but that this principle was abandoned in the final Directive.

2.3.2 'Being established' vs 'having an establishment'

To understand the legislative history, it is of particular relevance to recognise that application of the country-of-origin principle results in a sole place of establishment of the service provider in respect of the service involved. If a provider of e-commerce services has more than one place of business in the EU (i.e. more than one establishment), such provider is considered 'established' for purposes of application of the country-of-origin principle in the Member State where the service provider has its centre of activities for that particular service (i.e. has its primary establishment).[15] The same applies to broadcasting services.[16] The European Court of Justice (**ECJ**) has developed a body of case law to apply these criteria.[17] What is relevant here is that the concept of 'being established' for purposes of the country-of-origin principle (which refers to the primary establishment for purposes of the country-of-origin principle) is a different concept from the concept of 'having an establishment' (which is the basis for the applicability rule of the Data Protection Directive). The latter concept includes the primary establishment but especially refers to secondary establishments like subsidiaries, branches and agencies.[18] We will see that as a consequence the applicability rule of the Data Protection Directive may lead to more than one applicable law. The concept of 'having an establishment' is discussed in Paragraph 2.4.2 below.

---

15 See Recital 13 of the E-commerce Directive.

16 Article 2(3) Television without Frontiers Directive (n 10) provides a set of factors to determine which of multiple establishments involved in a certain broadcasting service should be considered to have 'effective control' over the relevant service (i.e. should be considered the 'primary establishment' for purposes of application of the country of origin principle).

17 See for an overview of the case law Oliver Castendyk, Egbert Dommering and Alexander Scheuer, *European Media Law* (Kluwer Law International 2008) 847–866.

18 Pursuant to Article 49 TFEU (formerly Article 43 EC Treaty), companies have the 'freedom of establishment' in the EU. This entails the right to set up and establish a primary establishment and the right to set up and manage secondary establishments such as subsidiaries, branches and agencies. The freedom of establishment entails that nationals of a Member State may also set up and manage secondary establishments on behalf of companies that have their primary establishment in another Member State. Most case law of the ECJ in respect of Article 49 TFEU relates to the latter issue.

2.3.3 The various stages of the legislative history

The final version of the Data Protection Directive (**Final Directive**) evolved from two draft versions, namely the Original Proposal,[19] and the Amended Proposal[20] (published together with an Explanatory Memorandum of the Commission).[21]

The three versions (i.e., the two draft versions and the final version) of the Data Protection Directive show substantial differences especially as regards Article 4(1)(a) and the corresponding Recitals. European legislators changed the connecting factor for the applicable law in each of the consecutive drafts, as a result of which the legal commentaries on Article 4 deviate according to the version of Article 4(1)(a) they relate to. Also the Explanatory Memorandum is often cited for explanatory purposes of the Final Directive, while this Memorandum relates to the Amended Proposal, which adopted a different connecting factor than that used in the Final Directive.

2.3.4 The Original Proposal: incorporating the country-of-origin principle

Article 4(1) of the Original Proposal reads as follows:

> '1. Each Member State shall apply this Directive to:
>
> (a) all files located in its territory;
> (b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.'

In the Initial Proposal the connecting factor for choosing the applicable national law was the location of the data file (i.e. based on territorial jurisdiction). In order to avoid circumvention of the applicability of EU data protection law, a transfer of the data file to a non-member country was not supposed to prevent the protection of EU data protection laws attaching to the data. This provision was also supposed to prevent cumulation of

---

19 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314 – 2, 1990/0287/COD (**Initial Proposal**).

20 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final – SYN 287, 15 October 1992 (**Amended Proposal**).

21 This Explanatory Memorandum is not available any more on the web site of the European Commission. It can be retrieved from the Archive of European Integration of the University of Pittsburgh at <http://aei.pitt.edu/10375>.

applicable laws. The Member State where the data file was located had the obligation to ensure the data processing was in accordance with EU law; the other Member States could not exercise supervision as the protection was considered sufficient to permit the free flow of data. Those familiar with the Television without Frontiers Directive and the E-commerce Directive recognise this language, which is used by European legislators to express the country-of-origin principle.

See also Recitals 10 and 12 of the Original proposal:

> "(10) Whereas any processing of personal data in the Community should be carried out in accordance with the law of the Member State in which the data file is located so that individuals are not deprived of the protection to which they are entitled under this Directive; whereas, in this connection, each part of a data file divided among several Member States must be considered a separate data file and transfer to a non-member country must not be a bar to such protection;"
>
> "(12) Whereas national laws may, under the conditions laid down in this Directive, specify rules on the lawfulness of processing; whereas, however such a possibility cannot serve as a basis for supervision by a Member State other than the State in which the data file is located, the obligations on the part of the latter to ensure, in accordance with this Directive, the protection of privacy in relation to the processing of personal data being sufficient, under Community law, to permit the free flow of data;"

2.3.5 The Amended Proposal: still the country-of-origin principle

Article 4(1) Amended Proposal reads as follows:

> '1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:
>
> (a) of which the controller *is established* in its territory or is within its jurisdiction;
> (b) of which the controller is not established in the territory of the Community, where for the purpose of processing personal data he makes use of means, whether or not automatic, which are located in the territory of that Member State.'

What is relevant here is that the phrase in italics 'is established' concerns the primary establishment and is still in line with the country-of-origin

principle. In the Explanatory Memorandum[22] of the Amended Proposal, the Commission gives the purposes of Article 4(1)(a) as follows:

> '[the intention of Article 4(1)(a) is] to avoid two possibilities:
> - that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;
> - that the same processing operation might be governed by the laws of more than one country'.

Thus, the Commission considered the location of the data file no longer to be an adequate rationale, and the new connecting factor became the place of establishment of the controller.

See Explanatory Memorandum[23]:

> "Under the original proposal the place where the file was located was to determine territorial jurisdiction, but this criterion has not been retained in the amended proposal, on the ground that the location of a file or of a processing operation will often be impossible to determine: processing operations may have more than one location and take place in several Member States (...) Under the amended proposal, therefore, the law applicable is defined by reference of establishment of the controller."

The Explanatory Memorandum further shows that it was still the intention of European legislators to introduce the country-of-origin principle for the EU data protection laws:[24]

> 'Under the Directive the protection provided is to follow the same lines in all Member States, and will thus be equivalent throughout the Community; and paragraph 2 accordingly prevents Member States from restricting the free flow of data in the fields covered by the Directive on grounds relating to the protection of data subjects..'

Again, those familiar with the Television without Frontiers Directive and the E-commerce Directive recognise this as the expression of the country-of-origin principle.

---

22 Explanatory Memorandum (n 21), at 13.

23 Explanatory Memorandum (n 21), at 13.

24 Explanatory Memorandum (n 21), at 9.

See also Recitals 12 and 13, where Recital 12 expresses the **first rationale** (avoidance of circumvention of the protection) and Recital 13 the **second rationale** (country-of-origin principle).

> "(12) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out by a person who is established in a Member State should be governed by the law of that State; whereas, the fact that processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas, in that case, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.(…);
>
> (13) Whereas Member States may more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas, however, more precise rules of this kind cannot serve as a basis for supervision by a Member State other than the member State of residence of the person responsible for the processing, since the obligation on the part of the latter to ensure, in accordance with this Directive, the protection of rights and freedoms with regard to the processing of personal data is sufficient, under Community law, to permit the free flow of data;"

2.3.6 The final version: cumulation of applicable laws

Article 4(1)(a) of the final version of the Data Protection Directive reads as follows:

> "'1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
> (…)
> (b) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."

The changes in the Final Directive compared with the Amended Proposal could not be more drastic. The country-of-origin principle apparently was not politically viable and was abandoned, and the Member States were each allowed to apply their own law (therefore making possible the cumulation of applicable laws). The drafters also detected a further gap in protection, since the controller itself could relocate outside the EU and thus avoid the applicability of the EU data protection laws. As a consequence the wording of Article 4(1)(a) and of the corresponding Recitals was changed drastically.

To cover the possible circumvention of EU laws by relocating the corporate seat of the controller, the connecting factor in Article 4(1)(a) first sentence was changed from the Member State where the 'controller is established' (i.e. the primary establishment) to 'establishment of the controller in a Member State' (so that the presence of a secondary establishment would be sufficient for the law to apply). The processing further has to take place in 'the context of the activities of such establishment' in order to cover the possibility of circumvention of EU data protection laws by relocation of the processing itself to a country outside the EU. Finally, a second sentence was added to Article 4(1)(a) to express the cumulation principle. In line with these changes, Recital 12 of the Amended Proposal could stay as this expressed the first rationale (avoidance of gaps) and became Recital 18. Recital 13 of the Amended Proposal (expressing the country-of-origin principle) was deleted. Added was a new Recital 19 to express the cumulation principle:

See Recitals 18 and 19 Final Directive:

> "(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;
>
> (19) Whereas **establishment on** the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether a simple branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a **single** controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that **each of the establishments** fulfils the obligations imposed by **the national law** applicable to its activities."

Theoretically, the first sentence of Article 4(1)(a) Data Protection Directive leaves open the possibility that the controller must be located on the territory of a Member State.[25] However, if that indeed had been the intention of the European legislators, the provision would simply have stated that the law of the Member State where the controller is established shall apply (as the provision read in the Amended Proposal). In any event, the second sentence of Article 4(1)(a) shows unequivocally that the intention was that the law of the Member State where the establishment is located applies. The second sentence states that a controller with more than one establishment in the EU must ensure that the establishments concerned comply with the national law applicable (pursuant to the first sentence). In other words, each of these establishments must comply with the obligations laid down in the national law of the Member State in which such establishment is located.[26] This does not mean that the controller itself must be established on the territory of the relevant Member State (just that its establishment is established there).[27] This interpretation is confirmed by Recital 19 Final Directive, which is repeated here:

---

[25] The Dutch DPA bases its interpretation that the Dutch Data Protection Act only applies if the controller is established in the Netherlands on an isolated reading of this first sentence of Article 4(1)(a) of the Data Protection Directive. This sentence is then interpreted as referring to 'an establishment on the territory of the member state of the controller' (in other words, the establishment must be located on the territory of the member state where the controller is established). This interpretation is untenable in the light of the second sentence.

[26] This is confirmed by the WP Opinion on applicable law (n 9), at 12: "First of all, the reference to "an" establishment means that the applicability of a Member State's law will be triggered by the location of an establishment of the controller in that Member State, and other Member States' laws could be triggered by the location of other establishments of that controller in those Member States. Even if the controller has its main establishment in a third country, just having one of its establishments in a Member State could trigger the applicability of the law of that country, provided that the other conditions of Article 4(1)a are fulfilled (see infra sub b). This is also confirmed by the second part of the provision, which explicitly provides that where the same controller is established on the territory of several Member States, the controller should ensure that each of the establishments complies with the relevant applicable law."

[27] This is confirmed by the WP Opinion on applicable law (n 9), at 7. See also the example given at 9: "Where X also has an establishment (Y) in Member State B, the national law applicable to the processing by Y will be the national law of Member State B, provided that the processing is carried out in the context of the activities of Y. If the processing by Y is carried out in the context of the activities of the establishment of X in Member State A, the law applicable to the processing will be the law of Member State A."; and at 13: "The notion of "context of activities" does not imply that the applicable law is the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities relating to data processing."

> 'whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.'

This leads to the conclusion that in the final version of the Directive, the country-of-origin principle is abandoned,[28] and the laws of more Member States may apply to a processing of data (cumulation of applicable laws). The relevant connecting factor is whether a processing 'takes place in the context of the activities of an establishment of a controller in a Member State'. The controller itself no longer needs to be established in a Member State, nor is it required that the processing itself takes place within a Member State.

This interpretation is also the prevailing opinion in the legal commentary[29] and is further confirmed by the leading commentary on the Data Protection Directive of Dammann and Simitis (Paragraph 2.3.7), by the First Implementation Report on the Directive (Paragraph 2.3.8), and recently also by the Working Party 29 in its Opinion on Search Engines (Paragraph 2.3.9). There are, however, also a number of authors and DPAs who hold a different view. Most notably, the Dutch DPA[30] has recently published an article defending the position that Article 4(1)(a) provides as the connecting factor for applicability the place of establishment of the controller and further

---

[28] See Peter P. Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet', (1998) 32 International Lawyer 991, 1007. Swire notes that under an interpretation whereby the Directive would apply only one applicable law to an act of data processing (based on stressing the singular in the term 'national law applicable' in Article 4(1)(a) Directive), the Directive would require a substantial new jurisprudence on how to select that unique law in the huge range of circumstances to which the Directive applies. He takes this as an indication that this interpretation was not the intention of the legislators.

[29] See Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press 2007) 117-118; M.B.J. Thijssen, 'Grensoverschrijdend gegevensbeschermingsrecht' (Cross-border data protection law), (2005) Privacy & Informatie 110; P.H. Blok, 'Privacybescherming in alle staten' (Privacy protection; a problem everywhere), (2005) Computerrecht at 299 and 300; the commentaries on Article 4(1) of J.M.A. Berkvens in *Wet bescherming persoonsgegevens; Leidraad voor de praktijk*, supplement 3 (Kluwer 2002); H. de Vries in *T&C Telecommunicatierecht* (Kluwer 2009) 559-560; G-J Zwenne and Ch. Erents, 'Reikwijdte Wbp; enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp' (2009) Privacy & Informatie at 60.

[30] This publication is written on behalf of the Dutch DPA by its international coördinator M.A.H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', (2008) Computerrecht, at 287–291.

contains a conflict rule indicating only one applicable law. The counter-arguments brought forward by these authors and the Dutch DPA are discussed in the footnotes and further in Paragraph 2.7.

2.3.7 Commentary of Dammann and Simitis

That the European legislators indeed had the above in mind when drafting the Data Protection Directive is confirmed by the leading commentary on the Data Protection Directive by Dammann and Simitis.[31] Simitis was one of the drafters of the Directive and is generally considered to have 'grandfathered' the Directive. As this commentary is no longer generally available an unofficial translation follows in English:

> 'The directive does not take into account the "person involved" (his domicile or nationality)[32], but the controller of the processing and then not the place of establishment of the parent company of the controller, but the place of establishment of an establishment of the controller in the context of which the processing activities take place. The directive herewith creates a decentralisation which to a large extent results in the territoriality principle, i.e. what is decisive is the place of the processing. As a rule this has the result that also the persons involved can rely on their own well-known law for maintaining their own rights'

Dammann and Simitis are of the opinion that the second sentence of Article 4(1)(a) provides for an independent obligation of the controller that has establishments in other Member States to ensure that these establishments indeed do comply with their own national data protection laws:[33]

> 'If a controller of a data processing has one or more establishments in another Member State, the Directive also applies to these establishments; the Member State in which she [the controller] is established should oblige her to "take the necessary measures to ensure that each of these establishments complies with the requirements imposed on such establishment by applicable national law" (sub 1(a), second sentence). This provision extends further than the title of Article 4 "applicable law", it also imposes material obligations. This material obligation can be enforced against the controller by the supervising authority on the basis of Article 28(3), whereby on the basis of the territorially limited

---

31 Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997) at 127-128.

32 That domicile and nationality are not relevant is confirmed by the Working Party 29 in its Opinion on applicable law (n 9), at 8.

33 Insofar as I can see, this obligation has not been implemented in any of the data protection laws of the Member States.

> authority of the supervisory authorities, which is not changed by Article 4, cooperation between the supervisory authorities of other Member States are required pursuant to Article 28(6).'

2.3.8 First Report on the implementation of the Data Protection Directive

That the Data Protection Directive does not incorporate a country-of-origin principle[34] but is based on the principle of cumulation of laws is also confirmed by the Commission in its First Report on the implementation of the Data Protection Directive.[35] Based on a survey of the various national implementation provisions of Article 4(1)(a) (Technical Analysis),[36] the Commission concludes that Article 4 has not been uniformly implemented and that as a result conflicts of law arise that the Data Protection Directive sought to avoid. In other words, due to a lack of harmonisation in the EU, controllers have to comply with divergent national laws, leading to conflicts of law which would have been avoided if Article 4 had been uniformly implemented throughout the EU. What is relevant here is that the "conflicts of law" the European Commission refers to are different from a rule of "conflict of law" where one law takes priority to the detriment of others (as in the country of origin approach).The Commission further indicates in the Report that it will not introduce a country-of-origin principle,[37] but will first ensure the correct implementation of Article 4 of the Data Protection Directive:[38]

> "This is one of the most important provisions of the Directive from the perspective of the Internal Market and its correct implementation is crucial for the functioning of the system. The implementation of this provision is deficient in several cases with the result that the kind of conflicts of law this Article seeks

---

34 This is also confirmed by the fact that data protection laws are excluded from the scope of applicability of the E-Commerce Directive (n 11) (and therewith from applicability of the country of origin principle). See Article 1(5) E-commerce Directive.

35 See First Report on the Directive (n 6), at 17. Pursuant to Article 33 of the Directive, the Commission has to report at regular intervals on the implementation of the Directive and, if necessary, provide suitable proposals for amendment.

36 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, attached to the First Report on the Directive (**Technical Analysis**).

37 As part of the evaluation process several companies and organisations proposed to also introduce the 'home country control principle' to privacy law. See for instance J.H.J Terstegge, 'Home Country Control – Improving Privacy Compliance and Supervision', [2002] P&I at 257-259.

38 See First Report on the Directive (n 6), at 17.

> to avoid could arise. Some member states will have to amend their legislation in this regard.
>
> The provision [of Article 4] was one of the most criticised during the review process. Submissions argued for a country of origin rule that would allow multinational organisations to operate with one set of rules across the EU. (…).
> As regards the country of origin rule, the Directive already allows for the organisation of processing under a single data controller, which means complying only with the data protection law of the controller's country of establishment. This of course does not apply where a company has chosen to exercise its right of establishment in more than one member state.
>
> The Commission's priority is, however, to secure the correct implementation by the Member States of the existing provision.(…).'

Where the Commission in the First Report gives a more or less correct reflection of the applicability rule of Article 4(1)(a), the applicability rule as presented in the Technical Analysis (stating that the first ground for applicability is the place of establishment of the controller) seems to be incorrect.[39]

2.3.9 Opinion on Search Engines

After some diverging opinions (which will be discussed in Paragraphs 2.6 and 2.10 below), the Working Party 29 found its voice in its 2008 WP Opinion on Search Engines.[40] Where the earlier opinions contained references to the country-of-origin principle,[41] these are abandoned and the WP Opinion on Search Engines confirms that the data protection laws also apply in the event the controller is established outside the EU, as long as such foreign controller has an establishment within the EU and the

---

39 Technical Analysis (n 36), at 6. On behalf of the Dutch DPA, Fonteijn-Bijnsdorp (n 30), at 288, quotes this passage from the Technical Analysis and indicates that these are the words of the European Commission which support the interpretation that Article 4(1)(a) provides for the place of establishment of the controller as the main ground for applicability. However, such interpretation cannot be based on an isolated citation from an underlying fact finding report which was commissioned by the Commission from a third party.

40 Opinion 1/2008 on data protection issues related to search engines (WP 148 4 April 2008) (**WP Opinion on Search Engines**).

41 See for citation para. 2.6.

processing takes place 'in the context of the activities of such establishment':[42]

> 'Where the search engine service provider is a non EEA-based controller, there are two cases in which Community data protection law still applies... When applied to a particular search engine whose headquarters are located outside of the EEA, the questions needs to be answered whether the processing of user data involves establishments on the territory of a Member State....
>
> It is the search engine service provider that is responsible for clarifying the degree of involvement of establishments on the territory of Member States when processing personal data. If a national establishment is involved in the processing of user data, Article 4(1)(a) of the Data Protection Directive applies.'

2.4 Review of key concepts Article 4(1)(a)

Given the complexity of the key concepts of the provision of Article 4(1)(a), it is necessary to review each of these concepts below.

2.4.1 Controller (and processor)

Article 2 Data Protection Directive provides that the 'controller' is 'the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data'. From the definition it follows that it is possible to have multiple controllers for the same processing ("co-controllers").[43] A 'processor' is 'the natural or legal person or any other body which processes personal data on behalf of the controller'.

Though at first sight the Data Protection Directive provides a clear distinction between controllers and processors, this distinction cannot be easily made in respect of many complex joint processing situations within multinational companies. In this publication I will sometimes refer to the common example of a complex joint processing which exists within many multinational companies. Most multinationals process their worldwide

---

[42] WP Opinion on Search Engines (n 40), at 9-10. See also more recently 'Opinion 1/2010 on the concepts "controller" and "processor"' (WP 169 of 16 February 2010) (**WP Opinion on concepts of controller and processor**), at 5.

[43] The concept of co-controllership is under dispute in France as the definition does not incorporate the wording 'alone or jointly with others'. See also Kuner (n 29), at 70. See in detail on the concepts of controller and processor WP Opinion on concepts of controller and processor (n 42).

employee or customer data in central systems.[44] In most cases the central HR systems or Customer Relationship Management (CRM) systems are operated by the parent company which therefore processes such employee (or customer) data on behalf of its subsidiaries. At first sight this would qualify the parent as a data processor for each of its subsidiaries.

In practice, however, it is most of the time the parent company that determines centrally which software and systems will be implemented to perform the central processing, which employees of which group companies have access to the central system, and – last but not least – which data are to be included and processed in the central system. The decision about which data are to be included and processed is often prompted by the need of the parent company itself for certain information or reports from these central databases for management information purposes. As a consequence, not only employee data are included that are strictly necessary for performance of the employment agreement (for payment of salary, etc.), but also information for what is known as worldwide 'succession planning', 'tracking of high potentials', participation in worldwide 'share option schemes', etc. Inclusion of these data is more in the interest of the parent company than in the interest of the individual subsidiaries. Further, because of the structure of their organisations, hierarchically the managers of employees of foreign subsidiaries are often found at the parent company (or at other intermediate holding companies). Employees of the parent company then, for all these purposes, have access to the data of the (other) group companies in the central systems. In this case it is difficult to argue that the central processing by the parent company of the employee data of group companies takes place only on behalf of the subsidiaries. In most cases, the parent company will even be primarily responsible for the aggregate data processing in the central system, and the relevant group companies are only jointly responsible with the parent for that part of the central system that concerns their employee data. In such case, one cannot but conclude that the parent qualifies as the controller for the central system as a whole, and the

44 In this publication, a central system refers to an IT system that is implemented in one location and to which all group companies worldwide have access. This is a development of the last ten years. Before this the group companies each had their own systems that at best were linked to one another. Recently companies started using CRM on demand services whereby a cloud supplier (e.g. salesforce.com) provides the CRM applications "as a service" (i.e. software as a service, SAAS).

respective subsidiaries qualify as joint controllers for their respective parts of the central processing.[45]

Can a branch qualify as a controller?

Some DPAs[46] are of the opinion that also a branch office can qualify as a controller. The fact that a branch is not a separate legal entity is not a decisive factor in establishing whether there is a person in a particular place who is competent to determine the purposes of a processing activity. 'Control' for data protection purposes is a very different concept than control under corporate law.[47] In this view a branch could qualify as a controller in

---

45 The Working Party 29 in its recent Opinion on concepts of controller and processor (n 42) does not discuss this common example. A similar example is, however, given by the Working Party 29 in its Opinion on applicable law (n 9), at 15:
"Example No. 4: Human resources centralised database
Situations where the same database can be subject to different applicable laws do increasingly happen in practice. This is often the case in the field of human resources where subsidiaries/establishments in different countries centralise employee data in a single database. While this traditionally happens for reasons of economies of scale, it should not have an impact on the responsibilities of each establishment under local law.
This is the case not only from a data protection perspective, but also in the context of labour law and public order provisions. If, for instance, data of the employees of an Irish subsidiary (which qualifies as establishment) were transferred to a centralised database in the UK, where data of employees of the UK subsidiary/establishment are also stored, two different data protection laws (Irish and UK) would apply.
The application of two different national laws is not simply a result of the data originating in two different Member States, but instead arises as the processing of the Irish employee data by the UK establishment takes place in the context of the activities of the Irish establishment in its capacity of employer." I take it that the Working Party 29 here means that UK law applies to the processing of the UK employee data and Irish law to the processing of the Irish data in the central data base (and not that both laws apply to the processing as a whole). The example does not discuss the situation where the UK subsidiary also uses the Irish data for its own purposes such as management information purposes, which is a common feature of central data processing systems.

46 For instance the Dutch DPA, see Fonteijn-Bijnsdorp (n 30), at 289. This despite the fact that the legislative history of the Dutch Data Protection Act clearly indicates that a controller is the formal legal entity that is responsible for the processing in order for those involved to be aware against which (legal) person they may exercise their rights. See Explanatory Memorandum to the Act, 25 892, no. 3, at 55

47 See also Kuner, (n 29), para. 2.23.

its own right.[48] How this should be reconciled with the legal obligations subsequently imposed on such a controller (like notification) is unclear. Only formal (legal) persons can have rights and obligations. In the case of a branch this would be the parent entity (to avoid one natural person within the branch being personally accountable for the processing of its employer). Any claim could only result in legal liability if it were brought against the legal entity controlling (under corporate law) the controller (under data protection law). Thus legal certainty would be best served if only the formal (legal) person being responsible for the processing at hand could qualify as a controller. In Paragraph 2.9 (Case II) it is shown why this properly fits with the interpretation of Article 4(1)(a) Data Protection Directive as advocated in this publication. In its recent Opinion on the concepts of controller and processor,[49] the Working Party 29 seems to confirm this by first indicating that for purposes of defining the concept of controller, 'it is important to stay as close as possible to the practice established both in the private and public sector by other areas of law' and that 'preference should be given to consider as controller the company (…) as such', so as ' to provide data subjects with a more stable and reliable reference entity for the exercise of their rights under the Directive'.

2.4.2 Establishment of the controller

There must be an 'establishment' of the controller. The notion of 'established' is left undefined by the Data Protection Directive save for some explanatory comments in Recital 19 of the Data Protection Directive: 'establishment on the territory of a Member State' is considered to imply 'the effective and real exercise of activity through stable arrangements' and 'the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect'. The Working Party 29 further indicated in various opinions[50] that 'the existence of an 'establishment' has to be determined in conformity with the case law of the ECJ.' The Working Party 29 seems to refer to Article 50 TFEU (formerly 43 EC Treaty) on the 'freedom of establishment'. The case law it cites, however, mainly concerns situations whereby Member States violate the freedom of establishment by introducing obstacles to the setting up and managing of secondary establishments in their Member States while the

---

48 The Dutch DPA for instances applies this view to subsequently conclude that the relevant branch is established in the Netherlands and that therefore the Dutch data protection law applies.

49 See n 42, at 15 – 16.

50 See Working Party 29, 'Opinion 1/2008 on data protection issues related to search engines' (Chapter 3, n 19), at 10. This is confirmed in the WP Opinion on applicable law (n 9), at 11.

primary establishment is located in another Member State and therefore seems of less relevance here.[51] The concept of 'establishment' features however in many EU regulations and directives. Of more relevance seems to be the case law under Articles 5(5) and 13(2) of the Brussels Convention[52] (the predecessor of the Brussels I Regulation[53]), which use the presence of an 'establishment' in a Member State as a connecting factor for jurisdiction purposes.[54] The ECJ[55] considers an essential factor for the concept of branch

---

51 The Working Party 29 in its WP Opinion on applicable law (n 9), at 11, confirmed the assumption that with its reference to case law of the ECJ it referred to case law of the ECJ in respect of the freedom of establishment under Article 50 TFEU, and acknowledged that "it is not clear whether this and subsequent interpretations by the ECJ as regards the freedom of establishment under Article 50 TFEU [can] be fully applied to the situations covered by Article 4 of the Data Protection Directive." At 11, the Working Party indicated that according to the ECJ "a stable establishment requires that 'both human and technical resources necessary for the provision of particular services are permanently available", this referring to "ECJ judgment of 4 July 1985, *Bergholz*, (Case 168/84, ECR [1985] p. 2251, paragraph 14) and judgment of 7 May 1998, *Lease Plan Luxembourg / Belgische Staat* (C-390/96, ECR [1998] p. I-2553). In the latter case the issue was to determine whether a company server, situated in a country different from the country of the service provider, could be considered a stable establishment for purposes of VAT payment. The judge refused to consider computer means as a virtual establishment (returning with this interpretation to a more "classical" notion of 'establishment', different from the one adopted in a previous judgment of 17 July 1997, *ARO Lease / Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, ECR 1997 p. I-4383).

52 Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, [1972] OJ L299/31 at 32, as amended by Conventions on the Accession of the New Member States to that Convention, consolidated text [1998] OJ C27/1.

53 EC Regulation 44/2001 of 22 December 2000 on jurisdiction and enforcement, [2001] OJ L12/1. The Brussels I Regulation should be interpreted in the light of the case law decided under the Brussels Convention, see the opinion of the A-G Leger in Case C-281/02 *Owusu* [2005] ECR I-1383.

54 According to the ECJ the term 'establishment' should be construed autonomously in the light of the purpose and scheme of the relevant regulation. The concept 'establishment' in the Data Protection Directive will therefore have to be construed in accordance with the purpose and scheme of the Data Protection Directive. See concerning Article 5(5) Brussels Convention: Case 33/78, *Somafar SA v. Saar-Ferngas AG* [1978] ECR 02183. See in detail Foss and Bygrave, 'International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law', 2000 International Journal of Law and Information Technology, volume 8, at 99 – 138, and Oren, 'Electronic Agents and the notion of Establishment', at 8, available at <www.eclip.org>. The Brussels I Regulation should be interpreted in the light of the case law decided under the Brussels Convention, see the opinion of the A-G Leger in Case C-281/02 *Owusu* [2005] ECR I-1383.

55 Case 139/80*, Blanckaert & Willems PVBA v. Luise Trost* [1981] ECR 00819, para. 9.

or agency 'the fact of being subject to the direction and control of the parent body'. Further conditions that have to be met according to the ECJ[56] are:

> 'the concept of branch, agency or other establishment implies a place of business which has the appearance of permanency, such as the extension of a parent body, has a management and is materially equipped to negotiate business with third parties so that the latter, although knowing that there will if necessary be a legal link with the parent body, the head office of which is abroad, do not have to deal directly with such parent body but may transact business at the place of business constituting the extension'.

It seems that the above conditions can equally apply to determine whether certain business activities of a parent entity qualify as an 'establishment' under the Data Protection Directive. Based on the above criteria the conclusion is that all subsidiaries and most branch offices will qualify as establishments. The interesting question in the data protection context is whether a third party (i.e. not a subsidiary) that processes personal data on behalf of a controller could qualify as an 'establishment' of such controller. An obvious example would be the case where a non-EU website is hosted by a service provider in the EU. What is relevant here is specific case law of the ECJ in respect of the circumstances under which an 'independent agent' may qualify as an establishment. According to the ECJ this depends on the degree of independence of such third party (whether the external perception is that he is under the 'direction and control' of the parent body). If the third-party agent is basically free to organise its own work and free to represent competing companies (it carries out its own decisions), such third party does not qualify as an establishment.[57] Based on this case law some authors conclude that under very special circumstances only external specialists and service providers would qualify as someone else's establishment.[58] An example could be a far-reaching form of BPO outsourcing where the employees of the relevant service provider are dedicated to the services and under the direction and control of the data controller. However, as a rule independent outsourcing service providers do not seem to qualify as an 'establishment' of the controller. Given the grey area here, it would obviously be welcomed if the Working Party 29 were to

---

56 Case 33/78 *Somafar SA v. Saar-Ferngas AG* [1978] ECR 02183.

57 Case 139/80 *Blanckaert & Willems PVBA v. Luise Trost* [1981] ECR 00819.

58 Mankowski, in Ulrich Magnus and Peter Mankowski (eds.) *Brussels I Regulation* (Sellier European Law Publishers 2007) at §§ 279 and 292–295.

elaborate under what circumstances a third-party agent could qualify as an 'establishment' of a controller (if any).[59]

Again, I note that the concept of "establishment" is also found in the Audiovisual Media Services Directive and the E-commerce Directive, but this concept is less relevant here. These directives make clear that if a service provider has multiple places of "establishment" in the EU, such service provider will be considered "established" for purposes of application of the country of origin rule in the Member State where the service provider for the e-commerce service has its centre of activities or is considered to have its centre of effective control over the broadcasting service (i.e. to determine the "primary establishment" for purposes of application of the country-of-origin principle). Any commentaries on these provisions focus on this aspect of being "established" and not on the prior question of when a certain activity qualifies as an "establishment" under the case law of the ECJ. These commentaries are therefore less relevant for the concept of "establishment" in the Data Protection Directive.[60]

---

59 In its Opinion on applicable law (n 9), at 11-12, the Working Party 29 gives four examples applying the case law of the ECJ as to the freedom of establishment:
"- Where "effective and real exercise of activity" takes place, for example in an attorney's office, through "stable arrangements", the office would qualify as an establishment.
- A server or a computer is not likely to qualify as an establishment as it is simply a technical facility or instrument for the processing of information.
- A one-person office would qualify as long as the office does more than simply represent a controller established elsewhere, and is actively involved in the activities in the context of which the processing of personal data takes place.
- In any case, the form of the office is not decisive: even a simple agent may be considered as a relevant establishment if his presence in the Member State presents sufficient stability." The Working Party 29 has not given direction on the grey area whether an independent third-party processor can qualify as an establishment of the controller.

60 See on Article 2 Audiovisual Media Services Directive: Dommering (n 17) at 847 – 866. On p. 850, the author draws a parallel between deciding under the Audiovisual Media Services Directive which company of a group of companies within the EU qualifies as the 'media service provider' based on the criteria for determining the 'centre of effective control' and the distinction the Data Protection Directive makes between the 'controller' and the 'processor'. In the opinion of the author, the media service provider is the equivalent of the 'controller' under the Data Protection Directive. This parallel does not work. Under the Audiovisual Media Services Directive (as under the E-commerce Directive) only **one company** of a group of companies within the EU qualifies as 'the media services provider' for a certain media service. Under the Data Protection Directive more group companies can qualify as co-controllers in respect of one processing. Further, the connecting factor under the Data Protection Directive is not the Member State where the controller is established, but sufficient is that an

2.4.3 Establishment of the controller on the territory of a Member State

There must be an 'establishment of the controller on the territory of a Member State'. This element does not require further discussion. It has just been shown that a review of the legislative history of the Data Protection Directive yields the interpretation that the national data protection laws already apply if an establishment of the controller is established in a Member State. For this purpose, the controller itself need not be established in a Member State.

2.4.4 In the context of the activities of an establishment

The national data protection laws only apply when the data processing takes place 'in the context of the activities of an establishment'. The Data Protection Directive does not state that the data processing must be carried out by the establishment in a Member State.[61] On the contrary, European legislators meant to abstract from the location where the data processing takes place. If location were be decisive, this would easily facilitate bypassing the national laws, for instance by relocating the servers to another jurisdiction.[62] It is therefore very well possible for data processing to take place in the context of the activities of an establishment in a Member State, but that the data processing itself is carried out by a third party outside this Member State (whether in another EU Member State or outside the EU). This underlines the long arm reach of the Data Protection Directive.

In today's context this has become a matter of course. For instance, a foreign parent company often processes data centrally for its EU group companies. If that processing takes place in the context of the activities of these EU companies (for instance, the foreign parent company has a central HR system and also processes the employee data of its EU group companies),

---

establishment of the controller is established in a Member State, see paras. 2.3 and 2.4.3.

61 This is confirmed by WP Opinion on applicable law (n 9), at 13: "The notion of "context of activities" does not imply that the applicable law is the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities relating to data processing."

62 Recital 18 of the Directive. This is also the position of the Working Party 29, see for instance Working Party 29, 'Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites' (WP 56, 30 May 2002), (**Working Document on Non-EU Based Websites**, at 6, fn 17. This is confirmed by the WP Opinion on applicable law (n 9), at 8.

the EU data protection laws will apply to those parts of the central processing which relate to the respective employees of the EU subsidiaries.

In its 2008 Opinion on Search Engines, the Working Party 29 gave some guidance when processing activities by a US search engine can be considered 'to be carried out in the context of the activities of its establishment in the EU':[63]/[64]

---

[63] Opinion on Search Engines (n 40), at 10.

[64] In its WP Opinion on applicable law (n 9), at 14, the Working Party 29 takes a functional approach to the concept of "in the context of the activities" and indicates that two elements have to be considered in order to decide whether data processing takes place in the context of the activities of an establishment: (i) the degree of involvement of the establishment in the activities and (ii) the nature of the activities of the establishment. See at 14: "The following considerations should be taken into account to conduct this analysis:
The degree of involvement of the establishment(s) in the activities in the context of which personal data are processed is crucial. Here the issue is to check "who is doing what", i.e. which activities are being carried out by which establishment, so as to be able to determine whether the establishment is relevant in order to trigger the application of national data protection law. Where an establishment is processing personal data in the context of its own activities, the applicable law will be the law of the Member State in which that establishment is located. Where the establishment processes personal data in the context of the activities of another establishment, the applicable law will be that of the Member State in which the other establishment is located.
The nature of the activities of the establishments is a secondary element, but it will help in identifying the law applicable to each establishment: the question whether an activity involves data processing or not, and which processing is taking place in the context of which activity largely depends on the nature of these activities. Alternatively, the fact that different establishments may be involved in totally different activities, in the context of which personal data are being processed, will have an impact on the law applicable."
See for the functional approach at 15: "A functional approach should be taken in the analysis of these criteria: more than the theoretical evaluation made by the parties about the law applicable, it is their practical behaviour and interaction which should be the determining factors: what is the true role of each establishment, and which activity is taking place in the context of which establishment? Attention should be paid to the degree of involvement of each establishment, in relation to the activities in the context of which personal data are processed. An understanding of the notion of "in the context of" is therefore also useful in complex cases to split different activities carried out by different EU establishments of the same company." See for the intention of the Working Party 29 to provide even further guidance on the concept of 'context of activities' at 32: "Some clarification would also be useful with regard to the notion of "context of activities" of the establishment. The Working Party has emphasised the need to assess the degree of involvement of the establishment(s) in the activities in the context of which personal data are processed, or in other words to check "who is doing what" in which

> 'However, a further requirement is that the processing operation is carried out "in the context of the activities" of the establishment. This means that the establishment should also play a relevant role in the particular processing operation. This is clearly the case, if:
>
> - an establishment is responsible for relations with users of the search engine in a particular jurisdiction;
> - a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state;
> - the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data.'

2.5 National implementations

The laws implementing the Data Protection Directive in the Member States are (more or less) based on the principle that the law of that Member State already applies if a foreign controller has an establishment in the relevant Member State.[65] Careful reading of them shows, however, many deviations concerning key concepts of Article 4(1)(a).

The German implementation[66] applies, for instance, also 'to a data controller not located in an EU Member State or in another EEA Contracting State that collects, processes, or uses personal data in Germany'. The UK implementation[67] applies to data processed by a data controller that is

---

establishment. This criterion is interpreted taking into account the preparatory works of the Directive and the objective set out at the time to keep a distributive approach of national laws applicable to the different establishments of the controller within the EU. The Working Party considers that Article 4(1)a as it stands now leads to a workable but sometimes complex solution, which seems to argue in favour of a more centralised and harmonised approach."

65 All texts of the laws referred to are unofficial English translations, to be found at <www.mofoprivacy.com>. That a different interpretation of Article 4(1)(a) leads to a very different interpretation of the various national implementation laws is shown by a recent research study commissioned by the Commission: Douwe Korff, New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (January 15, 2010). European Commission DG Justice, Freedom and Security Report, available at SSRN: http://ssrn.com/abstract=1638949, at 27 – 29.

66 Sec 1(5) of the Bundesdatengeschutzgezetz.

67 Sec 5(1) and (3) of the UK Data Protection Act 1998.

established in the United Kingdom and the data are processed in the context of that establishment. The law defines those established in the United Kingdom as 'any person who maintains in the United Kingdom an office, branch or agency through which he carries on any activity'. The Irish[68] and French[69] implementations are more or less similar to that of the UK.

The Dutch Data Protection Act implements the first sentence of Article 4(1)(a) and demonstrates the same ambiguity.[70] The legislative history of Article 4(1) of the Dutch Act, however, makes clear that the Dutch legislators followed the European legislators, and the Act already applies if an establishment of a controller is established in the Netherlands.[71] The Belgian and Portuguese laws are similar to the Dutch provision (and therefore require study of the legislative history to determine whether their legislators have followed the European legislators or not).[72] The Italian provision applies 'where a processing is performed by any entity established (...) in the State's territory' and thereby applies both to controllers and establishments of foreign controllers on its territory.[73] The Spanish implementation provision provides that Spanish law applies 'when the processing is carried out as part of the activities of an establishment pertaining to the data controller, whenever the establishment is in Spanish territory'.[74] This seems to imply that the controller itself can be established in another country. However, the provision provides that the law also applies if this subsection is not applicable, but the data processor is located in Spain.[75] This seems to imply that the first provision only applies if the controller itself is established on Spanish territory. Clearly deviating from all other implementation provisions are those of Sweden, Norway, and Finland,

68 Sec 3B sub (a) and (b) of the Irish Data Protection Acts 1988 and 2003.

69 Article 5(I)(1°) of Loi n° 78-17 du 6 janvier 1987 relative à l'information aux fichiers et aux libertés.

70 Article 4(1) Wet Bescherming Persoonsgegevens.

71 See n 29 for an overview of Dutch literature confirming this. See further n 30 for contrary opinions.

72 Article 3bis of Loi relative à la protection de la vie privée à l'egard des traitement de données à caractère personnel and Article 3 sub (a), (b) and (c) of the Lei 67/ 98 da Protecção de Dados Pessoais.

73 Section 5 sub (1) and (2) Codice in materia di protezione dei dati personali.

74 Article 3(1)(a) of the Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

75 Article 3(1)(a) of the Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

which provide that their implementation laws apply only if the data controller is established on their territory.[76] These provisions seem an incorrect implementation of the applicability rule of the Data Protection Directive. Apparently, however, these countries take a broad view of when a company may be considered to be 'established on their territory'. For instance in Finland, a company may already be considered established on its territory if a non-EU controller transmits advertising into Finland.[77] Also Finnish data protection law may therefore apply to a non-EU controller, an end result which is more similar to a correct implementation and application of Article 4(1)(a) than expected at face value of the Finnish implementation provision. Greek data protection law expands the scope of the Data Protection Directive's rule, by providing that Greek law also applies to data controllers outside the EU that process personal data of persons on Greek Territory,[78] and the data protection law of Denmark, which provides that Danish law applies to data processing carried out on behalf of a controller established in Denmark if the collection of data takes place for the purpose of processing in a third country.[79]

2.6 Working Party 29 Working Document on Non-EU Based Websites

It is also important to consider the Working Party 29 Working Document on Non-EU Based Websites,[80] which predates the Opinion on Search Engines and deviates substantially from it. The Working Document on Non-EU Based Websites has confused many DPAs and authors alike and some of its reasoning has found its way into other official documents of the European Commission.[81] The Opinion has also been quoted in a publication by the Dutch DPA in support of its interpretation that Article 4(1)(a) leads to the application of the law of one of the Member States only rather than to a cumulation of applicable laws.[82]

---

76 Section 4 of the Swedish Personal Data Act 1998 (Personuppgiftslag (1998:204); Section 4 of the Norwegian Personal Data Act (LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger); and Section 4 of the Finnish Personal Data Act (523/1999) (Henkilötietolaki 22.4.1999/523).

77 Kuner (n 29), at 84, mentions an unpublished case where McDonald's was found to be 'established' in Finland based on advertising that was transmitted into the country from abroad via cable television. This is not in conformity with the Directive.

78 See Article 3(3)(b) of the Greek Data Protection Act.

79 See Article 4(1) Danish Data Protection Act.

80 Opinion on Non-EU Based Websites (n 62).

81 Most notably the Commission's First Report on the Directive (n 35), at para. 4.4.1 and Korff (n 65) at 21 – 22 (dating after WP Opinion on Search Engines).

82 Fonteijn-Bijnsdorp (n 30), at 168.

The confusion starts where the Working Party 29 attempts to reconcile the possibility for the cumulative application of multiple laws under the Data Protection Directive with the country-of-origin principle. In short, according to the Working Party 29, the country-of-origin principle has been introduced into data protection legislation, so that if the controller is established in the territory of the EU, the law of the establishment of the controller applies. If the controller chooses to 'establish' itself in more than one Member State (i.e. has establishments in other Member States) it will have to comply with the law of all those (other) Member States in which it is 'established'. From this point of view the Data Protection Directive does not contain an exception to the country-of-origin principle, but merely constitutes a strict application of it. The explanation the Working Party 29 gives is, however, an incorrect interpretation of the country-of-origin principle as found in other EU Directives. Both the Television without Frontiers Directive and the E-Commerce Directive make clear that if a service provider has more than one place of business in the EU, such service provider is considered to be 'established' for purposes of application of the country-of-origin principle in the Member State where the provider of e-commerce services has its centre of activities or the media service provider is considered to have effective control. Application of the country-of-origin principle therefore results in no more than one place of establishment for the service involved, whereas with respect to data protection legislation each and every place of establishment (even if it is no more than a branch office) qualifies as place of establishment. An example for purposes of clarification is included below:

E-commerce Directive
A Dutch parent company provides a website for the online sale of products throughout the EU with its EU subsidiaries using the same system. The centre of activities regarding the provision of the online services is in the Netherlands. In line with the country-of-origin principle the website is governed solely by Dutch law.

Data Protection Directive
A Dutch parent company processes the company's employee data in a central HR system located in the Netherlands, with its EU subsidiaries using the same system. The centre of activities regarding the provision of services by the parent company is in the Netherlands. However, the law of the establishments (the EU group companies) governs that part of the central database that concerns the employee data of the relevant subsidiary. As a result, there are multiple applicable laws.

See the Working Document on Non-EU Based Websites for this creative turn regarding the application of the national data protection laws:[83]

> 'As the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of so-called "rule of conflict" and no recourse to other existing criteria of international private law is necessary.
>
> In order to find an answer, the Data Protection Directive uses the criterion or <connection factor> of the "*place of establishment of the controller*" or, in other words, the country of origin principle typically applied in the Internal Market. This means concretely:
>
> When the processing is carried out in the context of the activities of an establishment of the controller on the territory of one Member State, the protection law of this Member State applies to the processing.
>
> When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in the course of their activities. It is not an exception to the country of origin principle. It is merely its strict application: where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments.'

Another problematic aspect of the reasoning of the Working Party 29 is that the starting point that the controller 'has spread out over more than one establishment' appears to imply that each of the controller's establishments itself would be a controller (this would be in line with the country-of-origin principle). The point is, however, that these establishments very often do not qualify as a controller while the data processing takes place 'within the context of the activities of that establishment' (for a number of cases see Paragraph 2.9 below). The application principle of the Data Protection Directive (that the data processing must take place in the context of the activities of the establishment) results in the application of the law of the country of the establishment (and not therefore of the controller). This cannot be reconciled with the country-of-origin principle, which would lead to applicability of the law of the country of establishment of the controller.

---

[83] Working Document on Non-EU Based Websites (n 62), at 6.

2.7 Divergent opinions

Some commentators interpret Article 4(1)(a) as leading to the applicability of the law of the Member State where the controller is established.[84] Some quote in support of this interpretation the Explanatory Memorandum of the Commission[85] (see Paragraph 2.3.5 supra), where the Commission gives as the second rationale for the applicability rule of Article 4(1)(a) 'to avoid that one and the same data processing would be governed by the law of more than one country'. As noted above this Memorandum was published in respect of the Amended Proposal, therefore at the time the country-of-origin principle was still contained in the proposed Directive, a point these commentators appear to have overlooked.[86] It is also striking that the Dutch DPA in a recent publication (dating after the WP Opinion on Search Engines) still defends the position that Dutch data protection law only

---

84 See Lee A. Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation', to be found at <http://folk.uio.no/lee/oldpage/articles/Applicable_law.pdf>, at 8 (referring to the concept of establishment under the E-Commerce Directive and the Television without Frontiers Directive); Jeroen Terstegge's comment on article 4(1) Directive in Concise European IT law (Kluwer Law International 2004) at 39-41 (which is diametrically opposed to the interpretation of article 4(1) given in his earlier publication 'Home Country Control' (n 37) at 257-259); Bing, 'Data protection, jurisdiction and the choice of law', Privacy Law and Policy Reporter, [1999] 65, at 5-7 (referring to the concept of establishment under the E-Commerce Directive and the Television without Frontiers Directive); Fonteijn-Bijnsdorp (n 30), at 288; T. Hooghiemstra and S. Nouwt, *Tekst en Toelichting Wet Bescherming Persoonsgegevens* (Text and explanation Personal Data Protection Act) (SDU 2007), Explanation to Article 4, at 61: 'The key point of the Dutch Personal Data Protection Act is the place of establishment of the controller'; J.E.J. Prins and J.M.A. Berkvens, *Privacyregulering in theorie en praktijk* (Privacy regulation in theory and practice), (Series Recht en Praktijk, part 75) (Kluwer 2007) at 101: 'The consequence of the above is that, as to the question which body of law applies, the place of establishment of the controller of the processing is considered essential'; Korff (n 65) at 21 – 22.

85 Explanatory Memorandum (n 21), at 13.

86 See Bygrave (n 84), at 7-8. Bygrave gives as an explanation for the second rationale that at the time the Directive was drafted, it was the assumption and hope of the drafters of the Directive that the national privacy laws would be in harmony, as a result of which the applicability of more EU national laws would not be a problem, and only now is it apparent that the considerable margin that Member States have been given in implementing the Directive has lead to substantial disharmony. Despite this comment he however still takes as the main rule the application of the law of the Member State where the controller is established; Bing (n 84), at 9. Korff (n 65) at 21 – 22, this still referring to WP Opinion on Non-EU Based Websites, n 62, at 6, while at that time the WP Opinion on Search Engines was already issued.

applies if the controller is established in the Netherlands.[87] The main arguments of the Dutch DPA are discussed in the footnotes.[88]

2.8 Article 4(1)(c) Data Protection Directive

To fully understand the scope of applicability of the Data Protection Directive, knowledge of Article 4(1)(c) is required.[89] In short, this provision underlines the long arm approach of the Data Protection Directive[90] by providing that a national data protection law also applies in the event that the:

'controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community'.

The European legislators wished to ensure that even in the event that the controller has no establishment in the EU at all, EU data protection laws will nevertheless apply if the actual data processing takes place in a Member State by means of use of equipment. What is relevant here is that some DPAs[91] apply Article 4(1)(c) despite the controller having an establishment within the EU. They consider the branch or subsidiary to (also) qualify as 'equipment'. In its recent Opinion on Search Engines,[92] the Working Party 29 explicitly indicated that in those cases Article 4(1)(a) takes precedence over Article 4(1)(c).[93]

2.9 Cases

Because the above may be somewhat abstract, several cases will now be discussed involving an international situation (with a foreign controller and

87 Fonteijn-Bijnsdorp (n 30).

88 See n 46, n 84, n 25 and n 108.

89 See in detail Chapter 3.

90 See also Recital 20 of the Data Protection Directive.

91 In particular the French and Dutch DPAs. See Fontein-Bijnsdorp (n 30), at 291, note 28.

92 See Opinion on Search Engines (n 42), at 11: 'a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment. In such cases, the national law of the Member State in which the search engine is established applies.'

93 See in a different context also Kuner (n 29), at 122: 'a corporate subsidiary should not be considered to be 'equipment' of the non-EU company'. He considers this might be different if the subsidiary is a branch office only. The latter does not seem correct.

establishment in the EU), in order to clarify what may result from the above difference in interpretation of Articles 4(1)(a) and (c) of the Data Protection Directive. In some cases, the different interpretations lead to the same outcome via different routes. In other instances the outcomes are diametrically opposed. Each time I will apply the rule of Article 4(1)(a) as advocated in this article (**Opinion 1**) and then the deviating opinion as, for instance, advocated by the Dutch DPA (**Opinion 2**).

Case I: US parent with a branch in the Netherlands
A US parent company has a branch office in the Netherlands. The Dutch branch processes data of persons employed at the branch. Who is the controller, the US parent or the Dutch branch? As explained in Paragraph 2.4.1, the term 'controller' refers to the person who in a formal-legal sense controls the processing as a result of which those involved are aware of the legal persons against which they may exercise their rights. As the Dutch branch is not incorporated, it therefore cannot qualify as a controller. The US parent has control over the data processing in a formal-legal sense and therefore qualifies as the controller. Does Dutch data protection law apply?
Opinion 1
The processing of data of Dutch employees is carried out 'in the context of the activities of the Dutch establishment'. As the controller, the US parent must comply with the obligations laid down in Dutch data protection law.
Opinion 2
Dutch data protection law does not apply: Article 4(1)(a) Data Protection Directive does not apply because the controller (the US parent) is not established in the Netherlands. Article 4(1)(c) also does not apply because the US controller does have an establishment in the Netherlands (in Paragraph 2.8 we saw that this provision only applies if a controller outside the EU has no establishment in one of the Member States).

In order to fill this 'gap', some DPAs sometimes apply the fiction that the US parent is 'established' in the Netherlands as a controller because it has an establishment in the Netherlands.[94] Other creative solutions are that the branch itself is considered the controller and as this branch is established in the Netherlands, Dutch data protection law applies.[95] In Paragraph 2.4.1 we saw that this is not a correct interpretation. Some DPAs also just apply Article 4(1)(c), considering the branch 'equipment' in the Member State.[96] In Paragraph 2.8 we saw that this also is not a correct interpretation. These

94 In some Member States this fiction is even implemented in their data protection law (see for instance UK, Irish and French law, discussed in Paragraph 2.5).

95 See Fonteijn-Bijnsdorp (n 30), at 289.

96 See Fonteijn-Bijnsdorp (n 30), at 291 (footnote 28).

creative interpretations are unnecessary if the criterion of Article 4(1)(a) Data Protection Directive is applied in line with the Data Protection Directive.

Case II: the US central database

A US parent company has a subsidiary (a separate legal entity) in the Netherlands. The US parent has a central database located in the US that processes both employee and customer data of the Dutch subsidiary. The US parent processes more data than necessary for the purposes of the Dutch establishment and also determines the means used to process the data. The US parent qualifies as a joint controller in respect of the Dutch employee and customer data in the central system.

Opinion 1

The US parent processes the Dutch employee and customer data 'within the context of the activities of its Dutch establishment'. The Dutch data protection law applies to this part of the processing. Both controllers (the US parent and the Dutch establishment) must comply with the obligations under Dutch data protection law.[97]

Opinion 2

Dutch data protection law will also apply. The Dutch subsidiary is viewed as joint controller with regard to the Dutch employee and customer data processed in the central database. Because one of the joint controllers (the Dutch subsidiary) is established in the Netherlands, the Dutch subsidiary must comply with the obligations laid down in Dutch data protection law with respect to that part of the database which concerns the Dutch employees and customers.

The main difference here is that in the second opinion the US parent falls outside the ambit of Dutch data protection law. The creative interpretation possible in Case I (the US parent is 'established' in the Netherlands because it has a branch office in the Netherlands) does not work here because the subsidiary is a separate legal entity. If the interpretation in line with the Data Protection Directive is followed, the US parent would also be governed directly by Dutch data protection law. In view of the fact that the processing is undertaken by the US parent in the US (as a result of which the Dutch subsidiary does not have actual control over the processing), the first interpretation is to be preferred from an enforcement perspective.

---

97 This is confirmed by the Working Party 29 in its Opinion on applicable law (n 9), see example given at 15, as cited in n 45.

Case III: the US share option plan

A US parent company introduces a company-wide share option plan. Under this plan, the US parent grants share options to a very select group of employees of its worldwide subsidiaries, including its Dutch subsidiary. For this purpose the US parent processes certain assessment data of the employees and further the data necessary to grant (and later exercise) the share options. The controller for the processing is the US parent. The US parent determines the means and the purpose of the processing. The subsidiaries in question have no power of decision in the matter whatsoever. Their role is limited to providing certain data to the US parent.

Opinion 1

Insofar as the US parent processes data of Dutch employees in the context of the share option plan, these data are also 'processed in the context of the activities of the Dutch establishment', as the remuneration of the Dutch employees in respect of their work for the Dutch establishment is involved. Dutch data protection law is applicable to the processing of these employee data by the US parent (i.e., the US parent is directly subject to Dutch data protection law).

Opinion 2

Dutch Data Protection law is not applicable because the controller is not established in the Netherlands.[98] Because the controller does have an establishment in the Netherlands, Article 4(1)(c) is also not applicable. As a further consequence the transfer requirements do not apply. This result does not appear desirable from the perspective of the Data Protection Directive in terms of protection of individuals. Possibly DPAs will resolve this by using a broad definition of 'controller', by treating the Dutch subsidiary as a joint controller insofar as data of Dutch employees are processed in the context of this share option plan. This creative interpretation is unnecessary if an interpretation consistent with the Data Protection Directive is used. Furthermore, when an interpretation consistent with the Data Protection Directive is used, the US parent is directly subject to Dutch data protection law. If the interpretation of some DPAs is used, only the Dutch subsidiary is subject to Dutch data protection law. The first interpretation is therefore to be preferred from an enforcement perspective.

Case IV: US parent institutes worldwide whistleblower hotline

A US parent opens a call centre located in the US for employees of all its companies to file complaints. The US parent is obliged to do so under the US

[98] Fonteijn-Bijnsdorp (n 30), at 288. Incidentally, in the past the former Dutch Data Protection Commissioner (at present the EU Data Protection Supervisor) Mr Peter Hustinx, repeatedly indicated that the Dutch Personal Data Protection Act is certainly applicable to the processing of data of employees in the context of international share option plans.

Sarbanes-Oxley legislation. Is Dutch data protection law applicable to the personal data processed in the context of complaints by or about employees of its Dutch subsidiary? The US parent is the controller of this data processing (it determines the purpose and means of the processing).

Opinion 1

The whistleblower line also has an independent purpose for the Dutch establishment (the Dutch subsidiary independently benefits from the complaints procedure, such whistleblower facility being required under Dutch corporate governance requirements).[99] The data concerning complaints relating to the Dutch subsidiary are thus processed also in the context of the activities of the Dutch establishment. The US parent is directly subject to Dutch data protection law insofar as personal data of Dutch employees are processed.

Opinion 2

Dutch data protection law should not be applicable, since the controller is established outside of the Netherlands. Because the controller does have an establishment in the Netherlands, Article 4(1)(c) Data Protection Directive is also not applicable.[100] Dutch data protection law is therefore also not applicable to the transfer of the data by the Dutch employees to the US parent. Again, the DPAs may possibly resolve this by using a broad definition of controller by qualifying the Dutch subsidiary as a joint controller insofar as complaints are submitted by or about Dutch employees. In the case of a correct interpretation this is unnecessary and, moreover, the US parent company would be directly subject to Dutch data protection law, instead of (only) the Dutch establishment (which has no control over the processing whatsoever).

Case V: US call centre for product support

A US parent offers call centre services, offering customers of its worldwide subsidiaries an opportunity to submit questions about products brought onto the market by those subsidiaries. The Dutch establishment has access to the information of the US call centre, insofar as complaints by Dutch customers are involved. The information is necessary for the Dutch establishment for purposes of repairs or replacement of returned products. The US parent is the controller for the processing of the data that takes place in the context of the call centre (it determines the purpose and means).

Opinion 1

99 Dutch Corporate Governance Code, to be found at <http://www.commissiecorporategovernance.nl/Corporate_Governance_Code>.

100 The French DPA applies (the French equivalent of) Article 4(1)(c) in this context, with the argument that the telephones (the means) are located in France.

The data are processed by the US parent also in the context of the activities of the Dutch establishment (which is responsible for repairs and replacements). This involves support by telephone for the products that would otherwise have been provided by the Dutch establishment itself. Since the data are necessary for activities of the Dutch establishment, it must be concluded that the data are also processed in the context of the activities of this establishment. The US parent is directly subject to Dutch data protection law.

Opinion 2

Dutch data protection law will not apply to the processing of the data of Dutch customers because the controller is not established in the Netherlands. Because the controller does have an establishment in the Netherlands, Article 4(1)(c) Data Protection Directive is also not applicable. Again the DPAs may possibly resolve this by using a broad definition of controller or by qualifying the Dutch subsidiary as a joint controller insofar as support is requested by Dutch customers. In the case of interpretation in accordance with the Data Protection Directive, this is unnecessary and, moreover, the US parent company would be directly subject to Dutch data protection law.

A question that comes up is: what if the call centre data are not available in the Dutch establishment? Should the conclusion then be that these data are not processed 'also in the context of the Dutch establishment'?[101] The answer is: it depends. Possibly the handling of complaints has been organised in such a way that it is not necessary to provide the Dutch establishment with these data, whereas the complaints handling is still to such an extent linked to the products brought onto the market by the Dutch establishment that processing should indeed be deemed to take place in the context of the Dutch activities. According to the criteria formulated by the Working Party 29 in its Opinion on Search Engines, the answer could be 'yes', if the Dutch establishment was 'responsible for the relations with the Dutch customers' and was 'involved in the targeted advertisement for the relevant service in its jurisdiction'. This is without doubt a grey area. In my view, however, such processing should be seen as a separate activity. The support activity is then apparently an activity that can be performed by an independent third party.[102] In that case processing does not take place 'also in the context of the activities of the Dutch establishment.'

---

[101] In the affirmative Blok (n 29), at 299.

[102] An example of this is the maintenance of washing machines. There are enough parties in the market that offer maintenance for all brands. If such a third party processes data of Dutch customers with a Miele washing machine, this processing does not take place 'partly in the context of the activities of the Dutch Miele distributor'. The services in question are fully

2.10 The SWIFT Opinion

How does all of the foregoing relate to the SWIFT Opinion? In the SWIFT Opinion, the Working Party 29 concluded that the headquarters of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is established in Belgium and qualifies as the controller in respect of all processing activities of SWIFT in the EU (including the data processing in SWIFT's messages operating centre located in the Netherlands and its sales offices in various other Member States).[103] The Working Party 29 subsequently applied Belgian law to all processing activities on behalf of SWIFT anywhere in the EU, including data processing in the Dutch operating centre and in its sales offices in various other Member States. This amounts *de facto* to application of the country-of-origin principle (applying the law of the controller to also the data processing which takes place in the context of the activities of a branch in another Member State). Rumour has it that the Opinion was adopted on a far from unanimous basis.[104]

2.10.1 Background to the SWIFT Opinion

SWIFT supplies messaging services for financial transactions between financial institutions (processing more than 12 million messages on a daily basis). The information processed by SWIFT includes messages on the

---

independent. In my view the same should apply if another company belonging to the Miele group carries out this maintenance. I find support for this opinion in the WP Opinion on applicable law (n 9), at 15, where the Working Party 29 gives the following example: "A chain of "prêt à porter" shops has its head office in Spain, and shops all over the EU. The collection of data relating to clients takes place in every shop, but the data are transferred to the Spanish head office where some activities related to the processing of data take place (analysis of clients' profiles, service to customers, targeted advertising). Activities such as direct marketing of Europe-wide customers are directed exclusively by the head office in Spain. Such activities would qualify as taking place in the context of the activities of the Spanish establishment. Spanish law would therefore be applicable to these processing activities."

103 SWIFT Opinion (n 5).

104 See for the earlier opinion of the Belgium DPA: Advice No. 37/2007 of the Belgian DPA dated 27 September 2006, to be found at <www.privacycommission.be>. See for the position of the Dutch DPA for example: 'Verslag van het onderzoek naar gegevensverstrekking door banken aan de Amerikaanse autoriteiten', bijlage bij 'Onderzoek naar directe gegevensverstrekking aan de VS en antwoorden op kamervragen inzake SWIFT', nader rapport 27-06- 2007', to be found at <www.rijskoverheid.nl>. At the time the French DPA also issued an opinion: 'The Dossier SWIFT 'Affaire SWIFT: Que fait la CNIL?', this opinion is however no longer available on the website of the CNIL.

financial transactions of hundreds of thousands of EU citizens that contain without question their personal data. SWIFT is established in Belgium. SWIFT Belgium makes use of an operating centre in the Netherlands, where all data transmissions are processed. This operating centre is a branch office of SWIFT Belgium as are the various sales offices. The Working Party 29 considers SWIFT Belgium as the controller for the data processing by all branches because the critical decisions regarding this processing are taken by SWIFT Belgium. The Working Party 29 subsequently declared Belgian law applicable to all processing in the EU:[105]

> 'The head office of SWIFT is located in La Hulpe, Belgium. SWIFT also has two operating centers (one in Europe and one in the US, which is a complete mirror). In addition, SWIFT has several sales offices in the UK, France, Germany, Italy, Spain, etc. The critical decisions on the processing of personal data and transfer of data to the US were decided by the head office in Belgium. As a consequence, the processing of personal data by SWIFT is subject to Belgian law, implementing the Data Protection Directive, regardless of where the data processing takes place.'

The Working Party 29 does not assess in any way whether the processing of personal data by the Dutch operating centre takes place (also) in the context of the activities of (i) the sales offices or (ii) the operating centre itself. For instance the Dutch operating centre has as its only purpose the processing of the millions of messages, which constitutes the primary business activity of SWIFT. The Working Party 29 therefore in fact simply applies the country-of-origin principle here (the law of the controller is applicable). As explained above, this seems untenable as a starting position. The European legislators explicitly rejected introduction of the country-of-origin principle under EU data protection law.

---

[105] See SWIFT Opinion (n 5) at para. 2.2. See further para. 6.3: 'Actions regarding SWIFT: For all its data processing activities, SWIFT as a controller must take the necessary measures to comply with its obligations under Belgium data protection law implementing the Directive'. In para 2.3 the Working Party 29 further qualifies the financial institutions to be controllers in their own right insofar as 'their' message data is concerned. This entails also application of the laws of the financial institutions to their respective message data. See para 2.3: 'This means that, in the case of financial institutions, different – though harmonized – laws are applicable. The Working Party 29 stresses that, since personal data are being processed in financial transactions regarding hundreds of thousands of citizens via institutions established in the EU (the cooperative SWIFT as well as financial institutions making use of the SWIFTNet FIN services), the national laws on data protection – adopted in implementation of the Directive – of the different Member States concerned are applicable.'

2.10.2 The establishment acts as processor for a foreign controller

In the SWIFT case, the Dutch operating centre acted as a processor on behalf of the controller SWIFT Belgium. Some DPAs take the position that in the event an establishment on their territory acts as a processor for a controller in another Member State, the law of the controller applies to the processing ('processor follows controller'). Support for this view is found by some DPAs in the Technical Analysis attached to the European Commission's report on the Data Protection Directive:[106]

> 'None of the laws explicitly specify that they do not apply to processing on their territory if the processing takes place in the context of the activities of an establishment of a controller in another Member State, or to processing by a controller who has its main office on their territory but when processing takes place in the context of an establishment of that controller in another Member State.'

If this quote is read properly, I do not think that the Commission[107] intended to say that if an establishment acts as a processor for a controller in another Member State, the law of the controller is always exclusively applicable. The quote uses the concept of 'processing in the context of the activities of a controller in another Member State'. This cannot simply be considered equivalent to being a 'processor'. If the Commission had intended processors to be always subject to the law of the controller, it would simply have provided that if processing is carried out in the capacity as processor, the processing will be governed by the law of the state where the controller is established. The second sentence in the quote shows this unambiguously by allowing the explicit possibility that a controller in a Member State processes data in the context of an establishment of this controller in another Member State in which case the law of that establishment applies. It is therefore not invariably the law of the controller that is applicable. My conclusion is that the applicability of national data protection legislation does not follow the distinction controller / processor, but is subject to another test, namely whether data are (also) 'processed in the context of the activities of an establishment on the territory of a Member State' (in which case the data protection law of that Member State is applicable). As set out in Paragraph 2.4.4, the Working Party 29 gave some guidelines when data processing

[106] Technical Analysis (n 36), at 6. See Fonteijn-Bijnsdorp (n 30), at 289; Bygrave (n 84), at 7, indicates that the language of Article 4(1)(a) seems by contrast to imply that the law of a Member State does not apply to a processor established on its territory if the controller were established in another Member State.

[107] Note that the Technical Analysis is not drafted by the European Commission itself, see n 39.

should be considered to be 'processed in the context of the activities of an establishment'.[108] Specific guidance from the Working Party 29 on when processor activities should be considered to be performed in the context of the activities of the processor itself would obviously be helpful.

The above distinction becomes obsolete if one were to assume (apparently like the Working Party 29 in the SWIFT Opinion) that if a processing is performed by a processor, then it is always to be considered as having been performed exclusively in the context of the activities of the controller (thus sidelining the data protection law of the Member State of the processor). However, this position seems erroneous since it would lead to legal gaps being created in the protection of personal data, a result that the Working Party 29 presumably would not have welcomed had it given this more consideration (see Paragraphs 2.10.3 - 2.10.5 below). How these legal gaps are dealt with by a proper application of the provision of Article 4(1)(a) is discussed in Paragraph 2.10.6.

2.10.3 Undesirable result (1)

Application of the rule that a national data protection law is not applicable if the establishment processes data as a processor creates a lacuna in the protection of personal data if the controller is established outside the EU.[109]

---

[108] The Dutch DPA bases the rule 'processor follows controller' on Recital 18 of the Directive, especially the second sentence. This was however not the purpose of Recital 18 (see for citation Paragraph 2.3.6). As is the case with its predecessors (Recital 10 Original Proposal and Recital 12 Amended Proposal), Recital 18 expresses the first rationale for the Directive (avoiding potential circumvention of the protection) and not (as the Dutch DPA assumes) the second rationale (avoidance of cumulative application of laws). Also the second sentence of Recital 18 should be read in the context of avoiding circumvention of the protection (as evidenced by the introduction of this sentence 'whereas, in this connection'). The second sentence intends to express that the Directive cannot be circumvented by involving a processor outside the EU. The Recital makes clear that in that case the law of the Member State of the controller applies.

[109] The Working Party 29 in its Opinion on applicable law (n 9), at 13, confirms the rule "processor follows controller", but discusses only the example where the controller is established within the EU. In that case no gap in the protection is created. The Working Party 29, however, does not discuss how to solve the situation if the controller does not have establishments within the EU, in which case the gap will arise (as illustrated in this paragraph). It is sheer conjecture, but perhaps the Working Party 29 refrained form discussing the issue because, in its opinion, it proposes to introduce the country-of-origin principle, in which case the gap does not occur. I find support for this idea in the example discussed by the Working Party at 13 and 15, where a company has a number of sales offices in the EU. The parent processes the data centrally on behalf of these sales offices. The Working Party 29 considers that the customer data are

This is illustrated by the SWIFT case itself. If SWIFT were to move its Belgian headquarters to a country outside the EU, the controller would no longer be established within the EU and Belgium data protection law would no longer apply, nor to any other establishments of SWIFT in the EU (which apparently all qualify as data processors for the SWIFT headquarters). Also Article 4(1)(c) Data Protection Directive would not help; in Paragraph 2.8, I discussed why this provision only applies if the controller outside the EU has no establishment in one of the Member States. The Dutch processing centre of SWIFT, however, without doubt qualifies as an 'establishment' in the EU as a result of which Article 4(1)(c) Data Protection Directive does not apply.

The above gap in legal protection arises because the Working Party 29 (lacking an official country-of-origin principle that applies to the EU only) attempts to achieve the same result by attributing the processing by a processor to the controller of such processing. The result of this is that this rule also applies if the controller is established outside the EU, which cannot have been the intention of the EU legislators. In all other cases where the country-of-origin principle has been implemented, this only has effect within the EU. Providers established outside the EU cannot benefit from this rule, and will need to comply with the laws of all Member States involved.

2.10.4 Undesirable result (2)

The position of the Working Party 29 in the SWIFT Opinion leads to another gap in the protection of personal data: if a processor is never subject to its own law, the mandatory processor provisions of its own data protection law would not apply.[110] For compliance purposes it will then be required to solely rely on the mandatory processor agreements made between the controller and the processor.[111] If a controller outside the EU has a processor in the EU

---

processed in the context of the activities of the sales office and are governed by the law of the sales office. This outcome is similar to the solution I discuss in Paragraph 2.10.6 for the SWIFT case. See further n 119.

[110] Various EU data protection implementation laws contain mandatory processor obligations. Examples are the Irish Data Protection Act (see for instance Sections 2, 7 and 21); the Dutch Data Protection Act, under which processors are directly liable for any damages resulting from their processing activities (see Article 49(3); and the Greek Data Protection Act which applies to controllers and processors alike (see Article 3(3)).

[111] It is striking that for the processing provisions the European legislators have opted for the 'country of origin' principle. Pursuant to Article 17(3) Directive, the controller is to impose on the processor the security obligations of Article 17(1) of the Directive, as defined by the legislation of the Member State where the processor is established. This is to prevent a processor having to comply with the processor provisions of different Member States (which in

there would not even be an obligation to enter into such a mandatory processor agreement (e.g. if SWIFT were to move its headquarters outside the EU, its EU processing centre would therefore not be bound by any material processor obligations either). Though the DPA of the processor in theory would have formal enforcement powers,[112] there would be no material obligations to supervise. This gap does not arise if the interpretation advocated is followed.

2.10.5 Undesirable result (3)

With its interpretation the Working Party 29 apparently intends to avoid the cumulative application of the national data protection laws applicable to any processing.[113] However, application of the rule that a national data protection law is only applicable if the controller is established in the relevant Member State does not solve the problem of cumulative application of applicable rules at all. An example is provided in Paragraph 2.4.1, which deals with a central system operated by a parent on behalf of its subsidiaries (as a data processor for these subsidiaries). We saw that the data in these central systems will as a rule be processed also in the context of the activities of the parent's own establishment. If the parent company of such multinational is established in the EU, the data protection law of the EU country where the parent is established should apply to the processing at large (in addition to the laws of the subsidiaries for their relevant parts of the processing). In this case nothing is therefore achieved in practice by ruling that 'processors' follow 'controllers'.

However, even if one were to assume that a parent that operates the central HR system does so solely on behalf of its EU subsidiaries (i.e. as a processor), such central system is subject to a great many EU data protection laws (as many as there are EU subsidiaries). As each of the subsidiaries is the controller in respect of the processing of its own employee data, the various parts of the central HR system are consequently subject to

practice differ substantially) especially as regards to the required security measures. This is justified if the starting point is that the processor is indeed subject to the data processor requirements of its own law as supervised by its national DPA.

112 Pursuant to Article 28(6) Directive, the DPA of the processor has jurisdiction over data processing occurring on its territory 'whatever the national law applicable to the processing in question'. This is confirmed by the Working Party 29 in its Opinion on applicable law (n 9), at 10.

113 Fonteijn-Bijnsdorp, (n 30), at 288-289.

as many EU data protection laws.[114] As a result, each EU subsidiary, for example, has to notify the database (for its own part) to the DPA in its own country.

Multinationals therefore do not benefit in any way from the above interpretation by the Working Party 29. This explanation will at best entail that the Dutch parent (if it is considered a mere processor for its subsidiaries) does not have to notify the central database in its entirety in its own country, but only for the part that concerns its own employees. Simplification only occurs if the parent is to be considered as the sole controller for such central database and only needs to notify the database (in respect of the whole of the EU) in its country of establishment. This will only be achieved if the country-of-origin principle is introduced. This is by far preferable also from a supervisory perspective.[115] Article 28(6) of the Data Protection Directive provides that a DPA has supervisory jurisdiction over processing occurring on its respective territory, which applies irrespective of the national law applicable to the processing in question. The Data Protection Directive therefore contemplated that DPAs would under certain circumstances be required to apply foreign laws.[116] How is a DPA going to supervise a central system on its territory if such DPA will have to apply the data protection laws of a host of different Member States (which differ on numerous points) to the dispute in question?[117] In short: the Working Party 29 should not seek to effect the non-applicability of a national data protection law if a parent company processes data on behalf of its subsidiaries centrally. To the contrary, in these cases the DPAs benefit from the possibility of central supervision over this 'processor' while applying their own national law to the conflict.

Further thought has to be given to whether introduction of a country-of-origin principle should also apply to the rights of data subjects, or that data

---

[114] This example is discussed by the Working Party 29 in its Opinion on applicable law (n 9), at 15-16, The Working Party 29 comes to the same conclusion as to the applicability of the various laws of the Member States to the corresponding employee data. See for citations n 45.

[115] The Working Party 29 in its Opinion on applicable law (n 9), at 31, now also recommends introducing the country-of-origin principle: "The change envisaged in order to simplify the rules for determining applicable law would consist of a shift back to the country-of-origin principle: all establishments of a controller within the EU would then apply the same law regardless of the territory in which they are located. In this perspective, the location of the main establishment of the controller would be the first criterion to be applied. The fact that several establishments exist within the EU would not trigger a distributed application of national laws."

[116] This is confirmed by the Working Party 29 in its Opinion on applicable law (n 9), at 10.

[117] See also Kuner (n 29), at 112.

subjects would keep their rights under their national law. However, already under present legal rules, the rights of data subjects may in some cases be governed by the law of another Member State if the processing takes place in the context of activities of an establishment of a controller in another Member State. Full harmonisation of the rights of data subjects and cooperation between the DPAs in the event of complaints may be a better solution than excluding the rights of data subjects from applicability of the country-of-origin principle altogether.

2.10.6 SWIFT revisited

We just saw that if we follow the rule of the Working Party 29 (processor follows controller), and SWIFT were to relocate its Belgian headquarters to a country outside the EU, the controller would no longer be established within the EU and Belgian data protection law would no longer apply. This legal gap would not exist if the test advocated in this article is applied. If SWIFT's headquarters were in the US, the test would be: are the data (also) 'processed in the context of the activities of an establishment of SWIFT US on the territory of a Member State'. The Dutch processing centre as well as each of the sales offices qualifies as an establishment. Looking at the guidance provided by the Working Party 29 for criteria when processing activities by a non-EU controller can be considered to be carried out in the context of activities of establishments in the EU, the following criteria seem relevant:[118]

- The sales offices of SWIFT are responsible for relations with the customers of SWIFT (the financial institutions) in the relevant member States (with corresponding EU citizens as their end-customers).
- In most cases this will involve some local activities in the Member States (local sales people, local relationship management, local brochures about the services, etc).
- I assume that the Dutch processing centre actively complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to financial transaction data of EU citizens.
- The processing of financial transaction data is not a by-product, but a primary business process of SWIFT (i.e. the services of SWIFT are facilitating these transactions). The Dutch processing centre conducts therefore a primary

[118] I do not know the exact details of the activities of the SWIFT branches, so this is an educated guess.

business process which involves many employees. The processing of the data therefore takes place in the context of the activities of the Dutch branch.

The conclusion is that insofar as data are processed in the context of the activities of a sales office (data of the customers in certain Member states), the data protection law of the country of such sales office is applicable.[119] As the data are also processed in the context of the Dutch establishment, Dutch law also applies to the processing as a whole. This seems fully justified (even desirable) since the data processed concern financially sensitive data of millions of EU citizens.

2.11 Conclusion

At the moment there are a number of Member States that have not properly implemented the applicability rule of the Data Protection Directive. Also the Working Party 29 uses in the SWIFT Opinion an interpretation of the

[119] This is implicitly confirmed by the Working Party 29 in its Opinion on applicable law (n 9), at 13 and 15, where the Working Party 29 discusses two examples involving data collected in the context of a representative office and local shops. See at 13: "In the fourth scenario, the controller established in Austria opens a representation office in Italy, which organizes all the Italian contents of the website and handles Italian users' requests. The data processing activities carried out by the Italian office are conducted in the context of the Italian establishment, so that Italian law would apply to those activities. " And at 15: "A chain of "prêt à porter" shops has its head office in Spain, and shops all over the EU. The collection of data relating to clients takes place in every shop, but the data are transferred to the Spanish head office where some activities related to the processing of data take place (analysis of clients' profiles, service to customers, targeted advertising). Activities such as direct marketing of Europe-wide customers are directed exclusively by the head office in Spain. Such activities would qualify as taking place in the context of the activities of the Spanish establishment. Spanish law would therefore be applicable to these processing activities. However, the individual shops remain responsible for the aspects of the processing of their customers' personal data which take place in the context of the shops' activities (for example, the collection of customers' personal information). To the extent that processing is carried out in the context of each shop's activities, such processing is subject to the law of the country where the shop in question is established." See also example discussed at 17: "For the commercial offices based in other Member States, if their activity is limited to general non-user-targeted advertising campaigns which do not involve the processing of users' personal data, they are not subject to EU data protection laws. However, if they decide to conduct a processing in the context of their activities involving the personal data of individuals in the country where they are established (such as sending targeted advertisements to users and possible future users for their own business purposes), they will have to comply with the local data protection legislation."

applicability rule which seems contrary to the legislative history of the Data Protection Directive. This interpretation does not solve the problem of cumulative application of national EU data protection laws but rather creates gaps in the protection of personal data. A proper implementation and interpretation of the applicability rule does not give rise to these problems. Further, although the attempt of some DPAs and the Working Party 29 to prevent the cumulative application of legislation is commendable, this result will only be achieved if the country-of-origin principle is introduced. This should be done by the European legislators and not via the short-cut of opinions of the Working Party 29. For the question of how EU regulators can best ensure full harmonisation in respect of the applicability regime of the Data Protection Directive, I refer to Paragraph 10.6.5, where I propose replacing the Data Protection Directive by an EU regulation[120] in the upcoming revision of the Directive, or, as a next best alternative, to confer the implementing powers in respect of a revised Directive to the European Commission.[121] As EU regulations are directly applicable in the Member States and do not require implementation into national law, the chance of disparities between the national laws of the Member States will be eliminated. If there is one uniform EU data protection law, the country-of-origin principle will become superfluous. For completeness sake I note that so far as **jurisdiction** of the DPAs is concerned, the country-of-origin rule will remain relevant, which I will further discuss in Paragraph 4.10.1. As it is uncertain which legislative instrument will be chosen by EU regulators, my recommendations are based on the assumption that the Directive will not be replaced by an EU regulation. Again, if the Directive is replaced by an EU regulation, these will no longer be relevant.

Recommendation 1
Ensure an adequate harmonisation of the applicability regime of the Data Protection Directive.

Recommendation 2
Introduce the country-of-origin principle.

[120] Article 288 TFEU defines a regulation as follows: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States." Whereas "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."

[121] Which the European legislators are empowered to do pursuant to Article 291(1) of the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**).

3 Does EU data protection law apply to non-EU websites?

3.1 Introduction

With the maturing of the internet, EU citizens increasingly visit EU and non-EU websites alike. Most websites track the 'click stream data' (the surfing behaviour) of their visitors to make an inventory of their interests and requirements. Based on this information websites tailor the content of their websites to the individual likings of their visitors and present them with targeted advertising. Click stream data is collected by means of various techniques like 'cookies' or the online use of JavaScript, ad banners and spyware.[1] The use of these techniques has led to an unprecedented processing of EU personal data outside the EU. This form of behavioural marketing obviously leads to concerns about the protection of privacy of EU citizens[2] and a wish to extend the protection afforded by the Data Protection Directive also to such foreign processing of EU originating data. It is clear that the Data Protection Directive[3] dates from the time the internet was not yet widely used. The applicability regime of the Data Protection Directive was not devised with the vast increase in cross-border flows of personal data in mind which came with the maturing of the internet. Though the Data Protection Directive has a 'long arm' reach, the connecting factor for applying the Data Protection Directive is based on the territoriality principle and limited to situations where foreign controllers use processing 'equipment' located within the EU. As non-EU websites do not use such processing 'equipment' in the EU, the Data Protection Directive does not seem to apply to the processing of data by foreign websites. Despite this, the Working Party 29 took the position that EU data protection laws also apply if non-EU websites process personal data of EU citizens if these data are collected by means of 'cookies' or the use of JavaScript, ad banners and spyware. As almost all websites use one or more of these tools, this results in the potential applicability of the Data Protection Directive to websites worldwide. Though fully understandable or even commendable from a protection point of view, this expansive interpretation seems contrary to the legislative history of the Data Protection Directive and further leads to the application of EU data protection law whenever the data of an EU citizen are

---

1 See for definitions paras. 3.7.3 and 3.8.2.

2 European Commissioner Reding has warned in a speech that the European Commission would not shy away from taking action if behavioural targeting interfered with European citizens' privacy rights, see <www.ec.europa.eu>.

3 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31 (**Data Protection Directive**).

processed. Most commentators consider this an unacceptable form of 'regulatory overreaching'[4] as there is no prospect of enforcing EU data protection laws on such scale. Also governments and business groups have complained about this unwarranted extraterritorial effect of EU data protection law.[5] In any event the lack of guidance in the Data Protection Directive on the key concept of what constitutes 'equipment' has confused many national legislators and led to an unacceptable variation in national implementation provisions.[6] As a consequence, the national Data Protection Authorities are largely left to their own devices as to when to apply their data protection law, and in practice do so in a divergent manner.[7] The Data Protection Directive thus fails to meet its broader legal purpose to work as a single market measure.[8] In its first evaluation of the Data Protection Directive in 2003,[9] the European Commission recognised the lack of clarity

4 See in detail para. 3.7.3, in particular n 64.

5 Christopher Kuner, Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1) (October 1, 2010), International Journal of Law and Information Technology, Vol. 18, p. 176, 2010. Available at SSRN: http://ssrn.com/abstract=1496847, at 3, referring to Patrick Ross, 'Congress fears European privacy standards' CNET News (8 March 2001), <http://news.cnet.com/2100-1023-253826.html>, quoting the chairman of the Commerce Committee of the US House of Representatives as stating that the EU Data Protection Directive 95/46 is 'an effort to impose the EU's will on the US'. See also Jack Goldsmith and Tim Wu, Who controls the Internet? (Oxford University Press 2008) 175, referring to the 'aggressive jurisdictional scope' of the EU Data Protection Directive; and the Comments of the US Council for International Business (USCIB) for the Review of the EU Data Protection Directive (30 July 2002), <http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/paper/uscib_en.pdf>, stating 'Many businesses find the Article 29 Committee's assertion as to the jurisdictional reach of the Directive on the Internet to be unwarranted and contrary to international law and jurisprudence.'

6 See for a comprehensive overview of the differences Korff, 'EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws', Cambridge, September 2002, (Study Contract ETD/2001/B5-3001/A/49).

7 See Korff for examples and further para. 3.9 below and n 40.

8 The legal basis for the Data Protection Directive is Article 95 (formerly 100a) of the Consolidated Version of the Treaty establishing the European Community, [2002] OJ C325 (**EC Treaty**); see further Recitals 1-9 of the Data Protection Directive. The EC Treaty has been replaced by the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**). Article 95 EC Treaty is now Article 114 TFEU.

9 See Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final, at 17 (**First Report on the Directive**). Similarly, a study sponsored by the European Commission highlights the ambiguity and divergent implementation of the applicable law rules in the Directive and recommends that "better, clearer and unambiguous rules are desperately needed on applicable

of Article 4 of the Data Protection Directive, but announced that it would first take as its priority to ensure correct implementation of Article 4 of the Data Protection Directive in all Member States, before considering amendments. In December 2009, the Working Party 29 also acknowledged the problem of the lack of clarity of Article 4 and the many different interpretations of it, and announced that it would issue a further opinion on the concept of applicable law, including recommendations for revisions for the future legal framework. This was in response to the revision of the Data Protection Directive launched by the Commission on 1 July 2009.[10] The Commission seems to have moved on as well and announced in November 2010[11] that it will indeed revise and clarify the applicability rule. In this Chapter an attempt is made to provide a uniform interpretation of the applicability rule based on the legislative history of the Data Protection Directive and proposals are made for an amended applicability rule. In December 2010, the Working Party 29 issued its further WP Opinion on applicable law.[12] The publications on which Chapters 2 and 3 of this dissertation are based were available to the Working Party 29 when drafting its opinion. I have inserted additional footnotes in red to reflect the position of the Working Party 29 on the respective issues, which in many instances deviates from earlier its opinions.

3.2 The applicability regime of the Data Protection Directive

The key provision for the applicability of the EU data protection laws to non-EU websites is Article 4(1)(c) of the Data Protection Directive. To understand the scope of this provision knowledge is also required of Article 4(1)(a) of the Directive which contains the main default rule of the

---

law". See "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments", January 2010, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

10 See Working Party 29, 'The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168, 1 December 2009), at para. 26 – 28 (**WP Contribution on The Future of Privacy**).

11 See European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union', COM(2010) 609/3 (4 November 2010), at para. 2.2.1. and 2.2.3 (**EC Communication on revision of the Directive**).

12 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836/10/EN WP (**WP Opinion on applicable law**).

applicability regime.[13] Both provisions (a) and (c) are based on the 'territoriality principle' (whereby the connecting factor is the location of the actors) rather than the protection principle (whereby the connecting factor is the location of the persons to be protected, which places the emphasis on the actions of an actor). This is explained in more detail below.

3.2.1 Article 4(1)(a) Data Protection Directive

According to Article 4(1)(a) the Data Protection Directive applies 'to the processing of personal data in the context of the activities of an establishment of the controller on the territory of the Member State'.

The territoriality principle here has a more or less 'virtual nature'. The formal place of establishment of the controller is not relevant for the applicability of the Data Protection Directive.[14] The Directive is already applicable if the data processing is carried out in the context of the activities of an establishment of a controller which is located on Community territory. The controller of the data itself may be established outside of the EU.

Article 4(1)(a) Data Protection Directive further applies regardless of where the actual processing takes place. The EU data protection laws apply when the data processing takes place 'in the context of the activities' of an establishment. The provision does not state that the data processing must be carried out by the establishment in a Member State. On the contrary, the European legislators meant to abstract from the location where the data processing takes place. If location were to be decisive, this would easily facilitate bypassing the national data protection laws, for instance by relocating the servers to another jurisdiction.[15] It is therefore possible that the data processing takes place in the context of the activities of an establishment in a Member State, but that the data processing itself is carried out by a third party outside this Member State (whether in another EU Member State or outside the EU). This underlines the long arm reach of the Data Protection Directive.

In today's context this has become a matter of course. Many multinational companies now process data centrally. For instance, a foreign parent company often processes data from its EU group companies for central

---

13 See on Article 4(1)(a) Data protection Directive in detail Chapter 2.

14 See para. 2.3.6.

15 See Recital 18 of the Data Protection Directive. This is also the position of the Working Party 29, see for instance Working Document on non-EU Based Websites (Chapter 2, n 62), at fn 17. This is confirmed by the WP Opinion on applicable law (n 12), at 8.

management purposes. If that processing also takes place in the context of the activities of these EU group companies (for instance, the foreign parent company operates a central HR system both for its own central management purposes, but also for HR purposes of the EU group companies), the EU data protection laws will apply to those parts of the central processing which relate to the respective employees of the EU subsidiaries.[16] This applies also if the relevant parent company outsources the central processing to a third party outside the EU.

Despite abstracting from the location of the data controller and the location of the data processing, the territoriality principle is in fact adhered to by Article 4(1)(a) as the data processing is virtually connected to the territory of the EU (i.e. takes place in the context of the activities of the establishment in the Member State). That Article 4(1)(a) is based on the territoriality principle rather than the protection principle is further reflected by the fact that the nationality of the persons whose data are processed is of no relevance. The Data Protection Directive may well apply to data of non-EU nationals if these are processed in the context of the activities of an establishment in an EU Member State.[17]

3.2.2 Commentary by Dammann and Simitis

That the European legislators indeed had the above in mind when drafting the Directive is confirmed by the leading commentary on the Data Protection Directive of Dammann and Simitis (unofficial translation into English):

> 'The Directive adopts the place of establishment of a controller as the decisive connecting factor. With the implementation of the Directive, each member state has to extend this to all processing that takes place in the context of the activities of an establishment on its territory (1 sub a first sentence). Only on the surface of things did the Directive thus adopt a "personal" connecting factor to the detriment of the originally favoured territoriality principle, whereby the location of the processing or the place where the data are located was decisive. The directive does not take into account the "person involved" (his domicile or

[16] This is confirmed by the Working Party 29 in its Opinion on applicable law (n 12), at 15. See in more detail para. 2.4, in particular n 45.

[17] The Data Protection Directive makes no reference or distinction based on nationality of the data subject. See Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997) at 127-28; Working Party 29, 'Working Document on Non-EU Based Websites' (Chapter 2, n 62), at 7. This is confirmed by the WP Opinion on applicable law (n 12), at 8.

> nationality), but the controller of the processing and then not the place of establishment of the parent company of the controller, but the place of establishment of an establishment of the controller in the context of which the processing activities take place. The directive herewith creates a decentralisation which to a large extent results in the territoriality principle, i.e. decisive is the place of the processing. As a rule this has as a result that also the persons involved can rely for maintaining their own rights on their own well-known law.'[18]

3.2.3 Applicability of Article 4(1)(a) to non-EU websites

In the case of data processing by a non-EU website, it is possible that Article 4(1)(a) leads to applicability of the Data Protection Directive. This would be the case if, for instance, a US company with an establishment in an EU Member State operates a website that processes data of visitors from the relevant EU Member State. If the processing by the US company can be considered 'to be carried out in the context of the activities of the establishment', the data protection law of the relevant EU Member State will apply. In its 2008 Opinion on Search Engines,[19] the Working Party 29 gave some guidance when processing activities by (in that case) a US search engine can be considered 'to be carried out in the context of the activities of an establishment in the EU':

> 'However, a further requirement is that the processing operation is carried out "in the context of the activities" of the establishment. This means that the establishment should also play a relevant role in the particular processing operation. This is clearly the case, if:
>
> - an establishment is responsible for relations with users of the search engine in a particular jurisdiction;
> - a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state;
> - the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data.'

Obviously, similar factors will apply if a US company with an establishment in the EU (instead of a search engine) operates a website which processes

---

[18] Dammann and Simitis (n 17), at 127 -128.

[19] See Working Party 29, 'Opinion 1/2008 on data protection issues related to search engines' (WP 148, 4 April 2008), at 10 (**WP Opinion on Search Engines)**.

data of visitors from the EU. Such processing of data will be considered to be carried out (also) in the context of this EU establishment if:

- the establishment is responsible for relations with the users in the relevant EU country (if for instance the website sells products or services and the establishment is involved in delivery and (after) sales services);
- the website is promoted by the establishment by means of locally targeted advertisements to the inhabitants of that state.

If the relevant establishment has no involvement with the relevant customers in respect of the delivery and (after) sales services, Article 4(1)(a) will not apply.

3.3 Article 4(1)(c) of the Data Protection Directive

Article 4(1)(c) Data Protection Directive complements the main rule of Article 4(1)(a).[20] It underlines the long arm approach of the Data Protection Directive[21] where it provides that EU data protection laws also apply in the event the:

> 'controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said member state, unless such equipment is used only for purposes of transit through the territory of the Community'.

By connecting the applicable law to the location of the equipment used for the processing the Data Protection Directive still applies the territoriality principle (see further Paragraph 3.3.3 below).

In order to ensure that the data subjects can effectively exercise their data protection rights against such non-EU controller, Article 4(2) Data Protection Directive subsequently provides that a non-EU controller that uses equipment on Community territory must designate a representative established on the territory of the relevant Member State.

For the interpretation of Article 4(1)(c) the legislative history of this provision is relevant.

---

[20] Article 4(1)(b) requires that Member States also apply the Directive to their territories outside the territory of the EU if those are subject to their national laws by virtue of international public law. This part of Article 4 of the Directive will not be addressed in detail here.

[21] See also Recital 20 of the Data Protection Directive.

3.3.1 The legislative history of Article 4(1)(c)

The Data Protection Directive had two draft versions:

- the Original Proposal;[22] and
- the Amended Proposal,[23] published together with an Explanatory Memorandum of the European Commission.[24]

The final text of the Data Protection Directive was adopted in 1995.

The provision of Article 4(1)(c) Data Protection Directive was not included in the Original Proposal. In the Original Proposal the connecting factor for choosing the applicable national law was the 'location of the data file'.[25] In order to avoid circumvention of the applicability of the EU data protection laws, the Original Proposal further provided that 'a transfer of a data file by a controller in the EU to a non-member country was not to prevent protection of the EU privacy laws'. No provision was, however, made for a possible circumvention of the EU data protection laws if the controller itself were to relocate outside the EU (i.e. had no establishment within the EU). When this gap in protection was detected, the Amended Proposal added the text of Article 4(1)(c) to the main default rule[26] as a second ground for applicability of the Data Protection Directive and a corresponding Recital:

---

22 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314 – 2, 1990/0287/COD (**Original Proposal**).

23 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (92/C 311/04), [1992] OJ C/1992/311/30) (**Amended Proposal**).

24 See COM (92) 422 final – SYN 287, 15 October 1992, at 13 (**Explanatory Memorandum**). This Explanatory Memorandum is not available on the site of the European Commission. The following is based on the Dutch version.

25 Article 4(1) Original proposal:

'1. Each Member State shall apply this Directive to:
(a) all files located in its territory;
(b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.'

26 The main default rule then still deviated from the final Directive. The full text of Article 4(1) Amended Proposal was:

'1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:
(i) of which the controller is established in its territory or is within its jurisdiction;

> "Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice"

This provision (and related Recital 20) remained unchanged in the final Data Protection Directive.

This with the exception that the word 'means' in the English version of the Amended Proposal was replaced by the word 'equipment' in Article 4(1)(c) of the final Directive (note that the word 'means' was also used in Recital 20 of the English version of the final Directive but remained unchanged).

The Explanatory Memorandum[27] of the Amended Proposal confirms that the main purpose of the European Commission for the Amended Proposal was (unofficial translation from Dutch):

> 'to avoid the possibility that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this'.

This rationale is expressed in Recital 12 (second sentence):

> 'Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out by a person who is established in a Member State should be governed by the law of that State; whereas, the fact that processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas, in that case, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice'.

> (ii) of which the controller is not established in the territory of the Community, where for the purpose of processing personal data he makes use of means, whether or not automatic, which are located in the territory of that Member State.'

27 See the Explanatory Memorandum (n 24), at 13 for the rationale for amendment of Article 4(1).

3.3.2 'Equipment' versus 'means'

The last minute change of 'means' in the English version of the Amended Proposal to 'equipment' in the final Directive must have been made with a particular purpose in mind (otherwise, why change it?). A possible explanation could be that the term 'equipment' would appear to have a narrower meaning than 'means', namely suggesting a physical apparatus rather than 'any possible means'.[28] Except in the Italian and Swedish versions, this change was not, however, implemented in the other language versions of the final Data Protection Directive. In these language versions (still) the word is used which would translate into 'means' in English rather than 'equipment'.[29] As a consequence most national implementation laws use a term that would be a translation of 'means', which has resulted in a very wide interpretation indeed by the relevant EU DPAs (see Paragraph 3.9.1 below).

For interpretation purposes the question is which of the language versions takes precedence (if any).The European Court of Justice (**ECJ**) has ruled that all language versions of a directive are equally authentic and that interpretation of European law requires comparison of all language versions.[30] Though in certain cases the ECJ gave precedence to the wording used in the majority of the language versions of a directive or a specific language version,[31] it appears that the Court places more emphasis on systematic interpretation of the instrument in question together with its

---

[28] See Korff (n 6), at 48, who indicates that most examples given are the use of a telephone to collect data, the sending of paper forms to data subjects in the EU, etc.

[29] The French version, for example, uses 'moyens', the Spanish 'medios', in Italian the term 'mezzi' is used and in Portuguese 'meios'. The Dutch version uses 'middelen'. Only Ireland, Sweden, Denmark and the United Kingdom use the term 'equipment' or a comparable term.

[30] 'To begin with, it must be borne in mind that Community legislation is drafted in several languages and that the different language versions are all equally authentic. An interpretation of a provision of Community law thus involves a comparison of the different language versions.', Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415.

[31] Case C-64/95 *Konservenfabrik Lubella Friedrich Büker GmbH & Co. KG v Hauptzollamt Cottbuss* [1996] ECR, I-05105. In this case, most language versions of Commission Regulation 1932/93 establishing protective measures regarding the import of sour cherries referred to 'sour cherries', whereas the German version of this regulation mistakenly referred to 'sweet cherries'. However, the Court has also held in another case that under certain circumstances a single language version can be given preference to the majority of language versions, Case 76/77, *Auditeur du travail v Bernard Dufour, SA Creyf's Interim and SA Creyf's Industrial* [1977] ECR 02485.

aims and purposes than in accordance with specific language versions of the Directive:

> '[E]very provision of Community law must be placed in its context and interpreted in the light of the Community provisions as a whole, regard being given to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied.'[32]

Given the fact that the word 'equipment' is used in the English, Italian and Swedish language versions only, the above rules of interpretation make it unlikely that the (arguably narrower) word 'equipment' will prevail.[33] More likely is that both terms 'equipment' and 'means' will be interpreted by the ECJ in accordance with the purpose and meaning of the Data Protection Directive as discussed above. See Paragraph 3.4.2 for a detailed discussion of 'equipment' and 'means'.

3.3.3 Commentary by Dammann and Simitis

Also Dammann and Simitis emphasise that Article 4 (1)(c) in particular intends to prevent a controller that has its activities within the EU from circumventing the protection afforded by the Data Protection Directive by relocating its place of establishment outside the EU.[34] They further confirm that by connecting the applicable law to the location of the equipment used for the processing the Data Protection Directive explicitly falls back on the territoriality principle.[35]
Here follows an unofficial translation into English of the relevant part of the commentary):[36]

---

32 Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415, para 20.

33 Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415, para 20. The Working Party 29 in its WP Opinion on applicable law (n 12), 20, also interprets the word "equipment" as "means": "It has to be noted that there is a difference between the word used in the English version of Article 4 (1) c 'equipment', and the word used in other language versions of Article 4 (1) c, which are more akin to the English word 'means'. The terminology used in other language versions of Article 4 (1) c is also consistent with the wording of Article 2 (d) defining the controller: the person who decides about the purposes and the "means" of the processing. In view of these considerations, the Working Party understands the word "equipment" as "means". It also notes that according to the Directive this could be "automated or otherwise"."

34 Dammann and Simitis (n 17), at 129.

35 Dammann and Simitis (n 17), at 129.

36 Dammann and Simitis (n 17), at 129.

> 'Pursuant to paragraph 1c the Directive requires from the Member States that under certain circumstances they apply their national provisions also to the activities of a controller that is established outside the Community territory, i.e. in a third party state, or on the high seas or otherwise outside the territory of a sovereign state. With this provision the Directive aims to avoid in particular, that controllers that conduct their activities within the Community territory, can abscond from the harmonised data privacy laws by moving their corporate seat. The Directive requires the application of national laws in those cases in which the (external) controller, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the relevant Member State. Thus, the Directive reverts to the principle of territoriality.'

Based on the legislative history, the rationale for applicability of Article 4(1)(c) seems to be:

(i) the territoriality requirement:
the controller must have its business activities on the Community territory (albeit not by means of an establishment) and collect data in the context thereof;

(ii) the circumvention element[37]:
Article 4(1)(c) applies only if the Data Protection Directive would have been applicable were it not that the controller does not have an establishment within the EU.

3.4 Review of key concepts in Article 4(1)(c)

Given the complexity of the key concepts of the provision of Article 4(1)(c), each of these concepts is reviewed below. If elements of these concepts require further guidance from the Working Party 29, this is specified.

---

37 Re the purpose of Article 4(1)(c) see also Christopher Kuner, '*European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press 2007), at 119: 'It is useful to recall the purpose that Article 4(1)(c) is designed to play in the framework of the General Directive. The disposition of Article 4.1.c aim at covering situations in which data subjects are deprived, by an artificial manoeuvre, of the protection afforded by the Directive and situations which fall outside the scope of any protection whatsoever, even that considering transborder data flows....A German pharmaceutical company which establishes itself in Budapest and which collects data relating to medical prescriptions from a pharmaceutical network located within a Member State, in order to target European health professionals, is evidently trying to circumvent the provisions of the Directive and Article 4.1.c should apply. Article 4 (1)(c) is thus a protective provision designed to prevent evasion by data controllers of their legal responsibilities through relocation of their establishments outside the EU, while using technical means located in the EU to process data in a way that would activate their legal obligations if they were established in the EU.'

3.4.1 Controller is not 'established' on community territory

The notion of 'established' is extensively discussed in Paragraph 2.4.2. In short, an establishment is considered to be 'the effective and real exercise of activity through stable arrangements', whereby 'the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect'. Specifically in respect of websites the Working Party 29 states that[38]:

> 'the notion of establishment of a company providing services via an Internet web site is not the place, at which the technology supporting its web site is located or the place at which its website is accessible, but the place where it pursues its activity. Examples are: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London'.

Protection gap

When applying the applicability rules of Article 4(1)(a) and 4(1)(c) a gap in protection is created.[39] The cause of this gap is that the concepts used in these provisions are insufficiently aligned. Article 4(1)(c) provides for applicability of the Directive in situations where the controller is *not* established within the EU. However, Article 4(1)(a) does not apply in the reverse situation (that the controller is established within the EU) but applies only if the processing 'is carried out *in the context of the activities* of an establishment of the controller.' Mere establishment within the EU is not sufficient; the processing of the data should be in the context of the activities of the relevant EU establishment. Therefore in theory a controller established outside EU territory and using equipment on EU territory could avoid EU data protection laws by creating an establishment within the EU. If, for example, the processing takes place only in the context of the activities of the controller in the US (and not of the establishment in the EU), the Directive does not apply on the grounds of Article 4 (1)(a). If the US controller subsequently makes use of equipment on EU territory, the Directive would not apply either, since the controller does have an establishment on EU territory. This outcome is clearly contradictory to the intention of the drafters to avoid the evasion of the Directive's regime. Some

[38] Working Document on Non-EU Based Websites (Chapter 2, n 62), at 70.

[39] See also Blok (n 29), at 297-304 and 301-302.

DPAs[40] apply Article 4(1)(c) despite the fact that the controller does have an establishment within the EU. They consider the branch or subsidiary to (also) qualify as 'equipment'. In its recent Opinion on Search Engines,[41] the Working Party 29 explicitly indicated that Article 4(1)(a) applies to the detriment of Article 4(1)(c) in case a controller does have an establishment in the context of which the data is processed.[42] Based on the purpose of the Directive (to avoid circumvention), there are strong arguments that in case the processing cannot be considered to be carried out in the context of an establishment (in which case Article 4(1)(a) does not apply) such establishment may also be discarded for the application of Article 4(1)(c) which will then apply if use is made of 'equipment' in the EU (independently of the relevant subsidiary).[43] If my proposals for amendment of Article 4

---

40 In particular the French and the Dutch DPAs. See Fonteijn-Bijnsdorp, 'Art. 4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', 6/2008 Computerrecht at 285-289.

41 See Working Party 29, 'Opinion 1/2008 on data protection issues related to search engines' (n 19), at 11: 'a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment. In such cases, the national law of the Member State in which the search engine is established applies.'

42 See in a different context also Kuner (n 37), at 122, who indicates that 'a corporate subsidiary should not be considered to be 'equipment' of the non-EU company'. He considers this might be different if the subsidiary is a branch office only. The latter does not seem correct.

43 Independently as in case the equipment is operated by the establishment the likely conclusion will be that the relevant processing will (also) be carried out in the context of the activities of the relevant establishment. This interpretation is confirmed by the Working Party 29 in its Opinion on applicable law (n 12), at 19: "On the other hand, Article 4(1)c will apply where the controller has an "irrelevant" establishment in the EU. That is to say, the controller has establishments in the EU but their activities are unrelated to the processing of personal data. Such establishments would not trigger the application of Article 4(1)a. This means that, since there should be no lacunae or inconsistency in the application of the provisions of the Directive, the application of the "equipment" criterion need not be prevented by an irrelevant establishment: it could be prevented by the existence of an establishment only to the extent that this establishment processed personal data in the context of the same activities. A corollary of this interpretation is that a company with diverse activities could trigger the application of both Articles 4(1)a and 4(1)c if it used equipment and had establishments in different contexts. In other words, a controller established outside the EU/EEA and using equipment in the EU would have to comply with Article 4(1)c even if it had an establishment in the EU, as long as this establishment processed personal data in the context of other activities. This establishment would trigger the application of Article 4(1)a for these specific activities." At 20, the Working Party 29 proposes to clarify the interpretation given: "For this reason the Working Party considers that Article 4(1)c should apply in those cases where there is no establishment in the EU/EEA which would trigger

Data Protection Directive are followed (see Paragraph 3.12), the gap in protection will no longer present itself.

3.4.2 Equipment

The legislative history of the Directive provides little guidance for the concept of equipment. From the Explanatory Memorandum[44] that gives as examples 'terminals, questionnaires, etc' it can be derived that the drafters of the Directive had physical objects in mind (both automated and non-automated) which the data controller could locate in a Member State and use to collect data of EU citizens.[45] Dammann and Simitis give a comprehensive summary of the thinking at the time where they give two examples[46] where a controller does not have an establishment in the EU but still is active on EU territory and processes data of EU citizens. The first is where the controller uses automated equipment to process for instance orders for goods within the EU which (by means of telecommunications equipment) are subsequently dealt with from outside the EU without such controller having an establishment within the EU. The second is where the data controller conducts business within the EU by means of travelling salesmen and collects data by means of questionnaires[47] etc:

---

the application of Article 4(1)a or where the processing is not carried out in the context of the activities of such an establishment."

44 Explanatory Memorandum (n 24), at 14.

45 See Kuner (n 37), at 120, where he concludes that the use of the term 'equipment' betrays the origins of the Data Protection Directive in the pre-internet area', at which time 'the concept' 'was generally thought to refer to a computer, telecommunications network, or **other** physical object which the data controller could locate in a Member State and then operate remotely from an establishment outside the Community. What evidently was not contemplated at the time of drafting was the existence of a ubiquitous, seamless information network (i.e. the internet) which, owing to its decentralised nature, would routinely allow EU citizens to transfer back and forth to millions of computers throughout the world.'

46 Dammann and Simitis (n 17), at 129-130. Note that the examples given in the Explanatory Memorandum (terminals and questionnaires) are also used in the examples given by Dammann and Simitis.

47 The Working Party 29 in its WP Opinion on applicable law (n 12), at 20, gives a similar interpretation of the term "equipment" which it understands as "means" (see citation in n 33) and gives a broad interpretation: "In view of these considerations, the Working Party understands the word "equipment" as "means". It also notes that according to the Directive this could be "automated or otherwise". This leads to a broad interpretation of the criterion, which thus includes human and/or technical intermediaries, such as in surveys or inquiries. As a

> 'Automated equipment in terms of the Directive is for example an EDP-system which is physically located within the territory of a Member State, through which EDP-system information services are provided or through which EDP-system orders for goods can be received electronically and which EDP-system is not administered through an establishment in the relevant Member State, but through control and maintenance by means of telecommunication from outside the Community territory. If such system is merely electronically accessible via a telecommunication network in a Member State, whereas it is physically maintained in a third party State, the Directive does not apply. In such case, it is not the controller but the user that makes use of automated equipment located within the Community territory.
>
> The Directive also requires the application of national law in case the controller established in a third party State makes use of 'non-automated' equipment situated in the relevant Member State. This applies for example when travellers instructed by the controller collect data in the context of sales or market research and process this in the form of collections of questionnaires or indexes, without the justification of an establishment. If the controller, established in the third party state, communicates with the traveller within the Community territory by means of mail or telephone, it cannot be established that he makes use of non-automated equipment.

3.4.3 Equipment situated on the territory of a Member State

From the above quote from Dammann and Simitis it is clear that the drafters of the Directive had the physical location of physical objects on EU territory in mind.[48]

3.4.4 Making use of equipment

According to Dammann and Simitis, a controller can further only 'make use of' equipment when the equipment is within the actual control of the controller.[49] In this very capability to exercise control lies the legitimisation

---

consequence, it applies to the collection of information using questionnaires, which is the case, for instance, in some pharmaceutical trials."

48 This is also the interpretation of the Working Party 29, see citation n 47. Kuner (n 37), at 123, comments (in respect of the question whether software can constitute equipment) that: 'it stretches credulity to describe a series of electrical impulses downloaded over the internet to a computer in the EU as 'situated' within such country'.

49 Kuner (n 37), at 121 (with reference to Dammann and Simitis) comments: 'In fact 'make use' here should be interpreted in the sense of 'determines', i.e., the data controller must control how the equipment is used to process data, so that the English term 'makes use' is a misnomer. It is

of submitting the non-EU data controller to the law of an EU Member State. What is normative here is the controller's ability to control the manner in which the processing takes place, not the ownership of the equipment:[50]

> 'One can only say that the controller 'makes use of equipment (...)', if he is in actual control of this equipment. This provides the legitimation to subject him to the laws of a Member State. Decisive here for is the control over the manner of processing personal data, whereas the private law ownership and the bearing of costs are not decisive.'

3.4.5 For purposes of transit only

If the equipment located on the territory of an EU Member State is used 'only for purposes of transit through the territory of the Community', the use by a controller outside the EU of this equipment will not lead to applicability of EU law. As this is an exception to the equipment criterion it should be subject to a narrow interpretation.[51] Dammann and Simitis comment that in the event of 'naked transit through Community territory' the Data Protection Directive assumes that the rights and freedoms of EU citizens are not 'affected' in a particular manner.[52]

---

true that 'it is not necessary that the controller exercise full control over the equipment. The necessary degree of disposal is given if the controller, by determining how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing.'

50 Kuner (n 37), at 121.

51 See also the Working Party 29 in its WP Opinion on applicable law (n 12), at 23. Examples listed by the Working Party 29 are: "telecommunication networks (cables) or postal services which only ensure that communications transit through the Union in order to reach third countries." The Working Party 29 at 23, further notes that application of this exception becomes increasingly infrequent: "It should be noted that the effective application of this exception is becoming infrequent: in practice, more and more telecommunication services merge pure transit and added value services, including for instance spam filtering or other manipulation of data at the occasion of their transmission. The simple "point to point" cable transmission is disappearing gradually. This should also be kept in mind when reflecting on the revision of the data protection framework."

52 Dammann and Simitis (n 17), at 130. The Working Party 29 in its WP Opinion on applicable law (n 12), at 20, confirmed this interpretation (referring to its earlier Working Document on Non-EU Based Websites' (Chapter 2, n 62): "The Working Party has already clarified that the concept of "making use" presupposes two elements: some kind of activity of the controller and the clear intention of the controller to process personal data. Therefore, whilst not any use of equipment within the EU/EEA leads to the application of the Directive, it is not necessary for

3.5 Summary rationale Article 4(1)(c)

Based on the legislative history the requirements for applicability of Article 4(1)(c) may be summarised as follows:

(i) the territoriality requirement: the controller must have its business activities on the Community territory (albeit not by means of an establishment) and collect data in the context thereof;
(ii) the circumvention element: Article 4(1)(c) applies only if the Data Protection Directive would have been applicable were it not that the controller does not have an establishment within the EU;
(iii) equipment must be physical objects physically located on EU territory;
(iv) in order to 'make use' of equipment the equipment must be 'under the control of the controller (he should be able to decide the manner of processing, ownership is not relevant);
(v) the laws do not apply if equipment is used for transit purposes only.

Whether Article 4(1)(c) applies in any given case should be decided based on these requirements.

3.6 Outsourcing to EU processor

An example of potential applicability of Article 4(1)(c) that was totally unforeseen by the drafters of the Data Protection Directive is the case where for instance a US based company (without establishments and activities in the EU) outsources its IT to an EU outsourcing supplier (or locates its processing activities in the EU). As a consequence, US data will be stored and processed on servers located in the EU (the servers qualifying as 'equipment') whereby such data processing cannot be considered merely for transit purposes. This occurs more and more often as companies implement 'follow the sun' arrangements ensuring around the clock ICT or helpdesk support for the whole company at the lowest cost (i.e. by making use of regular working hours of locations around the world). As a consequence, EU data protection law is applicable while the data processed concern (in this case) US data only, which fall within the EU scope because these data are exported to the EU and transferred back again to the US.[53] Many DPAs have

---

the controller to exercise ownership or full control over such equipment for the processing to fall within the scope of the Directive."

53 The Working Party 29 confirmed in its Opinion on applicable law (n 12), that in cases where a non-EU controller uses a processor in the EU this constitutes the "use of equipment" in the EU as a result of which the Data Protection Directive applies, including the data transfer rules. See

indicated that insofar as the relevant data are indeed coming from outside the EU and are transferred back again, enforcement of the EU data transfer rules 'will not be their priority'.[54]/[55] Applying the above requirements would not lead to applicability of Article 4(1)(c), since the controller (i) does not have business activities on EU territory; (ii) the data are not processed in the context of these business activities; and (iii) there is no circumvention of Article 4(1)(a) by using technical means located in the EU rather than having these performed by an establishment within the EU. Article 4(1)(c) should

---

at 20: "There is a question whether outsourcing activities, notably by processors, carried out in the EU/EEA territory on behalf of controllers established outside EEA may be considered as "equipment". The broad interpretation advocated above leads to a positive answer." See further at 25: "Another practical consequence of the application of Article 4(1)c concerns the interaction between this provision and Articles 25 and 26 of the Directive. The fact that the controller established outside the EU/EEA uses equipment on EU/EEA territory – and must therefore comply with all relevant provisions of the Directive - would also entail the possible application of Articles 25 and 26."

54 Korff (n 6), at 50, quotes the UK Information Commissioner's Office (the UK DPA): 'It is hard to see the justification for applying the Directive to situations where a data controller is not established in any Member State but nevertheless uses equipment in a Member State for processing. If, for example, a business in the US collects personal information on US citizens in the US but processes the personal data on a server in the UK it is subject to the requirements of the Directive. This extra-territorial application of the law makes little sense, is very difficult if not impossible to enforce and is a disincentive for businesses to locate their processing operations in the EU. If a collection of personal data is controlled and used in a non-EU jurisdiction regulation should be a matter for that jurisdiction regardless of where the data are actually processed. Furthermore the Directive requires that a data controller outside the EU appoints a representative in the Member State where processing takes place. What is the purpose of this? There is no apparent basis on which the Commissioner could take action against a representative for a breach of UK law by a data controller established outside the EU.' Also the CNIL publicly announced that it will not enforce in these cases. See publication at the website of the CNIL "CNIL facilitates the use of outsourcing services performed in France on behalf of non-European companies", dated 15 March 2011, to be found at http://www.cnil.fr/english/news-and-events/news/article/cnil-facilitates-the-use-of-outsourcing-services-performed-in-france-on-behalf-of-non-european-compa/.

55 This result is also not satisfactory in the opinion of the Working Party. See WP Opinion on applicable law (n 12), at 21: "However, as mentioned, it also highlights some consequences which are not satisfactory, when the result is that European data protection law is applicable in cases where there is a limited connection with the EU (e.g. a controller established outside the EU, processing data of non-EU residents, only using equipment in the EU)."; and at 24, where the Working Party 29 again discusses the example where a non-EU controller processing non-EU data involves a processor in the EU and concludes that Article 4(1)(c) applies, but that "[t]his may have undesirable consequences in terms of economic impact and enforceability"

therefore not apply. In case my proposals for amendment of Article 4 Data Protection Directive are followed (see Paragraph 3.12), it will be made explicit that Article 4(1)(c) does indeed not apply when a non-EU controller involves an EU processor (or performs its processing activities in the EU).

I note that this interpretation of Article 4(1)(c) has in its turn as a consequence that the data security requirements under EU data protection law will also not apply to such EU data processing activities and further has an inherent risk that the EU will be used as a digital haven[56] as there will be no legal basis under EU data protection law to act against these data processing activities in EU territory, even if the relevant data processing would be considered unethical to EU standards. Data protection being a fundamental right under EU law, this is an unacceptable situation. However, rather than applying the full scope of the Directive, it seems sufficient that in these cases the data processing (i) meets the EU data security provisions (as inadequate security in EU territory may expose the EU to cybercrime); and (ii) provides for an "adequate level of data protection" (which enables DPAs to enforce in case of blatant violations of the "material data processing principles"[57]). See for my text proposal in this respect Paragraph 3.12.

3.7 Application of Article 4(1)(c) to data collection by non-EU websites

Hereafter follows an assessment on whether the telecommunications and other equipment involved with data collection by foreign websites constitutes the 'making use of equipment situated on EU territory'. There are many types of 'equipment' involved with collecting the data of users

[56] The latter risk is also highlighted by the Working Party 29 in its Opinion on applicable law (n 12), see conclusion at 31-32: "The criterion of the equipment/means: this criterion has shown to have undesirable consequences, such as a possible universal application of EU law. Nonetheless, there is a need to prevent situations where a legal gap would allow the EU being used as a data haven, for instance when a processing activity entails inadmissible ethical issues. The equipment/means criterion could therefore be kept, in a fundamental rights perspective, and in a residual form. It would then only apply as a third possibility, where the other two do not: it would address borderline cases (data about non EU data subjects, controllers having no link with EU) where there is a relevant infrastructure in the EU, connected with the processing of information. In this latter case, it might be an option to foresee that only certain data protection principles – such as legitimacy or security measures – would apply. This approach, which obviously would be subject to further development and refinement, would probably solve most of the problems in the current Article 4(1)c."

[57] See for a discussion of the material data processing principles para. 7.1.1 and for the requirement of an adequate level of protection para. 7.1.3.

when visiting a website. Next to the user's computer (see Paragraph 3.7.1) and (the hard- and software of) the underlying web server of the website, the entire physical connection between the user's computer and the website is involved in this collection of data (including the equipment of the access provider of both the user and the website) (see Paragraph 3.7.2). In many cases the content of web pages is further provided by websites or web servers of third parties and this 'content' may also play a part in the data collection. Websites may further make use of tools like cookies, JavaScript code, banners and spyware to collect data. From the Working Document on Non-EU Based Websites, it may be deduced that the use of these tools may also constitute the use of equipment (see Paragraph 3.8).

3.7.1 Personal computers

Users visit a website by making use of a personal computer or a hand-held device (like a smart phone or tablet). From a technical perspective a website visit works as follows: when a user types a website address of the internet browser operated on his computer (or hand-held device) and presses return, the browser sends a request to the website's server for the page in question. The server, in turn, sends the requested webpage to the user's computer . The webpage is subsequently executed by the web browser. Most websites are written up in the language 'Hypertext Markup Language' (HTML), the 'regular' language in which web pages are written. HTML has the possibility to request information from the user, such as name and contact details, which can be sent to the web server operating the website. A standard visit to a website can therefore involve the processing of the user's personal data (without the use of cookies or JavaScript, see Paragraph 3.7.3 below).

It is clear that the internet browser and the personal computer of the user play a role in the visit to the website. The question is whether this constitutes 'use' by the website 'of equipment situated within the EU' when collecting the data. Applying the rationale of Article 4(1)(c) the answer should be: no. The personal computer of a user is under the control of the user rather than of the website. The website therefore does not actively 'make use of this equipment' to collect data.[58]

[58] See also Kuner (n 37), at 120-121: 'While the type of device (a computer) would qualify as 'equipment' within the meaning of the term as the drafters of the General Directive seemed to have conceived of it (i.e., as a physical object which processes the personal data of a data subject), it is also necessary under Article 4(1)(c) that the data controller outside the EU 'make use' of the equipment (in this case, the data subject's computer) in order for Member State law to be applicable. In cases where an internet user in the EU is accessing a foreign website, it is

3.7.2 Communications network

Both users and websites require access to the internet via an internet service provider who deploys a host of equipment to provide the physical connection between the user's computer and the website. For the same reasons as set out above in respect of the personal computers of users, the use of telecommunications equipment will not constitute 'the making use of equipment'. It is not the website but rather the user who makes use of the telecommunications network to access the website and in any event the telecommunications network is not under the control of the website. Any other interpretation would amount to Article 4(1)(c) always being applicable as in all cases telecommunication lines are required for accessing a website.[59]

See along the same lines (in respect of communications equipment for transmission of e-mails) Recital 47 of the Data Protection Directive:

> 'Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.'

---

the user, rather than the website, which should be considered the data controller. Moreover, even if the data controller is deemed to be located outside the EU, the mere fact that a data subject located in the EU communicates with a data controller outside it by means of a computer (for example, sends the controller an e-mail, etc) cannot under normal circumstance result in the data controller 'making use' of the data subject's own computer.'

59 See also Kuner (n 37), at 121-122: '[I]t is actually not the *foreign website* making use of a network in Europe, but the *European user* who does so, since it is the user who connects to the network in order to access the website, and the non-EU data controller has no control over the connection: thus, in such a case, the user, and not the network operator, should be deemed to be the data controller. More fundamentally, deeming a network to be 'equipment' would be tantamount too making the entire internet subject to EU law, which would be an absurd result. This means that EU data protection law does not apply to foreign websites merely because of the fact that they can be accessed by European users.'

3.7.3 Cookies

A cookie is a small piece of text[60] (data) that is placed by a website on a user's computer. Cookies can be used for purposes of session management (to facilitate a particular website visit, i.e. by tracking a shopping cart during the website visit), to facilitate future visits to the website (e.g. by remembering a login name or website setting (language or other preferences) or gather information on a user's surfing activity (tracking users). Cookies may contain all kinds of data, but next to expiration date,[61] a domain name[62] and a path,[63] it usually only contains an identification code by which the website can recognise the user and his session when the website is visited again from the same personal computer. Normally the relevant personal data, such as (past) content of shopping carts, login details or preferences are stored on the web server (on which the website is operated). Not only is this more secure, but the information which can be stored in cookies is rather limited. Without cookies, each retrieval of a (component of a) web page would be an isolated event. Cookies are (by now) an intrinsic part of almost all websites.

From a technical perspective, cookies operate as follows. When a user types the address of a website in the internet browser operated on his computer (or a handheld device) and presses return, the browser sends a request to the website's server for the page in question. At the same time, the browser will search the user's computer for the cookie that the relevant website has placed on the user's computer. If a cookie is found, the browser will send the information contained in the cookie to the website's server. The information is then used by the website's server. If no cookie is present, the server sends the requested webpage (and perhaps a cookie) to the computer of the user. The webpage is executed by the web browser.

Web browsers offer users the possibility to change the cookie settings. This can be used by users to disable cookies. Some web browsers (e.g., Internet

---

60 Cookies are not executable and are neither software, spyware or viruses, although they can be used to track users. Cookies merely consist of data and allow for the exchange of information between a user's computer and the website that placed the cookie.

61 The expiration date tells the browser when to delete the cookie. By specifying an expiration date cookies are not deleted at the end of session and can be used in a next browser session. Such a cookie is called a persistent cookie. A session cookie is deleted at the end of a surfing session when the user closes the browser.

62 The domain tells the browser to which domain the cookie should be sent. If nothing is specified, it defaults to the domain of the object requested.

63 The path enables the developer to specify a directory on the web server where the cookie is active.

Explorer) also offer the possibility to make a distinction between first- and third-party cookies**.** See for an example:

(From: http://www.helpwithpcs.com/tipsandtricks/internet-explorer/disable-cookies-1.gif.)

As cookies may in practice take many forms (varying from just containing the elementary information whereby the data itself is collected on the web server and cookies that itself collect data), I will discuss the most elementary version as a starting point.

Case II: Cookies from non-EU websites

A US company without establishments in the EU operates a website providing product information (but not selling products and services). The US website is not supported by local advertisements within the EU or other sales (promotion) activities within the EU. The website uses cookies to collect data from its visitors to tailor its site and banners to the preferences of the visitors. The cookie contains the elementary information of expiration date, domain name, path and identification code only, and does not collect personal data (the personal data are collected on the web server in the US).

If the website is visited by EU citizens and data are collected relating to these visitors from the EU does Article 4(1)(c) apply to this processing of data?

Applying the requirements for application of Article 4(1)(c) to this use of cookies the answer should be: no, as:

1. **the territoriality principle is not adhered to**:
   a. the relevant US company operating the website has no concrete business activities on EU territory (does not undertake active local advertising, has no local sales people to solicit business, etc);
   b. the EU visitors access the relevant website on their own initiative without local prompting, i.e. the EU citizen is not visited or contacted by whatever means within its own territory but rather itself actively seeks access to a foreign website 'outside' its own territory;
   c. the US company does not make use of 'equipment' physically situated within the EU to collect data. The cookies are used for identification purposes rather than data collection itself (which takes place within the US). The placing of the cookies did not require further actual activities of the US company within the EU.
2. **there is no circumvention aspect**:
   the Data Protection Directive would not have been applicable were it not for the fact that the US company does not have an establishment in the EU. Even if the US company were to have had an establishment within the EU, the Data Protection Directive would not apply as the data processing cannot be considered to take place in the context of the activities of such establishment (there being no sales (promotion) activities within the EU, see Paragraph 3.2.3 on the applicability of Article 4(1)(a) to non-EU websites).
3. **there is no making use of equipment as there is no control**:
   the website owner does not have control over the cookies. The website owner can try to place them, but the user can prevent this by means of his browser settings and the user can disenable cookies at any time thereafter (see Paragraph 3.7.3 above).
4. **there is no physical equipment that is physically situated on EU territory**:
   cookies concern merely text and cannot qualify as a physical object. The cookies cannot qualify as equipment used for processing as the cookies are used for identification purposes rather than data collection itself (which takes place within the US).
5. **transit purposes only**: as cookies do not qualify as equipment (see sub 1 – 4 above), this exception is not relevant.

Again, as users use a personal computer for visiting websites and websites use cookies to facilitate use of websites, applying Article 4(1)(c) to any and all data processing of EU nationals whenever cookies are used would amount to applying the protection principle (relevant factor is the action: the Directive applies to the processing of data of EU users) rather than the territoriality principle (i.e. relevant factor is the actor, i.e. the location of the equipment used), which was not the choice made by the legislators.

This is also the prevailing opinion in the legal commentary.[64]

---

[64] See Kuner (n 37), at 125: 'The view that cookies constitute 'equipment' would also in effect result in the location of the data subject (rather than the place of establishment of the data controller) always determining the applicable law, which is clearly not the principle underlying Article 4 of the General Directive'; Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet', 32 International Lawyer 991 (1998), at 1011, argues that there is no real basis for interpreting the scope of Article 4 (1)(c) to have such a wide reach (as to apply to cookies). First, if it were intended to expand EU jurisdiction law to such an extent, this would have taken place through a 'publicized or negotiated effort' in stead of a provision in a specialised Directive. Second, the expansion of jurisdiction to websites around the world by means of a Directive drafted in the early 1990's, before there was any real conception of the Internet and how to regulate it, does not appear to make much sense. Finally, the broad expansion of jurisdiction under the Directive raises 'traditional concerns about notice, fairness, comity and national sovereignty.' According to Kobrin, 'The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance', Working Paper Series, The Wharton School (November 2002), at 23, such an expansive interpretation of 4(1)(c) leads to a situation which he describes as 'hyper-regulation', whereby extraterritorial reach becomes the norm rather than the exception'. See along the same lines Blok (Chapter 2, (n 29), at 301 and Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation', [2000] Computer Law and Security Report 252 at 255. See also Terwangne & Louveaux, 'Data protection and online networks', 13 Computer Law & Security Report 239 (1997) who (in a publication of 1997 therefore dating well before the Article 29 Working Document on Non-EU Based Websites) consider that collection of data by a non-EU website through the use of cookies does not fall within the scope of Article 4(1)(c). They however are of the opinion that this results in a lack of protection of EU nationals and propose to extend the applicability of Article 4(1)(c) to situations where no use is made of equipment (i.e. in case cookies are used). Christopher Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2) (October 1, 2010), International Journal of Law and Information Technology, Vol. 18, 2010. Available at SSRN: http://ssrn.com/abstract=1689495, at 14, qualifies the extensive application of Article 4(1)(c) as: "this can be characterized as a kind of 'regulatory overreaching' (…) The applicability of law to conduct, or the adjudication of a dispute by a court or regulator, is not a purely theoretical matter, but must have a reasonable chance of enforcement in order to have meaning" (referring to H.L.A. Hart, The Concept of Law (Oxford University Press 2nd edition 1997), at

3.8 The Working Party 29's position on cookies

The position of the Working Party 29 is diametrically opposed to the above findings. In its Working Document on Non-EU Based websites,[65] the Working Party 29 takes the position that Article 4(1)(c) does apply to data collected by means of cookies by a US website.[66] The Working Party 29 considers the placing of cookies on personal computers located within the EU as 'the making use of equipment' within the EU:

> 'As explained above, the user's PC can be viewed as equipment in the sense of Article 4(1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and [...] several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.
>
> The Working Party is therefore of the opinion that the national law of the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk'.

116, stating that one of the minimum conditions necessary for the existence of a legal system is that 'those rules of behaviour which are valid according to the system's ultimate criteria of validity must be generally obeyed...'; Hans Kelsen, General Theory of Law and State (Transaction Publishers 2005), 42, stating: 'A norm is considered to be valid only on the condition that it belongs to a system of norms, to an order which, on the whole, is efficacious'. See also Jack Goldsmith, 'Unilateral Regulation of the Internet: A Modest Defence' (2000) 11 European Journal of International Law 135, 139, stating 'the true scope and power of a nation's regulation is measured by its enforcement jurisdiction, not its prescriptive jurisdiction'".

65 Article 29 Working Party, 'Working Document on Non-EU Based Websites' (Chapter 2, n 62), at 11.

66 This remains the opinion of the Working Party 29. See WP Opinion on applicable law (n 12), at 21, where the Working Party 29 in general terms (referring to its Working Document on Non-EU Based Websites, at 10): states: "A case-by-case assessment is needed whereby the way in which the equipment is actually used to collect and process personal data is assessed. On the basis of this reasoning, the Working Party recognized the possibility that personal data collection through the computers of users, as for example in the case of cookies or Javascript banners, trigger the application of Article 4(1)c and thus of EU data protection law to service providers established in third countries".

The Working Party 29 took a similar position in its earlier Working Document on Privacy on the Internet,[67] though there it did not explicitly designate the computer as the equipment. Rather, the cookie itself was designated as 'means' through which data were collected:

> 'While the interpretation of the notion of 'equipment' or 'means' has given rise to debate about their extent, some examples undoubtedly fall within the scope of application of Article 4.
>
> This will be the case, for example, for a text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country. Such text files, named cookies, are used to collect data for a third party. If the computer is situated in an EU country and the third party is located outside the EU, the latter shall apply the principles of the national legislation of that Member State to the collection of data via the means of the cookie.'[68]

As a consequence, the Working Party 29 requires that users are informed of the use of cookies when visiting a website:

> '[T]he user should be informed when a cookie is intended to be received stored or sent by Internet Software. The message given to the user should specify, in clear terms, which information is intended to be stored in the cookie and for what purpose as well as the period of validity of the cookie. The user should then be given the option to accept or reject the sending or storage of a cookie as a whole and they should be given options to determine which pieces of information should be kept or removed from a cookie depending on, for example, the period of validity of the cookie, or the sending and receiving web sites.'[69]

3.8.1 Review of the Working Party 29's underlying reasoning on cookies

The underlying reasoning of the Working Party 29 merits a detailed discussion in order to decide whether its position on cookies is convincing or not. The short conclusion of this analysis is that the Working Party 29 acknowledges that Article 4(1)(c) is based on the territoriality principle but subsequently makes a creative turn by interpreting the territoriality

---

67 Article 29 Working Party, 'Working Document Privacy on the Internet, An integrated approach to on-line Data Protection', (WP 37, 21 November 2000), at 28.

68 Working Document Privacy on the Internet, An integrated approach to on-line Data Protection' (n 67), at 28.

69 Working Document on Non-EU Based Websites (Chapter 2, n 62), at 11.

principle in accordance with the protection principle (i.e. by concluding that the territoriality principle 'reflects a true concern to protect individuals on [their] own territory). This results *de facto* in the Working Party 29 applying the protection principle which is contrary to the (legislative history of) the Data Protection Directive.

The Working Party 29 starts its Working Document with a broad introduction to the question of application of the EU data protection laws to the processing of personal data by websites that are based outside the EU. It starts by indicating that this is a 'general question of international law which arises in on-line and off-line situations where one or more elements are present that concern more than one country'. According to the Working Party 29:

> 'these decisions involve a consideration of a number of factors. First and foremost, the concern of a given State is to protect the rights and interests of its citizens, residents, industry and other constituencies recognised under national law.'[70]

This seems to be a reference to the *lex protectionis*, whereby the laws apply of the location of the data subject (i.e. of its residence or nationality). The Working Party 29 then continues with a list of examples[71] where community law is applied on an extra-territorial basis and concludes that in these examples of Community law 'similar criteria are applied'. 'Whether it is a requirement that the relationships have a 'community dimension' or 'close connection' with the Community, in certain situations the European Court of Justice, the European Parliament and Council as well as the European Commission see fit to impose EU rules on non EU based entities'. In all examples given by the Working Party 29 the extra-territorial application is based on the conventional principle of the *lex protectionis* (whereby the connecting factor is the location of the (legal) persons to be protected, which places the emphasis on the actions) rather than the territoriality principle (whereby the connecting factor is the location of the actors to a territory).[72]

The relevance of this summary given by the Working Party 29 is somewhat unclear as the Data Protection Directive contains a specific provision for the applicability of the Data Protection Directive which takes priority over the

---

70 Working Document on Non-EU Based Websites (Chapter 2, n 62), at 3.

71 Working Document on Non-EU Based Websites (Chapter 2, n 62), at 3-4.

72 Bing, 'Data protection, jurisdiction and the choice of law', Privacy Law and Policy Reporter [1999] 65, at 7.

general conflict rules of international private law.[73] The Working Party 29 subsequently acknowledges this itself where it concludes the introduction with: 'Against this background, it has to be noted that the EU data protection directive contains an explicit provision on the applicable law indicating a criterion. Irrespective of whether this provision is easy to understand or to handle, it is nevertheless an advantage for the benefit of individuals and business that the data protection directive addresses this essential question'.[74]

After this catalogue of examples of EU laws based on the protection principle it is somewhat surprising that the Working Party 29 subsequently indicates that the explicit provision in the Data Protection Directive is one based on the physical link with a Member State and that it is not the nationality of the individuals that is decisive but the location of the processing equipment. The Working Party 29, however, subsequently makes a full reversal by then concluding that this principle 'reflects a true concern to protect individuals on [their] own territory'[75] and that 'at international level it is recognised that

---

73 Under international private law, rules of semi-public law or special obligatory rules of private law take precedence over general rules of international private law. In this context, the Directive can be considered as containing rules of precedence as they contain mandatory rules that aim to protect a group of relatively weak legal persons, as is expressed in Recital 10 of the Directive. See Blok (Chapter 2, n 29), at 302. See more extensively para. 12.3.2.

74 Working Document on Non-EU websites (Chapter 2, n 62), at 5.

75 Kuner (n 37), at 21 – 22, referring to this citation of the Working Party 29, seems to conclude that Article 4(1)(c) is not based on the territoriality principle but rather on the "protective principle" or even the "effects doctrine" (i.e. whereby the connecting factor is the fact that conduct outside a state has effects within the State. See Kuner at 22, for his conclusion as to the protective principle: "The Article 29 Working Party has indicated that the protection of individuals inside the EU is one of the main purposes of Article 4(1)(c), a view which is shared by some commentators [Ulrich Dammann, 'Internationaler Datenschutz' (2002) Recht der Datenverarbeitung, at 73].Thus, it seems that the function of this provision is largely to protect individuals in the EU, even if it does not fulfill the traditional criteria of protective jurisdiction."; and Kuner at 22 for his conclusion as to the effects doctrine: "While seeming to apply the objective territoriality principle, Article 4(1)(c) is focused not on the use of equipment per se, but on preventing data controllers from evading EU rules by relocating outside the EU. Thus, Article 4(1)(c) also focuses on the effect produced in the EU by data processing outside the EU, and the protection of EU citizens, meaning that it can also be viewed as an application of the effects doctrine." Kuner's opinion seems to contradict his earlier opinion in Kuner (n 37), at 125 as cited in n 64), where he concluded that the interpretation whereby cookies amount to equipment "would (…) in effect result in the location of the data subject (rather than the place of establishment of the data controller) always determining the applicable law, which is clearly not the principle underlying Article 4 of the General Directive". Further, as shown in this Chapter,

states can afford such protection'. This is a creative manner indeed to transform the territoriality principle into the protection principle:

> 'The European Parliament and the Council decided to come back to one of the classic connection factors in international law, which is the physical link between the action and a legal system. The EU legislator chose the country of the territorial location of equipment used. The directive therefore applies when a controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State.
>
> The objective of this provision in 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law.
>
> It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States law on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen. It is the location of the processing equipment used that counts.
>
> The Community legislator's decision to submit processing that uses equipment located in the EU to its data protection laws thus reflects a true concern to protect individuals on its own territory. At international level it is recognised that states can afford such protection. Article XIV of the GATS allows to lay down exemptions from free trade rules in order to protect individuals with regards to their right to privacy and data protection and to enforce this law'.[76]

---

the Working Document on Non-EU Based Websites is contrary tot the legislative history of the Directive as well as the commentary of Dammann and Simitris thereon (see citation in para. 3.3.3). More in general I remark that the connecting factor of territoriality obviously also leads to protection of citizens in the relevant territoriality. The fact that this connecting factor leads to such protection may even be a or the reason to choose this connecting factor, but this in itself does not justify the conclusion that the connecting factor is 'thus' based on the protection principle or the effects doctrine.

[76] Working Document on Non-EU Based Websites (Chapter 2, n 62), at 5.

In its subsequent interpretation of Article 4(1)(c) the Working Party 29 interprets the provision in line with the protection principle rather than the territoriality principle (with an emphasis on the action rather than the actor) by taking the position that the sending by a non-EU based website of 'cookies' to the computers[77] of internet users in the EU constitutes the use of 'equipment' in the EU. As all users use a computer (or hand-held device) to visit a website (and almost all websites use cookies) this amounts to indiscriminately applying the Data Protection Directive to all data processing of EU nationals who visit foreign websites.

It may be derived from the Working Document that the Working Party 29 itself is also not too sure about the tenability of its position where it advocates a 'cautious approach' when applying Article 4(1)(c):[78]

> 'The Working Party would advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is there is a reasonable degree of enforceability having regard to the cross-border situation involved.'

It may be clear that these factors are not based on the Data Protection Directive and are so vague (the Data Protection Directive applies when it 'makes sense'?) and therefore cannot constitute a valid basis for controllers to decide whether to apply the EU data protection laws.

The conclusion is that the interpretation given by the Working Party 29 is contrary to the legislative history of Article 4(1)(c). Although the attempt of the Working Party 29 to provide protection to EU nationals is commendable, this result should be achieved by amendment of the applicability rule for instance by bringing this rule in line with the general rules of international private law. This should be done by European legislators and not via the short-cut of opinions of the Working Party 29.

---

77 The Working Party 29 only refers to computers. By now many users access the internet by means of hand-held devices (like smart phones). As the browsers of (most of) these devices also use cookies, this will probably not change the position of the Working Party 29.

78 Working Document on Non-EU Based Websites, (Chapter 2, n 62), at 11-12.

3.8.2 JavaScript, Ad banners and Spyware

A similar position (based on similar considerations) is taken by the Working Party 29 in respect of the use of JavaScript, ad banners and spyware. In summary the position of the Working Party 29 is that these 'tools' are used to collect and process data whereby use is made of the equipment of the data subject (computer, browser, hard drive). Based on the rationale of Article 4(1)(c) as applied in respect of cookies (see Paragraph 3.7.3 above), also here the conclusion should be that applying Article 4(1)(c) to these tools would amount to applying the protection principle (the applicable law is that of the nationality of the user visiting the website) rather than the territoriality principle, which was not the choice made by the legislator. For the sake of completeness, I have listed a description of these tools at the end of this publication as well as the position of the Working Party 29 in respect thereof.

Before discussing how Article 4(1)(c) may be amended, I first briefly discuss the various national implementation provisions and the findings of the European Commission in its First Report on the implementation of the Data Protection Directive.[79]

3.9 National implementation laws

3.9.1 Equipment versus means

Article 4(1)(c) has been more or less uniformly implemented by most Member States.[80] The main hiccup in the implementation in national laws is presented by the different language versions of the Data Protection Directive itself (as discussed in Paragraph 3.1 above) whereby the English version of Article 4(1)(c) uses the word "equipment", while the word used in other language versions would translate into "means" in English. As a consequence, most national implementation laws use a term that would be a translation of "means". Only Ireland, Sweden, Denmark and the United Kingdom use the term "equipment" or a comparable term.[81] The term "means" would appear to be wider than "equipment" which suggests a physical apparatus.[82] Korff[83] noted that many national DPAs take "means" to

---

79 European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final (**First Report on the Directive**).

80 Korff (n 6), at 48-51.

81 The Swedish law, for example, uses the word 'untrusting'.

82 Korff (n 6), at 48 , who indicates that most examples given are the use of a telephone to collect data, the sending of paper forms to data subjects in the EU, etc.

83 Korff (n 6), at 48-51.

have a very broad meaning indeed, covering all conceivable means as collection of data by telephone, access of a non-EU website by means of a PC or terminal based in the EU or the sending of paper forms by a non-EU controller to EU nationals. If such a broad interpretation is given, "in effect, all processing involves means". In this interpretation "equipment" or "means" is in fact meaningless and could as well have been deleted from Article 4(1)(c). This may explain why some national implementation provisions do not contain any reference to "equipment" or "means".

Examples where no reference is made to "equipment" or "means" are the laws of Germany and Austria. These laws apply to **all** processing in Germany and Austria, irrespective of the presence or use of specific types of means or equipment:

> "This Act shall apply in so far as a controller which is not located in a member state of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data in Germany."[84]

The same applies for the Austrian law, which refers to the "use" of personal data.[85] Danish law did implement Article 4(1)(c) but added a second provision which extends the applicability of the law to all situations where data are collected within Denmark for purposes of processing in a third country, regardless of the means used:

> "This Act shall also apply to a controller who is established in a third country, if
>
> (1) the processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the European Community; or
> (2) **the collection of data in Denmark takes place for the purpose of processing in a third country**."[86]

3.9.2 For purposes of transit only

The exception with regard to controllers who use equipment "only for purposes of transit through the territory of the Community" is also

---

84 Federal Data Protection Act of 15 November 2006, section 1 sub 5.

85 Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), section 3 sub 1.

86 The Act on Processing of Personal Data, Act No. 429 of 31 May 2000 as amended by section 7 of Act No. 280 of 25 April 2001, section 6 of Act No. 552 of 24 June 2005 and section 2 of Act No. 519 of 6 June 2007, article 4 sub 3.

implemented in various ways. Danish, Italian and Portuguese law have implemented it as such.[87] Other countries (France and Luxembourg) have specified transit as taking place through their own territory or through the territory of other EU Member States, which basically brings about the same outcome. Sweden defines transit as taking place between "third countries" (i.e. between non-EU countries). This also seems to result in a semantic difference. As the EU is in that case used for transit between these third countries only, this also seems to amount to the same result. The Netherlands, Greece, Denmark and Spain refer to transit without mentioning a geographical dimension. This will not pose a problem. If the question is submitted to a national court, such court will have to apply the applicable national implementation law in accordance with the Data Protection Directive (i.e. transit through EU territory).[88] The United Kingdom, Finland, Belgium and Ireland only refer to transit through "their own territory". This might make a difference if for instance equipment in the UK is used for transit purposes within the UK only (in which case UK law will not apply), but for other purposes in another Member State (therefore not for transit purposes only). However, this scenario seems to work only if equipment is also located in such other Member State (which is then not used for transit purposes only) as a consequence of which the national law of that Member State will apply. The application of the UK provision will therefore not result in a gap in the protection. In fact, application of the UK provision thus prevents an unnecessary cumulation of applicable laws. The rule of Article 4(1)(c) leads to the applicability of the laws of all Member States where equipment is used (also of those where the equipment is used for transit purposes only), while the UK provision would lead to the applicability of the Member State's law only where the equipment is used for other purposes. In my opinion the UK provision whereby cumulation of applicable laws is avoided may be considered an improvement as regards the present provision. An amendment of the Directive in accordance with the UK provision would therefore be welcomed.

---

87 Danish Act on processing of Personal Data, article 4 sub 3 (1), Italian Personal Data Protection Code (Legislative Decree No.196 of June 30, 2003), section 5 sub 2, Portuguese Act on the Protection of Personal Data (Act 67/98 of 26 October), article 4 sub 3(b).

88 This means that the national court must interpret rules of national legislation as much as possible in the light of the wording and the purpose of the relevant directive, in order to reach the intended result. Interpretation in accordance with a directive finds its limitation if the relevant interpretation would be a clear violation of the national law (i.e. would be *contra legem*). In that case the national court will have to apply the national rule; plaintiffs will have to address their legislator for wrongful implementation of the Directive into national law. Case C-106/89, *Marleasing SA v. La Comercial Internacional de Alimentacion SA* [1990] ECR I-04135, par. 8.

However, as the UK provision (and those of Finland, Belgium and Ireland) is clear cut in this respect, it will not be possible to interpret these laws "in accordance with the Data Protection Directive" which finds its limitation if such interpretation were to be *contra legem*. The laws of these countries therefore create a disparity between the EU national laws which should be avoided.

3.9.3 EEA states

Another disparity between national implementation laws is created by how the various Member States treat the EEA states (Iceland, Liechtenstein and Norway). Some Member States treat these countries as EU Member States.[89] A consequence of this is that in these countries Article 4(1)(c) does not apply if the relevant controller is established in these EEA countries. Guidance would be welcomed on how to treat controllers of EEA states (and of other "adequate countries"[90] for that matter) in a uniform manner.

3.10 First Report on the Data Protection Directive

Pursuant to Article 33 of the Data Protection Directive, the European Commission has to report at regular intervals on the implementation of the Data Protection Directive and, if necessary, provide suitable proposals for amendment. Based on a survey of the various national implementation provisions of Article 4(1) (Technical Analysis)[91] the Commission concludes in its First Report on the Data Protection Directive that Article 4(1)(c) has not been uniformly implemented and that the substantial divergences in implementation mean that potential positive and negative conflicts of law remain between the Member States.[92] This means that due to lack of harmonisation in the EU controllers have to comply with deviating national

---

89 Denmark, Sweden, Ireland and the UK.

90 Pursuant to Article 25(6) and 31(2) Data Protection Directive the European Commission may issue a so-called adequacy finding in respect of a country. See for the countries that obtained an adequacy finding http://ec.europe.ec/home/fsj/privacy/thirdcountries/index_en.htm, presently being Argentina, Canada, Switzerland, Guernsey, Jersey, Isle of Man, and the U.S. (in respect of transfers of air passenger name records data and companies that have adhered to the Safe Harbour principles). Kuner (n 37) at 119 comments that 'at least some commentators take the view that Article 4(1)(c) applies whether or not the controller is established in a country that has been determined to offer an adequate level of data protection under the Directive'.

91 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, attached to the First Report on the Data Protection Directive (Technical Analysis).

92 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, attached to the First Report on the Data Protection Directive (Technical Analysis), at 7-8.

law (which creates conflicts of law). Such conflicts would have been avoided if Article 4 had been uniformly implemented throughout the EU. Regarding Article 4(1)(c), the Technical Analysis mostly focuses on the use of the term 'means' vs. 'equipment' (see Paragraph 3.1 above). Despite these divergences the Commission did not recommend that Article 4(1)(c) be amended.[93] The Commission indicated that it is its 'priority to secure the correct implementation by the Member States of the existing provision' and that 'more experience with its application and more reflection is needed, taking into account technological developments, before any proposal to change Article 4(1)(c) might be made'.[94] The Commission continued that it:

> 'is aware that the 'use of equipment' criterion of 4(1)(c) may not be easy to operate in practice and needs further clarification. Should such clarification not be sufficient to ensure its practical application, it might in due course be necessary to propose an amendment creating a different connecting factor in order to determine the applicable law.'[95]

In November 2010, the Commission in its Communication on revision of the Directive[96] repeated its intention to consider a different connecting factor:

> "The Internet makes it much easier for data controllers established outside the European Economic Area (EEA) to provide services from a distance and to process personal data in the online environment; and it is often difficult to determine the location of personal data and of the equipment used at any given time (e.g., in "cloud computing" applications and services). However, the Commission considers that the fact that the processing of personal data is carried out by a data controller established in a third country should not deprive individuals of the protection to which they are entitled under the EU Charter of fundamental Rights and the EU data protection legislation."

3.11 Proposed revision of Article 4(1)(c)

When thinking about revising Article 4(1)(c), it should be taken into consideration that:

1. any connecting factor that relates to the making use of 'equipment' (even if used in a 'technology-neutral' meaning) is no longer suitable given the speed of developments whereby the 'means' used for data

93 First Report on the Directive (n 79), at 17.

94 First Report on the Directive (n 79), at 17.

95 First Report on the Directive (n 79), at 17.

96 EC Communication on the revision of the Directive (n 11), at 11.

collecting and processing are in constant development; any connecting factor should apply irrespective of the means used;[97]

2. the underlying principle of territoriality whereby a physical connection is required to a territory is no longer suited to be applied in the current day reality.[98] The principle of territoriality can only work if it has a true 'virtual nature';
3. an unbridled expansion of applicability of EU data protection laws to processing of data of EU citizens wherever in the world should be prevented;[99]

---

97 Kuner (n 37), at 4, rightfully notes that this is in conformity with trends in other areas of the law that the presence of computer or telecommunications equipment should not be used as a connecting factor, giving as an example Article 2(c) of the E-Commerce Directive, stating 'the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider".

98 As Kobrin (n 64), at 23, states it: 'Extraterritorial reach not only becomes the norm, the concept itself looses meaning as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system.' And at 28: 'Transnational integration, however, is increasingly relational rather than geographic; the new political space from which effective and legitimate governance must emerge takes the form of relational networks rather than territory, a 'space of flows' rather than a 'space of spaces'.

99 This would amount to applying the so-called 'effects doctrine', which is already in the off line world criticised as it is too open-ended, i.e. leads to applying the laws of a state even if the effects are insubstantial. See Thomas Schultz, 'Carving up the Internet: Jurisdiction, legal Orders, and the private/Public International Law Interface', (2008) 19 European Journal of International Law 799, at 815. See also Kuner (n 5), at 21 (and literature there referred to): "Perhaps the most controversial jurisdictional basis of all is the 'effects doctrine', under which jurisdiction is based on the fact that conduct outside a State has effects within the State. The effects doctrine has been vehemently criticized, but seems to have become widespread, at least with regard to assertions of jurisdiction over conduct on the Internet. The basic problem with the effects doctrine is that it is open-ended, since 'in a globalized economy, everything has an effect on everything'. An additional problem is that 'the widening of the reach of effect based jurisdictional rules results in a widening of the gap between reasonable grounds for jurisdictional, and application of law, claims on the one hand and reasonable grounds for recognition and enforcement of foreign judgments on the other'. Kuner (n 64), at 22 (after having evaluated the main jurisdictional grounds in Kuner (n 5)), however comes to the overall conclusion that: "The threshold for finding a type of jurisdiction to be 'exorbitant' or 'improper' under public international law is high, and claims that particular types of jurisdiction 'violate international law' should thus be taken with a grain of salt". As to the effects doctrine he concludes at 23:
"The effects doctrine is more controversial, but it seems that it is becoming widely (albeit sometimes grudgingly) accepted" (this referring to: Working Document on Non-EU Based

Websites, at 4, stating 'whether it is a requirement that the relationship have a "community dimension" or "close connection" with the Community, in certain situations the European Court of Justice, the European Parliament and Council as well as the European Commission see fit to impose EU rules on non EU based entities'; Ian Brownlie, Principles of Public International Law (7th ed Oxford University Press 2008), at 311-312, finding that extraterritorial acts can be the subject of jurisdiction if the following tests are met: (1) there is a substantial and bona fide connection between the forum and the subject matter; (2) the principle of non-intervention in the domestic or territorial jurisdiction of other States must be respected; and (3) principles such as accommodation and proportionality must be observed. See also Jack Goldsmith, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review 1199, at 1208, stating '[I]t seems clear that customary international law…permits a nation to apply its law to extraterritorial behavior with substantial local effects'." At 23 he, however, concludes that "even protective jurisdiction 'does not dispense with the requirement for a substantial connection between the forum and the parties and/or the dispute', and the criterion of 'use of equipment' as contained in Article 4(1)(c) of the EU Data Protection Directive seems both too tenuous and too unclear to serve as a sufficient jurisdictional link" (this referring to "Jonathan Hill, 'The Exercise of Jurisdiction in Private International Law' in: Patrick Capps, Malcolm Evans and Stratos Konstadinidis (eds.) *Asserting Jurisdiction: International and European Legal Perspectives* (Hart Publishing 2003) 39, at 53")

For reference purposes below follow a number of examples of rules in EU legislative instruments that have an indiscriminate application: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L201/37; as revised by Directive 2009/136/EC of the European Parliament and of the Council 25 November 2009 (**E-Privacy Directive**). The E-Privacy Directive lacks a specific applicability regime. The prevailing view is however that the opt-in requirements for the use of cookies and direct e-mail apply to all interactions with internet users in the EU. This is based on Article 3(1) E-privacy Directive, which states: 'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks *in the Community*' (emphasis added). As all internet users in the EU use a public network located in the EU, the rules of the E-Privacy Directive apply to all e-mail from outside the EU to individuals in the EU as well as to all visits of EU citizens to non-EU websites. See also Kuner (n 5), at 24 referring to European Commission, DG Information Society, Communications Committee Working Document on 'Practical follow-up to the opt-in approach regarding unsolicited electronic mail for direct marketing as included in Directive 2002/58/EC' (unpublished) at 6, stating 'the new Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. As a consequence, Article 13 establishing the opt-in rule is applicable to all unsolicited commercial communications received on or sent from networks in the Community. This implies that such messages originating in third countries must also comply with EC rules, as must messages originating in the EC and sent to addressees in third countries'. A similar indiscriminate scope is included in Directive 97/7/EC of the

4. an unbridled applicability of EU data protection laws to the processing of data on behalf of foreign data controllers with no other link to the EU than the use of processing services of an EU data processors should be prevented; and
5. gaps in protection should be prevented (the gap in protection created by non-alignment of Articles 4(1)(a) and (c) (see Paragraph 4.2 above) should be avoided, i.e. these provisions should be aligned.

Without upsetting the rationale of the applicability regime of the Data Protection Directive the above factors would require that Article 4(1)(c) be amended in such a manner that it is will be a true 'virtual' reflection of the territoriality principle. This will entail:

- elimination of any 'physical location' as a connecting factor (whether of the controller, the equipment used or the activities of the controller);
- elimination of the 'use of means' as a connecting factor;
- if 'use of means' is no longer a connecting factor the exception for use of equipment 'for transit purposes only' can be eliminated.
- the unbridled application of Article 4(1)(c) to all processing through websites and to data processing on behalf of foreign controllers by EU data processors can be prevented by requiring that the processing takes place 'in the context of the activities of the controller **on or directed at**[100] the territory of the Member State'.
- by using this as the connecting factor, Articles 4(1)(a) and (c) will also be aligned and gaps in the protection will be avoided.

The above reflected into a text proposal[101] amounts to applying Article 4(1)(c) to situations where the:

European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, [1997] OJ L144/ 19 (the 'Distance Selling Directive'). The online contracting and information requirements of the Distance Selling Directive apply to all entities that contract for goods or services via email and internet with EU citizens, therefore also non-EU entities.

[100] This element has to prevent discussions whether certain online activities of a controller should be considered to take place on the territory of a Member State. A comparable element was part of the proposed provision on applicable law and jurisdiction in the latest Madrid draft proposal for International Standards. The provision was however left out of the final version (see for the text of the relevant provision para. 4.6, in particular n 30).

[101] Though the Working Party 29 in its Opinion on applicable law (n 12) confirmed its interpretation that the use of cookies constitutes the use of equipment under Article 4(1)(c) (see citation in n 66), the Working Party 29 in fact adopted a similar approach to revision of Article

4(1)(c) as I advocated for, which will result that in many cases Article 4(1)(c) will no longer apply to the use of cookies, if the relevant non-EU website is not directed at the EU. See at 14, where the Working Party 29 indicates that it no longer considers the use of "equipment" suitable as a connecting factor and further suggests replacing Article 4(1)(c) with a connecting factor based on "targeting of individuals" as also used in other EU instruments. These starting points are very similar to the starting points set out above. See also at 24: "The application of the Directive to a controller for the whole processing should be supported as long as the link with the EU is effective and not tenuous (such as by almost inadvertent, rather than intentional, use of equipment in a Member State). A more specific connecting factor, taking the relevant "targeting" of individuals into account (…) could be useful in terms of legal certainty, as further developed in the conclusions. Such a criterion is not new and has been used in other contexts in the EU [footnote: Article 15(1)c of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 12, 16.1.2001, p.1)], and by the United States' legislation on the protection of children on-line. This is also the case in some national laws transposing Directive 2000/31/EC on electronic commerce, stating that providers not established in the EEA will fall within the scope of these national laws when they target services specifically to their territory. The application of a similar criterion for the data protection legislation in the EU could be reflected upon during future discussions on the revision of the data protection framework." See further the conclusions of the Working Party 29 at 31-32: "Additional criteria should apply when the controller is established outside the EU, with a view to ensuring that a sufficient connection exists with EU territory, and to avoid EU territory being used to conduct illegal data processing activities by controllers established in third countries. The two following criteria may be developed in this view:

– The targeting of individuals, or "service oriented approach": this would involve the introduction of a criterion for the application of EU data protection law, that the activity involving the processing of personal data is targeted at individuals in the EU. This would need to consist of substantial targeting based on or taking into account the effective link between the individual and a specific EU country. The following examples illustrate what targeting could consist of: the fact that a data controller collects personal data in the context of services explicitly accessible or directed to EU residents, via the display of information in EU languages, the delivery of services or products in EU countries, the accessibility of the service depending on the use of an EU credit card, the sending of advertising in the language of the user or for products and services available in the EU. The Working Party 29 notes that this criterion is already used in the field of consumer protection: applying it in a data protection context would bring additional legal certainty to controllers as they would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules.

- The criterion of the equipment/means: this criterion has been shown to have undesirable consequences, such as a possible universal application of EU law. Nonetheless, there is a need to prevent situations where a legal gap would allow the EU to be used as a data haven, for instance when a processing activity entails inadmissible ethical issues. The equipment/means criterion could therefore be kept, in a fundamental rights perspective, and in a residual form. It would

> 'controller is not established on Community territory but the processing of personal data takes place in the context of the activities of the controller in or directed at the territory of the Member State'

Article 4(1)(a) and (c) being thus aligned, they can then also be simply taken together by providing that the national laws apply:

> 'to the processing of personal data in the context of the activities of the controller in or directed at the territory of the Member State'

To ensure that the EU does not become a digital haven for data processing by EU data processors in EU territory (see Paragraph 3.6), a second ground for applicability can be added if the first ground does not apply.[102] Rather than applying the Data Protection Directive by imposing obligations on the foreign data controller, I prefer a solution whereby the Directive imposes obligations directly on the EU data processor performing the data processing activities in EU territory. The obligations to be imposed on the data processor would concern the data security obligations of Article 17 Directive and further the obligations to ensure that an adequate level of protection is provided for the data processed, within the meaning of Article 25(2) of the Directive. This should not be too onerous for EU data processors. For instance, in practice we already see solutions whereby the data are transferred to the EU data processor in encrypted form as a result whereof the Data Protection Directive does not apply to such processing.

If the foregoing obligations are included in the Directive, the second ground for applicability can be:

> "if a processing of personal data takes place in the territory of a Member State, the national law of that Member States applies insofar as it implements the obligations of the data processor to ensure that the data processing (i) is

---

then only apply as a third possibility, where the other two do not: it would address borderline cases (data about non EU data subjects, controllers having no link with the EU) where there is a relevant infrastructure in the EU, connected with the processing of information. In this latter case, it might be an option to ensure that only certain data protection principles – such as legitimacy or security measures – would apply. This approach, which obviously would be subject to further development and refinement, would probably solve most of the problems in the current Article 4(1)c."

[102] The Working Party 29 in its Opinion on applicable law (n 12), at 32 proposes to keep the "equipment/means" criterion in residual form for these purposes, see citation in n 101 (last paragraph).

> adequately secured in accordance with Article 17 of this Directive and (ii) provides for an adequate level of protection for such data processing within the meaning of Article 25(2) of the Directive."

The Working Party 29 can subsequently contribute in expanding on the requirements when any processing by a controller can be considered to take place 'within the context of the activities of the controller on or directed at the territory of a Member State'. This should not be problematic as this can be done along similar lines as in its Working Document on Non-EU Based Websites in respect of Article 4(1)(a), see Paragraph 3.2.3 above.[103]
Relevant criteria would for instance be if the controller contracts with visitors from the EU, performs actual deliveries and (after) sales services in this Member State, if the website is promoted by means of local targeted advertisements to the inhabitants of that state, i.e. by listings with local search engines, banner advertisements on local websites, off line advertisements or product placements in shops, provision of Member State specific information (for instance the tax regime) relating to a Member State, etc.

The applicability regime of the data protection Directive is thereby also brought in line with the jurisdiction and applicable law regime for consumer contracts of Article 6 of EC Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I),[104] which provides that (in the absence of a valid choice of law) a consumer contract:

---

[103] In its Opinion on applicable law (n 12), at 14-15, the Working Party 29 already elaborated on the concept of "in the context of the activities" of an establishment, see for citations 2.4.4, n 64. At 32, the Working Party 29 indicated it had the intention to provide even further guidance: "Some clarification would also be useful with regard to the notion of "context of activities" of the establishment. The Working Party has emphasised the need to assess the degree of involvement of the establishment(s) in the activities in the context of which personal data are processed, or in other words to check "who is doing what" in which establishment. This criterion is interpreted taking into account the preparatory works of the Directive and the objective set out at the time to keep a distributive approach of national laws applicable to the different establishments of the controller within the EU. The Working Party considers that Article 4(1)a as it stands now leads to a workable but sometimes complex solution, which seems to argue in favour of a more centralised and harmonised approach."

[104] [2008] OJ L177/6. The Working Party 29 indicated in its Opinion on applicable law (n 12), at 24, that a parallel may be found with Article 15(1)c of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 12, 16.1.2001, p.1) (**Brussels I Regulation**) and for its interpretation to the Conclusions of Advocate General Trstenjak, 18 May 2010, in C-144/09, Hotel Alpenhof. As Article 4(1)(c) concerns a provision of applicable law the logical parallel is to

> 'shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional [seller]:
> (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or
> (b) by any means, directs such activities to that country or to several countries including that country,
> and the contract falls within the scope of such activities.'

Some guidance as to when there is 'directed activity' is to be found in Recital 24 to Rome I:

- it is not sufficient that an undertaking targets its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State, a contract must also be concluded within the framework of its activities;
- the mere fact that an internet site is accessible is not sufficient for this provision to be applicable, although a factor will be that this internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means;
- the language or currency which a website uses does not constitute a relevant factor.

Applying these starting points to the proposed article 4(1)(c) would entail that the mere fact that a non-EU website processes personal data of visitors from the EU should not be sufficient for the Data Protection Directive to apply. Even the conclusion of an online contract alone should not be sufficient. The website owner should actively solicit those visits and sales by visitors from the EU by some activity targeted to these visitors. In most cases this will involve some local activities in a Member State (local advertisements, listings with local search engines, contacts with local distributors). In any event the text proposal for Article 4(1)(c) and the connecting factors of Rome I all have in common the need to be further expanded as these concepts all lack clarity.[105]

---

be found with Rome I, which provides rules on applicable law. However, this does not make much difference since according to Recital 24 of Rome I, Article 6 of Rome I should be interpreted harmoniously with Article 15 of the Brussels I Regulation.

[105] See for criticism what 'targeting' means: Uta Kohl, *Jurisdiction and the Internet: a Study of Regulatory Competence over Online Activity* (Cambridge University Press 2007) at 76-78; and Schultz (n 99), at 818.

The acid test here is whether the consumer protection rules of Rome I would apply to, for instance, the .com website of Amazon, assuming that Amazon had no localised versions of its website, that any products bought would be sent directly by Amazon US to any consumer around the world and that the website was not supported by local advertisements or other promotions. The conclusion should be that the consumer protection rules of Rome I would not apply in those circumstances as the site would not be targeted specifically to EU citizens. In the same vein, EU national laws implementing the Data Protection Directive should not apply to any processing of personal data by Amazon of these visitors from the EU.[106]

3.12 Proposed solutions in legal commentary

Bygrave suggests letting the protection principle prevail by amending the Data Protection Directive and making the applicable law the law of the state in which the data subject has his or her domicile.[107] This would parallel the existing European rules on jurisdiction and choice of law in the case of consumer contracts, such as the Brussels, Lugano and Rome Conventions.[108] According to Bygrave, this option deserves serious consideration in light of "the close relationship between the concerns of data protection law and consumer protection."[109]

Reidenberg[110] (presenting to the European Commission his opinion on whether the applicability regime of the Data Protection Directive is satisfactory) seems to be of the same opinion as Bygrave where he concludes:

---

[106] By now Amazon has many localised websites around the world, including several in the EU, and visitors to amazon.com are automatically routed to those localised websites. The EU consumer and data protection rules apply to such localised websites.

[107] Bygrave (n 64), at 10.

[108] Bygrave (n 64), at 10.

[109] Bygrave (n 64), at 10. He also launches as a possible compromise solution a solution suggested by another commentator to adopt a qualified version of the 'data subject domicile criterion'. This would stipulate that the data protection law of the country in which the data subject is domiciled will apply if the data controller should reasonably have expected that his processing of data on the data subject would have a potentially detrimental effect on the latter'. It is difficult to see that this would solve the problem of the EU data protection laws apply indiscriminately to all processing of data of EU nationals.

[110] Reidenberg, Workshop 4: International issues: international data transfers, applicable law and jurisdiction (European Commission Conference on the Implementation of Directive 95/46/EC, 2002), at 3-4.

- An expansive choice of law rule is consistent with other countries' rules (e.g. the US Children's Online Privacy Act [...] applies to any website on the Internet collecting information from children whether or not the web site is located on a US based server)
- The collection of data for processing is "doing business" within the forum where the individual is located and data protection law should require that data collectors be responsible in that forum for their activities conducted with that forum.

According to **Kuner**, the interpretation of 4 1(c) should be focused on the goal of the provision, which can be done without taking the extreme position that cookies should be considered equipment under all circumstances.[111] Kuner's suggestion is to limit the long arm reach of Article 4(1)(c) by making an analogy with the findings of the ECJ in the *Lindqvist* case.[112] In that case, the ECJ found that the data transfer restrictions under Article 25 of the Directive should not become a general rule that would apply to the entire Internet without the data controller taking a positive step to actively transfer personal data outside the EU.[113] This finding suggests that the rules of Article 4 should also not be applied to activities that could result in EU data protection law being extended to the entire Internet indiscriminately, "unless the non-EU data controller of a website has taken some positive steps to 'target' individuals in the EU."[114] Though commendable, this constitutes a solution which requires controllers to first apply the outdated connecting factor of "the use of equipment situated in a Member State" to subsequently apply the rule of the Lindqvist case. In his further publication in 2010[115] Kuner solved this issue by proposing: "In its ongoing review of the

---

111 Kuner (n 37), at 126-127.

112 Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

113 Kuner (n 37), at 124. Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para 69: 'If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the Directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.'

114 Kuner (n 37), at 124.

115 Kuner (n 64), at 20-21 (see footnote 172, for an overview of literature where the criterion of "targeting" is criticised).

EU Data Protection Directive, the European Commission should consider revising Article 4(1)(c) to focus it away from the use of equipment in the EU, and more towards the targeting criteria of Article 15(1) of the Brussels I Regulation, although it can be difficult to determine when an online activity is 'targeted' or 'addressed' at a particular State."

Terwangne & Louveaux[116] consider that the situation "where a data transfer is exclusively carried out by a controller located in a third country" should also fall within the scope of Article 4(1)(c).[117] They consider that the case when data is collected by a non-EU website through the use of cookies. They propose to extend the applicability of Article 4(1)(c) to also these situations, i.e. also situations where no use is made of equipment:

> "The principal criteria, therefore, which determines the applicability of the Directive to controllers situated outside of the European Union must not be limited to the use of equipment on the territory of a Member State. This use is only one element in the analysis **of the context in which the operations are carried out** in order to determine that the controller is "abnormally" established abroad even though his activities are mainly centred in Europe, or that one finds itself in the presence of a situation lacking any protection whatsoever".

Terwangne & Louveaux do not elaborate on the criteria "when operations can be considered carried out in Europe". They, however, give two examples where the scope of Article 4(1)(c) needs to be extended (Hungary was not part of the EU at the time the authors gave this example):

> "A German pharmaceutical company which establishes itself in Budapest and which collects data relating to medical prescriptions from a pharmaceutical network located within a Member State, in order to target European health professionals, is evidently trying to circumvent the provisions of the Directive and Article 4.1.c should apply.
>
> Similarly a company which collects data relating to the use of credit cards by Europeans in Europe (shopping in Paris, cinema in London, restaurant in Milan,..) and which sends the data to its subsidiary in the US in order to process it to obtain complete personal profiles of credit card users in Europe, should also fall under Article 4.1.c."

Note that the examples given by Terwangne & Louveaux would already fall within the scope of Article 4(1)(c) based on the requirements identified in this paper (i.e. should therefore not require amendment of Article 4(1)(c)).

---

116 Terwangne & Louveaux (n 64), at 239.

117 Terwangne & Louveaux (n 64), at 239.

That being said, the solution proposed by Terwangne & Louveaux is quite similar to the amendment to Article 4(1)(c) as proposed in this paper.

3.13 Conclusion

At the moment there are a number of Member States that have not properly implemented the applicability rule of Article 4(1)(c) of the Data Protection Directive. The Working Party 29 also uses an interpretation of this rule which seems contrary to the (legislative history of the) Data Protection Directive. Although the attempt of the Working Party 29 to provide protection to EU nationals is commendable, this result should be achieved by amendment of the applicability rule. Further, the applicability rules of Article 4(1)(a) and (c) should be aligned to avoid gaps in protection. These revisions should be done by European legislators and not via the short-cut of opinions of the Working Party 29. For the question of how EU regulators can best ensure full harmonisation in respect of the revised applicability regime, I refer to Paragraph 10.6.5, where I propose replacing the Data Protection Directive by an EU regulation in the upcoming revision of the Directive or, as a next best alternative, to confer the implementing powers in respect of a revised Directive to the European Commission.[118]
In conclusion, I recommend the following to EU legislators when revising the Data Protection Directive:

Recommendation 3
Delete Article 4(1)(a) and (c) and instead provide that the data protection law of a Member State applies:

- to the processing of personal data in the context of the activities of the controller in or directed at the territory of the Member State;
- and if the first ground is not applicable, to the processing of personal data in the territory of the Member State, but only insofar as it implements the obligations of a data processor to ensure that the data processing (i) is adequately secured in accordance with Article 17 of this Directive and (ii) provides an adequate level of protection for the data processed within the meaning of Article 25(2) of the Directive.

[118] Which the European legislators are empowered to do pursuant to Article 291(1) of the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**).

4 The jurisdiction regime of the Data Protection Directive

4.1 Introduction

In Chapters 2 and 3, I discussed when EU data protection law is applicable. In this Chapter I discuss the jurisdiction regime of the Data Protection Directive addressing the following two questions: when are the DPAs competent to take enforcement action and when can individuals address the DPAs or the courts of a Member State with a complaint or claim that their data protection rights have been violated? The Data Protection Directive provides a specific regime for jurisdiction of the DPAs, both as to the competence of the DPAs to take enforcement action at their own initiative, as well as when individuals may address the DPAs with a complaint. As to the right of individuals to address the courts, the Data Protection Directive only provides that the Member States must ensure that individuals have proper judicial remedies for any breach of their data protection rights, including the right to damages. It is left to the Member States how to implement this requirement. In most Member States no specific jurisdiction provisions are included in the national data protection law. As a result the courts in most cases (have to) decide their jurisdiction based on their general national rules of civil or administrative procedure.[1] A fundamental discussion of the concepts of applicable law and jurisdiction is outside the scope of this dissertation. A general note, however, is that the questions of applicable law and jurisdiction are separate questions which are generally subject to different regimes.[2] This entails that a court may have jurisdiction to hear a case but may not automatically be allowed to apply its own law. Conversely, the fact that the law of a Member State is applicable does not automatically entail that its courts also have jurisdiction to hear the case. Regimes of applicable law and jurisdiction are, however, closely related and their substantive scope and provisions are mostly aligned to ensure consistency.[3]

---

1 See para. 4.8.

2 Also under EU rules of private international law, the issues of applicable law and jurisdiction are subject to separate conventions, see for the rules on jurisdiction: EC Regulation 44/2001 of 22 December 2000 on jurisdiction and enforcement, [2001] OJ L12/1 (**Brussels I Regulation**); and for the rules on applicable law: EC Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations [2008] OJ L177/6 (**Rome I**); and EC Regulation 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations [2007] OJ L 99/40 (**Rome II**).

3 For instance the substantive scope and the provisions of Rome I, Rome II and the Brussels I Regulation are fully aligned to ensure consistency. See para. 12.5, in particular n 67.

4.2 Data Protection Authorities

The Data Protection Directive has ensured that each of the Member States has established a DPA to monitor and enforce compliance with its national data protection law.[4] The DPAs exercise their function with complete independence.[5] The Data Protection Directive has further ensured that each of the DPAs has been endowed with: investigative powers, effective powers of intervention and the power to engage in legal proceedings.[6]

The main rules for the competence of the national DPAs are set out in Article 28(4) and (6) Data Protection Directive:

> "(4) Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim."

> "(6) Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
>
> The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."

4.2.1 Jurisdiction to hear claims

"Any person" who wishes to file a claim concerning his rights under the Data Protection Directive may do so with any DPA, regardless of his nationality and regardless of which of the data protection laws of the Member States is applicable.[7] Complaints about violations of the Data Protection Directive can

---

4 Article 28(1) Data Protection Directive.

5 Recital 62 and Article 28(1) Data Protection Directive. See further Article 8(3) TFEU. See on the requirement of independence of DPAs in detail para. 14.7.5. At present, the independence of the DPAs is still not properly ensured in all Member States. See for more detail footnote 175 in that para.

6 Article 28(3) Data Protection Directive.

7 Article 28(4) Data Protection Directive. That it is not a requirement that the own law of the DPA applies can be derived from Article 28(6) Data Protection Directive "Each supervisory authority is competent, whatever the national law applicable to the processing in question". With

therefore never be rejected based on lack of jurisdiction of a DPA.[8] The jurisdiction regime for DPAs to hear claims is very broad indeed and has a strong protective element.[9] If the relevant DPA requires the assistance of another DPA to decide on the claim (for instance, the claim is governed by the law of another Member State) or to investigate the claim (the actual processing takes place in another Member State), such other DPA has to provide all relevant information and assistance.[10] Claims may also be lodged by "an association representing that person." This is not the equivalent of the traditional concept of a "class action" where damages may also be claimed, as DPAs do not have the right to award damages,[11] but in other respects its effect may be similar.[12] It entails that organisations such as civil liberty organisations, consumer associations, trade unions or privacy activist groups may lodge a complaint with the DPA on behalf of an individual or

---

"national law" reference is made to one of the data protection laws of another Member States rather than any other foreign law. This can be derived from the fact that the Directive contains many other provisions, which contain references to "applicable national law", which all refer to the laws of the Member States only. This can also be derived from the commentary of Ulrich Dammann and Spiros Simitis, EG-Datenschutzrichtlinie (Nomos Verlagsgesellschaft 1997), at 313 (see citation in para. 4.4).

8 Dammann and Simitris (n 7), at 313 (see citation in para. 4.4).

9 It is difficult to classify the jurisdiction basis of Article 28(4) in a distinct category. In any event the jurisdiction basis is not the territoriality principle since the jurisdiction of the DPA is not dependent on the fact that the data processing takes place within its country or that the controller is established in its country. The jurisdiction basis is also not the personality principle as the claimant may also be a non-national. The jurisdiction basis which shows the most connection is the "effects doctrine", which is concerned with protection of the nationals in that state's territory. The difference here, however, is that the protection is not only afforded to the nationals in the territory, but to all individuals regardless of their nationality. This is considered justified as the Data Protection Directive provides for protection of a fundamental right which should be afforded not only to own nationals. Whether this constitutes a too far-reaching basis for jurisdiction is discussed in para. 4.11.

10 Article 28(6) Data Protection Directive: "The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."

11 The right to award damages is not included in the powers the DPAs are to be endowed with pursuant to Article 28(3). Article 22 Data Protection Directive ensures that individuals may bring a claim for damages through the courts, see para. 4.8.

12 Douwe Korff, New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (January 15, 2010), European Commission DG Justice, Freedom and Security Report, available at SSRN: http://ssrn.com/abstract=1638949, at 99.

groups of individuals.[13] The DPA will then be able to exercise its enforcement powers.

Decisions by the DPAs may be appealed before the courts.[14]

4.2.2 Jurisdiction to enforce

Concerning the enforcement powers of the DPA, the rule of jurisdiction is based on the territoriality principle: each DPA has jurisdiction in its own territory. Conversely, DPAs cannot enforce their powers outside their territory. The Data Protection Directive (again) provides jurisdiction regardless of which of the laws of the Member States is applicable. This is relevant as the applicability regime of the Data Protection Directive may well lead to the applicability of the data protection law of another Member State than the Member State where the data processing takes place.[15] As a result, whenever these powers may factually be exercised (i.e. because a processing takes place in the relevant territory or if a controller is established in the relevant territory), the DPA of the relevant Member State has jurisdiction. By this provision the Data Protection Directive ensures that there is always one DPA that can actually exercise its powers. Otherwise the DPA where the individual has filed his claim cannot exercise its powers, as for instance the relevant data processing is not in its territory or the relevant controller has no establishment in its territory. By ensuring that such DPA can request the assistance of the DPA that can exercise its powers, effective enforcement is ensured throughout the EU (i.e. enforcement is based on a "network approach").

4.3 The legislative history of Article 28(4) and (6)

The Data Protection Directive had two draft versions:

- the Original Proposal;[16] and
- the Amended Proposal,[17] published together with an Explanatory Memorandum of the European Commission.[18]

---

13 Korff (n 12), at 99.

14 Article 28(3) Data Protection Directive.

15 For instance, if the controller is established in one Member State and involves a processor in another Member State to process data on its behalf. See on the scope of Article 4 in detail Chapters 2 and 3.

16 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314 – 2, 1990/0287/COD (**Original Proposal**).

17 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (92/C 311/04), OJ C/1992/311/30) (**Amended Proposal**).

The final text of the Data Protection Directive was adopted in 1995.

The provision of Article 28(4) Data Protection Directive was already included in the Original proposal and remained more or less unchanged. The provision of Article 28(6) Data Protection Directive was not included in the Original Proposal and the Amended Proposal. The Explanatory Memorandum does not contain any relevant clarifications.

4.4 Commentary by Dammann and Simitis

That the European legislators indeed had the above in mind when drafting the Data Protection Directive is confirmed by the leading commentary on the Data Protection Directive of Dammann and Simitis (translation by the author).

See comments in respect of Article 28(4):[19]

> "The Directive expressly requires the right to lodge a complaint with "**every** supervisory authority". In other words, every Member State must allow complaints lodged with the supervisory authorities it has established in accordance with sub-clause 1. This provision effects that a complaint may never be rejected because of lack of jurisdiction. If the addressed supervisory authority is locally or factually not competent, then it has to forward the complaint to the competent supervisory authority in accordance with the mandatory mutual cooperation as required by Paragraph 6, second paragraph, and inform the person who has filed the complaint accordingly. However, if there are doubts whether this person agrees to forwarding the complaint, the person must first be asked whether for reasons of protecting confidentiality, he agrees to the forwarding of the complaint".

And the comments in respect of Article 28(6):[20]

> "19. "Sub clause 6 requires the supervisory authorities to mutual cooperation and to exercise their powers, also on a cooperative level. Therewith the Directive confirms that exercise of the enforcement powers of sub clause 3 is based on the territoriality principle: every supervisory authority is competent "in the sovereign territory of its

---

[18] See COM (92) 422 final – SYN 287, 15 October 1992, p. 13 (**Explanatory Memorandum**). This Explanatory Memorandum is not available on the site of the European Commission, but can be retrieved from Archive of European Integration of the University of Pittsburg, at: <http://aei.pitt.edu/10375>.

[19] Dammann and Simitris (n 7), at 306.

[20] Dammann and Simitris (n 7), at 313.

own Member State…". In other words, no supervisory authority can exercise its enforcement powers outside of the sovereign territory of its own state. This is in line with the explanatory statement in the Directive that this allocation "is regardless of the law that is applicable to the relevant processing". Pursuant to Article 4 this may in individual cases also be the law of another Member State. This applies solely to the law applicable to the processing, while the law to determine jurisdiction of the supervisory authority is always that of its own Member State.

20. In view of the limitation of competence of the supervisory authority to the territory of its own Member State, in case of cross-border cases it is of great practical significance that the supervisory authorities of the relevant Member States provide enforcement support in international cases. Therefore the Directive specifies in sub clause 6 first paragraph, second sentence, that every supervisory authority "may be requested to exercise its powers by an authority of another Member State." This expresses at the same time the corresponding obligation to exercise these powers.

21. Additionally, the Directive under sub clause 6 second paragraph, generally requires the supervisory authorities to "….cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information." The obligation is valid within the individual Member States (if more than one supervisory authority exists) and between the supervisory authorities of different Member States. The legal effect of this provision is both to provide for the mandatory character as well as to provide a legal basis for the exchange of personal data, and for other forms of cooperation, such as the cooperation between employees of the supervisory authorities of several Member States in the local collection of facts with a cross-border significance."

4.5 Working Party 29 Opinion on applicable law

In December 2010 the Working Party 29 in its Opinion on applicable law also confirmed this interpretation:[21]

[21] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836/10/EN WP (**WP Opinion on applicable law**), at 10.

> "II.2.d) Applicable law and jurisdiction in the context of the Directive
> In the area of data protection, it is particularly important to distinguish the concept of applicable law (which determines the legal regime applicable to a certain matter) from the concept of jurisdiction (which usually determines the ability of a national court to decide a case or enforce a judgment or order). The applicable law and the jurisdiction in relation to any given processing may not always be the same.
>
> The external scope of EU law is an expression of its capacity to lay down rules in order to protect fundamental interests within its jurisdiction. The provisions of the Directive also determine the scope of applicability of the national laws of the Member States, but they do not affect the jurisdiction of national courts to decide relevant cases before them. The provisions of the Directive do, however, refer to the territorial scope of the competence of the supervisory authorities that may apply and enforce the applicable law. Although in most cases these two concepts – applicable law and competence of supervisory authorities – tend to coincide, usually resulting in Member State A's law being applied by Member State A's authorities, the Directive explicitly foresees the possibility of different arrangements. Article 28(6) implies that the national data protection authorities should be able to exercise their powers when the data protection law of another Member State applies to the processing of personal data carried out within their jurisdiction. The practical consequences of this issue will be further examined in a future opinion of the Working Party. Such situations result in the handling of cross-border cases, and highlight the need for cooperation between DPAs, taking into account the enforcement powers of each DPA involved. This also illustrates the need for national law to properly implement the relevant provisions of the Directive, as this may be decisive for an effective cross-border cooperation and enforcement."

This interpretation is also the prevailing opinion in the scarce legal commentary.[22]

4.6 Divergent opinion

[22] Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation (2nd ed. Oxford University Press 2007), at 112-113 (see however n 24); Ulrich Dammann, 'Internationaler Datenschutz' (2002) Recht der Datenverarbeitung, at 70, 73, 77. See further Peter Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet' (1998) 32 International Lawyer 991, at 1008. Striking is that some commentaries on the Directive, do not discuss the jurisdiction base for DPAs at all, but just discuss the different powers of the DPAs. See for instance the commentary on Article 28 by Christopher Klug, in: Concise European IT law (Kluwer Law International 2004), at 130-138.

The first in-depth publication on "Internet jurisdiction and data protection" appeared in 2010.[23] The author is of the opinion that Article 4 Data Protection Directive provides not only which law is applicable to a data processing, but that Article 4 at the same time also provides for jurisdiction.[24] The publication subsequently discusses whether Article 4 (and

---

[23] The publication was published in two parts: Christopher Kuner, Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1) (October 1, 2010), International Journal of Law and Information Technology, Vol. 18, p. 176, 2010. Available at SSRN: http://ssrn.com/abstract=1496847 (**Kuner I**); and Christopher Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2) (October 1, 2010). International Journal of Law and Information Technology, Vol. 18, p. 227, 2010. Available at SSRN: http://ssrn.com/abstract=1689495 (**Kuner II**).

[24] See Kuner I (n 23), at 5-6: "jurisdiction and choice of law are closely related, and the distinction between the two terms, if it ever was clear, has become increasingly vague", and "[t]he interface between jurisdiction and choice of law is particularly close in the area of data protection law, as can be shown by the example of EU law". Under acknowledgement of the fact that "Article 4 has the heading 'national law applicable', and would thus seem to be purely a choice of law provision" and "[t]he fact that the Directive includes specific rules on jurisdiction of the data protection authorities in Article 28(6)", Kuner still concludes that Article 4 does not only provides which law is applicable but at the same time provides for jurisdiction. See at 7: "[i]n the context of data protection law, applicable law rules may also serve much the same purpose as do jurisdictional rules". This opinion is contrary to his earlier interpretation of Article 4 in Kuner (n 22) at 112, where he comments (after having inserted the full text of article 4 Data Protection Directive): "These purposes might seem to argue for using Article 4 not only as a choice of law provision, but also as a positive basis of jurisdiction (i.e. for finding that a particular member state should have jurisdiction over a particular act of processing when that member state's law applies as determined by the Article's rules) and as a conflict of jurisdiction provision (i.e., that it should regulate not only which member state's law should apply to a particular act of processing, but also which member state's courts or data protection authorities have jurisdiction over such processing. In practice, some EU data protection authorities do seem to view Article 4 as providing a basis for direct jurisdiction over data controllers. Nevertheless, Article 4 must be seen as a choice of law provision, and not as a provision that allocates the jurisdiction of national courts and data protection authorities, since the General Directive includes specific rules on jurisdiction. Thus, the Directive contemplates the possibility of a national data protection authority (DPA) or court applying the law of a different member state in a dispute." Kuner refers for this position (at 112, footnotes 9 and 10) to :"Ulrich Dammann, 'Internationaler Datenschutz' (2002) Recht der Datenverarbeitung, at 70, 73, 77; and "Peter Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet' (1998) 32 International Lawyer 991, 1008, who sets forth various arguments for not regarding Article 4 as a jurisdictional provision (e.g. that it was not drafted as part of a 'publicised or negotiated effort to expand jurisdiction law generally', that Art 4 contains no mention of the word 'jurisdiction',

in particular Article 4(1)(c) Directive) constitutes "exorbitant" jurisdiction.[25] If this position were to prove correct, this would have far-reaching consequences for the jurisdiction regime of the Directive. I will briefly discuss below the arguments put forward to support this position. The first argument is that: "Article 28(6) seems to be as much about allocating the jurisdiction of the European DPAs among themselves as it is about determining what the proper boundaries of international jurisdiction under the Directive should be."[26] This argument is not conclusive. First of all, Article 28(6) concerns the rule for jurisdiction **to enforce** (see Paragraph 4.2.2). That Article 28(6) indeed has as a consequence that the jurisdiction **between** DPAs is allocated (i.e. each DPA to enforce in its own territory only), does not change the fact that Article 28(6) **also** provides for a positive ground for jurisdiction of the DPAs to enforce within its respective Member State in cases with an international element. DPAs, for instance, may also have jurisdiction to enforce in their territory if the relevant controller is established **outside the EU** or if the data processing takes place **outside the EU**. In the second place, Article 28(6) is not the only provision for jurisdiction of the DPAs; Article 28(4) provides for the jurisdiction of the

---

and that the general Directive was drafted 'before there was any significant deliberation about the nature of the internet and how to regulate it'".

25 See further on exorbitant jurisdiction para. 4.11.2.

26 Kuner I (n 23), at 7. In his footnote 25, Kuner supports his interpretation by stating that this: "is in accordance with the jurisdictional approach taken in other EU legal instruments such as the Brussels I Regulation. See Ralf Michaels, 'Two Paradigms of Jurisdiction' (2006) Michigan Journal of International Law 1003, stating at 1042 that 'Europeans do not typically distinguish between jurisdiction and international venue', and at 1043, that the main objective of the Regulation is 'to allocate jurisdiction to the most appropriate Member State, regardless of sovereignty interests of the Member States'." It is outside the scope of this dissertation to discuss the merits of these statements, and I will here limit myself to stating that the concept of international venue is indeed not a concept recognised as such in EU legal instruments. This, however, does not mean that the jurisdiction rules of the Brussels I Regulation would "thus" just regulate the "relative competence" between the courts of the Member States. The jurisdiction rules of the Brussels I Regulation provide for absolute competence rules, which also apply to cases with an international element, and may in certain cases also provide for jurisdiction in respect of defendants that are not domiciled in a Member State. A notable example is the consumer protection regime of Article 15(1)(c) Brussels I Regulation, where a consumer in matters relating to a consumer contract can sue its contracting party who is not domiciled in a Member State, if "the contract has been concluded with a person who pursues commercial or professional activities in the Member States of the consumer's domicile or, by any means, directs such activities to that Member States or to several States including that Member States, and the contract falls within the scope of such activities."

DPAs **to hear complaints** (see Paragraph 4.2.1).[27] This rule provides for a positive basis for jurisdiction to hear complaints on violations of EU data protection law which includes cases with an international element. As long as EU data protection law applies, the DPAs are competent to hear any complaints "by any person". This competence may therefore include cases where the controller is established outside the EU, the data processing takes place outside the EU, the affected individual is a non-EU national or any combination of the aforementioned. Further, the rule leads to concurrent jurisdiction of all DPAs whenever a violation of EU data protection law occurs and thus cannot be said to "just allocate jurisdiction **between** DPAs".

The second argument put forward is that "in practice, national data protection authorities often equate jurisdiction and applicable law."[28] This is undoubtedly correct and concerns a mistake also often made by regular courts, but cannot be a valid argument that the distinction "thus" does not exist. To illustrate the fact that DPAs often equate applicable law and jurisdiction, the author refers to the fact that "the global legal instrument on data protection drafted in 2009 by a group of data protection authorities chaired by the Spanish DPA adopts the same criteria for determining both applicable law and jurisdiction."[29] This is in itself correct[30], but the author refrains from mentioning in this context that the relevant provision never

---

27 Kuner I (n 24), completely ignores Article 28(4) as a rule of jurisdiction which is based on the effects doctrine rather than the territoriality principle. See for instance at 23: "Jurisdiction for claims brought before the national data protection authorities is determined by Article 28(6) of the EU Data Protection Directive, which sets forth a rule of territoriality, so that each national DPA has jurisdiction over data processing occurring on its territory."

28 Kuner I (n 23), at 7.

29 Kuner I (n 23), at 7.

30 See article 25 of the Agencia Espanola de Proteccion de Datos, Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data' (unpublished draft, 24 April 2009):

"25. Applicable Law and Jurisdiction

1. The processing of personal data will be governed by the applicable law and the competent tribunal of the State in which territory the responsible person has an establishment, within the framework of whose activities the processing is carried out.

2. In those cases where the responsible person has no establishment in a State but addresses its activity specifically to its territory, processing of personal data carried out under such activity will be governed by the applicable law and the competent tribunal of that State.

3. In the context of this paragraph establishment shall mean any stable facility that allows the real and effective exercise of an activity, regardless of their legal form."

See n 81 on why the relevant provision did not make it to the final version.

made the final version as adopted.[31] I fail to see how a proposal made in another context, which moreover for valid reasons[32] did not make it to the final version, can be decisive here.

A final argument brought forward[33] is that the Working Party 29 in its Working Document on Non-EU Based Websites stated that "an individual in the European Union who experiences problems with a non/EU website could submit his case to the competent national data protection supervisory authority".[34] Based on this quote the author concludes: "Thus, the Working Party 29 clearly equates the applicability of a particular Member State's law to a non-EU website with the DPA of that Member State having jurisdiction over the website." The quote from the relevant Working Document is an isolated sentence which is taken out of context. In the relevant passage the Working Party 29 (after having discussed when Article 4 applies to non-EU websites), discusses (under the heading "enforcement") "that enforcing rules in an international context is not as easy as solely within one given country" and that "the citizen has to be (made) aware of this." The Working Document then continues that "nevertheless, several possibilities exist and can be developed with a view to achieving a reasonable degree of enforcement." After having discussed that for instance "raising awareness about the EU rules", or introduction of "EU web seals" may be productive, the Working Party 29 provides a second possibility:

> "Furthermore, in a concrete case, an individual in the European Union who experiences problems with a non-EU website could submit his case to the competent national data protection supervisory authority. This authority would determine whether the directive, respectively the national data protection law, applies. If it does, the authority could develop contacts with the foreign website with a view to resolving the problem. "

The Working Party 29 does not discuss the rule for jurisdiction of the DPAs here, but merely refers to the "competent national data protection

---

31 Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, as adopted on 5 November 2009 at The International Conference of Data Protection and Privacy Commissioners in Madrid by the participating data protection authorities, to be found at www.agpd.es (**Madrid Draft Proposal for International Standards**).

32 See on the reasons for deleting Article 25, para. 4.11.

33 Kuner I (n 23), at 7.

34 Working Party 29, 'Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites' (WP 56, 30 May 2002) (**Working Document on Non-EU Based Websites**), at 15.

supervisory authority". It can be derived from the next sentence that the "competent relevant authority" (i.e. to be decided based on the rule for jurisdiction) subsequently has to decide whether the "Directive, or the national data protection law," applies (i.e. based on the rule for applicable law). It will not require much elaboration that this isolated (admittedly awkwardly phrased) sentence of the Working Party in a general passage on enforcement cannot support the far-reaching conclusion that Article 4 "thus" also provides for jurisdiction. In any event the quote is superseded by the more recent opinion of the Working Party 29 on applicable law (see citation above in Paragraph 4.5), where the Working Party 29 made explicit that the concepts of applicable law and jurisdiction under the Directive are distinctive and do not always lead to the same outcome.

This being said, I note that some of the confusion of whether Article 4 (also) provides for jurisdiction may be caused by the fact that Article 28 provides for such an extensive basis for jurisdiction, that whenever the law of a Member State applies, the DPA of such Member State will also always have jurisdiction. This, therefore, *de facto* leads to equation of the jurisdiction rule with the applicability rule. Why then still insist on making the distinction between the rule for applicability (Article 4) and the rules on jurisdiction (Article 28)? The reason is that the reverse situation is not a given. If a DPA has jurisdiction, this does **not** automatically entail that also the law of its Member State is applicable. DPAs may well have to apply another law. This may seem a semantic issue, but proves very relevant when assessing the applicability and jurisdiction regime of the Directive. As already indicated in the introduction, the rules of applicable law and jurisdiction are generally very much aligned, may in some cases coincide (as illustrated by Article 28) or be otherwise interrelated (as for instance the broadening of the scope of one may lead to a broadening of the scope of the other, or the other way around), but each regime has to be evaluated on its own merits.[35]

---

[35] Qualification of Article 4 as (also) a rule of jurisdiction, has for instance as a consequence that Kuner I (n 23), at 7, subsequently evaluates the applicability regime of the Directive against international principles on jurisdiction. See Kuner I, at 8: "This article is concerned with the allocation of regulatory authority between States as it relates to data protection law, and will focus on rules of jurisdiction, as opposed to those concerning applicable law and enforcement of judgments." With this focus, he overlooks to evaluate whether Article 28 Data Protection Directive possibly constitutes "exorbitant jurisdiction". Given the unbridled scope of jurisdiction provided by Article 28, this is a question worth asking, which I will discuss in para. 4.11. The cause for the confusion in Kuner's publication seems to be that the concept of jurisdiction is not equivocal and Kuner mixes the different concepts up, in the sense that he switches between the two. The different meanings of the concept of jurisdiction are well explained by Piet Jan Slot

and Eric Grabandt, Extraterritoriality and jurisdiction, Common Market Law Review 23 [1986], at 546 (emphasis added): "The concept of jurisdiction is (…) equivocal. It denotes the power of states to set rules on certain subjects and the power to enforce these. It also refers to the power of national courts to adjudicate claims brought by individual claimants. The former is a concept of **public** international law, the latter is a matter of **private** international law. As such these concepts seem to belong to two different worlds, yet there are interchanges. For example the question may be raised whether there are rules of **public** international law limiting the jurisdiction of the courts in civil trials" (i.e. the latter being a rule of private international law). For the following it is important to note that the concept of **jurisdiction** under public international law includes (at least) two elements, the first of which is "**Legislative**" jurisdiction which "denotes the power of an individual state under international law to enact laws and regulations" (see Slot and Grabandt at 546) and the other is "**Enforcement**" jurisdiction, "which denotes the power of a states under national law to enforce its legislation" (see Slot and Grabandt at 49). The first element (legislative jurisdiction) often boils down to the question "may states apply their law on an extraterritorial basis?", and therewith resembles and to a certain extent overlaps with the question of applicable law under **private** international law. Ignoring the qualifications given by Kuner, what Kuner in fact does in his publication is that he provides the definition of the concept of jurisdiction under **public** international law (see Kuner I, at 12-13), subsequently gives a summary of the traditional categories of jurisdictional basis also under **public** international law (both as to legislative and enforcement powers of states)(see Kuner I, at 17-23) and finally evaluates whether the **applicability regime** of the Directive (which constitutes a conflict rule under **private** international law) meets these **public** international law criteria (see Kuner II). This is in itself a worthy exercise and is in line with the question earlier posed by Slot and Grabandt (see citation above). Slot and Grabandt, at 557, elaborate on this question as follows (emphasis added): "Several concepts of **private** international law are relevant here. Their relevance arises because we are concerned with the legality of extraterritorial application of national laws as well as the scope of legislation and enforcement jurisdiction under **public** international law. The latter may include the law (…) concerning the power of national courts to hear cases with international connections, conflict of law rules (…), and recognition of foreign judgments. Similarly the question of which law to apply in such cases may be considered in the context of **public** international law jurisdiction." In other words: it is worth evaluating the rules on applicable law and jurisdiction under **private** international law against criteria of jurisdiction under **public** international law (insofar as the criteria for legislative jurisdiction are concerned). Kuner, however, makes matters very complicated by not distinguishing between the different concepts. Instead of straightforwardly evaluating Article 4 (as a conflict rule of applicable law under **private** international law) against the **legislative** jurisdiction criteria under **public** international law, he tries to argue that Article 4 is actually a rule of **jurisdiction** (using arguments related to jurisdiction of the DPAs and thus in the meaning of jurisdiction under **private** international law), this in order to justify that he evaluates this "jurisdiction" rule against the jurisdiction rules under public international law. To make the confusion complete he explicitly mentions that he will **not** focus on rules of applicable law (see quote above), while the only thing he does in his publication is evaluate the

4.7 National implementations

The national implementation laws show many divergent implementations of Article 28(4) and (6).[36] A cause for this may have been that some Member States prior to implementation of the Data Protection Directive already had enacted national data protection laws implementing Convention 108.[37] Convention 108 already contained explicit provisions on national data protection supervisory authorities and their competence, which were somewhat stricter.[38] A correct implementation explicitly providing that the

---

applicable law provision of the Directive against the legislative jurisdiction rules which overlap with the question of applicable law.

[36] See Douwe Korff, ed. (2010) "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Country Study A.3 – France," available at available at: http://ssrn.com/abstract=1638955, at 33-34. A variation is, for instance, provided by Article 51(1) of the Dutch Data Protection Act, which explicitly also provides for jurisdiction of the Dutch DPA in case the laws of another county of the EU apply, but only in case "the processing takes place in the Netherlands: "An Office of the Data Protection Commission has been established with the task to oversee the processing of personal data in accordance with the provisions laid down by and under the Act. The Commission shall also oversee the processing of personal data in the Netherlands, where the processing takes place in accordance with the laws of another country of the European Union."

[37] Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 28 January 1981 (**Convention 108**), to be found at <www.conventions.coe.int>. Countries that had already enacted national data protection laws prior to adoption of the Directive, closely following Convention 108 are Ireland, Spain, the UK and Portugal. See Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data," 80 Iowa L. Rev. 445 1994-95 , at 451.

[38] Pursuant to Article 14(1) Convention 108, the national supervisory authorities have competence to hear claims lodged by any person on violations of its **national** law. The supervisory authority therefore can only apply its own law to a dispute. This principle can for instance also be found in sections 7-14 of the UK 1998 Data Protection Act, which only grants enforcement powers to the Information Commissioner and the courts on the matters of compliance with the Act and not with the laws of another Member State. In Convention 108, the solution to remedy the fact that this would entail that individuals may have to address the supervisory authority of another Party to Convention 108, is that the individual must be provided the option to lodge his complaint with the supervisory authority of his own country, who will then act as an intermediary (the supervisory authority of the country of the individual therefore has competence to **accept** the claim, but not to **hear** the claim). See Article 14 Convention 108:
"**Article 14 – Assistance to data subjects resident abroad**
1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

applicable law may be different from the law of the forum is the Belgian data protection law.[39] Most other laws do not deal with this issue or seem to leave it to the general principles of their administrative procedural law to decide on issues of jurisdiction.[40] Though this may in many cases lead to the DPA having competence, it may mean that an individual will have to resort to the DPA of another Member State, which was not the intention of the Directive.[41] I therefore recommend that European legislators ensure a correct implementation of Article 28(4) and (6) of the Data Protection Directive.

4.8 Redress to the courts of the Member States

Article 22 Data Protection Directive ensures that individuals are provided in the Member States with the following remedies: "the right for every person[42]

---

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party."
See for a similar provision Article 1(2) of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows Strasbourg, 8.XI.2001, also to be found at <www.conventions.coe.int>.

39 Korff (n 12), at 96: "However, the question of "applicable law" is, also in this regard, separate from the issue of forum. As the Belgian law makes clear, the courts of EU Member States may be called upon, in this respect and more generally, to apply and enforce the law of another EU Member State, if that law of that other State is the "applicable" law in respect of the processing in question.

40 Korff (n 12), at 96-97: "Most other laws do not deal with this issue, or leave it to the general principles of their legal system to determine the forum in this respect, but the principle set out in the Belgian law would still appear to be the most appropriate one: without it, data subjects would have to resort to foreign fora, which would be prohibitive."

41 See n 40.

42 Dammann and Simitris (n 7), at 259, comment in respect of the element "every person": "according to the Directive the right to a judicial remedy must be given to "every person", not just to the "data subject" (as defined in Article 2a). The Directive here chooses a broader term, as it did in respect of the right to file a complaint with the DPA in accordance with Article 28(4). In both cases this is with a view to the procedural situation. When filing the claim or complaint it is then possible to first establish whether the person is indeed affected. This broader wording does not change the fact that the Directive as a whole is directed at protection of rights of persons whose data are processed. Persons who cannot show such own involvement, do for that reason not need the guarantee of a judicial remedy." A more logical explanation for the fact that reference is made to "every person" rather than "data subject" is given by Peter Carey, Data Protection, A Practical guide to UK and EU law, Oxford University Press, at 157: "The reference in the Directive and the UK Act to "person", rather than to individual, in this context means that the right applies to companies as well as natural persons."

to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question".[43] The reference to a judicial remedy indicates that a claim may be filed through a "court" of the Member States.[44] The Directive does not prescribe which court; this is left to be decided by the Member States.[45] The Directive also does not describe which remedies. General opinion, however, is that a judicial remedy does not only concern a ruling on whether the breach occurred, but also includes the possibility to obtain mandatory or prohibitive injunctions (the former to order a defendant to do something; the latter to refrain from doing something, or to stop doing it).[46] Article 22 stipulates that the rights individuals enjoy are those of the "the national law applicable". As indicated before, this may be a different law than the law of the court.[47] Article 22 Data

---

43 "Article 22 - Remedies
Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question."

44 The German language version of the Directive is more explicit in this respect where it requires that "every person can file a claim through the court" ("jede Person (...) bei Gericht einen Rechtsbehelf einlegen kann"). See further Dammann and Simitis (n 7), at 260.

45 Dammann and Simitris (n 7), at 260: "Which type of court and which court should be chosen in the different cases, is to the discretion of the national law. The Directive just requires that a judicial remedy is available through a court."

46 Dammann and Simitris (n 7), at 260 (para. 5), come to this conclusion based on the fact that Article 22 "entails that **effective** remedies must be provided". Korff (n 12), at 96, notes that there is no specific guidance in the Directive and by the Working Party 29 on the precise form (or forms) that the remedy should take, but indicates that "in this respect it is instructive to look at the clarification issued by the EU on the somewhat weaker but still similar requirement in the "Safe Harbor" principle on enforcement, that there must be an "independent recourse mechanism" available to data subjects. In the Frequently Asked Questions (FAQs) on this principle, it is made clear that the mechanism must be able, in so far as feasible, to "reverse or correct" any effects of non-compliance, to ensure that future processing will be in conformity with the Safe Harbor principles, and where appropriate, that processing of the personal data of the individual who has brought the complaint will cease (FAQ 11). Clearly, mutatis mutandis these should also be the minimum requirements for effective judicial remedies under the Directive. They imply that courts, apart from awarding compensation, should also be able to issue injunctions in the relevant proceedings, ordering controller to either take specific action or to refrain from certain matters (injunctions are indeed expressly mentioned in Safe Harbor FAQ 11)."

47 Korff (n 12), at 95-96, notes that this is relevant as these rights (and the exceptions and derogations from those rights) differ per Member State. At 96, Korff further notes that Member

Protection Directive adds that the requirement of a judicial remedy is "without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Art. 28."[48] Article 23 Data Protection Directive ensured further a right to "compensation for any damage suffered by the individual as a result of an unlawful processing operation, or of any other act incompatible with the applicable national law."[49] Article 24 ensures that the Member States have laid down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.[50] The Data Protection

---

States "(at least in the opinion of the Article 29 Working Party) (…) are not entirely free to determine what kind of damage may provide a cause of action. This is again made clear in an assessment of the appropriateness of safeguards in the context of transborder data flows, specifically in its comments on the adequacy of sectoral codes of conduct in this regard. On this, the Working Party writes that: If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject. This remedy must put right the problem (e.g. correct or delete any inaccurate data, ensure that processing for incompatible purposes ceases) and, if damage to the data subject has resulted, allow for the payment of appropriate compensation. It should be borne in mind that "damage" in the sense of the data protection directive includes not only physical damage and financial loss, but also any psychological or moral harm caused (known as "distress" under UK and US law). (emphasis added) If this applies in that context, it should also apply to the implementation of the right to compensation in the national laws of the Member States", referring to Article 29 Working Party, Working Document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12 of 24 July 1998), p. 13).

48 Dammann and Simitris (n 7), at 260, comment that this element is included in Article 22 to make clear that the Member States "must offer both possibilities concurrently". They further note "that the Directive does not elaborate on how the procedural architecture should be. It does for example not forbid to restrict the access to the court if not first an administrative procedure has been completed, for instance the complaints procedure with the DPA. Relevant is only that the judicial remedy is available."

49 "Article 23 - Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage."

According to Korff (n 12), at 96, also the "the right to compensation under Article 23 (…) is to be granted under the "applicable law". This (…) is important, because (…) the laws in the Member States differ in this respect".

50 "Article 24 - Sanctions

Directive does not provide for jurisdiction rules for the courts in data protection cases.

The legislative history of these provisions (insofar as relevant here) do not provide relevant clarifications.[51] Other than specific references made in the footnotes, the same applies to the commentary of Dammann and Simitris.[52]

4.9 National implementations

All Member States allow for the possibility of individuals to seek redress, and corrective action, though the courts.[53] Due to the discretionary powers of the Member States in the implementation of the Directive, there are many different manners in which Member States have chosen to implement the requirement to provide for judicial redress.[54] However, under most national implementation laws, claims for damages have to be brought before the civil courts (either based on tort or on enforcement of a right *sui generis*)[55] and questions of when and which remedies, such as injunctions or damages are to be awarded, are left to the national law on administrative or civil liability.[56] As to jurisdiction, most Member States have left it to their courts

---

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive".

Dammann and Simitris (n 7), at 266 (para. 3), indicate that this provision also relates to the judicial remedies prescribed by Articles 22 and 23.

51 Other than that the basic provisions of Articles 22 – 24 were already included in the Initial Proposal, whereby the scope of Article 22 was broadened in the Amended Proposal. The Explanatory Memorandum (insofar as relevant here) does not contain any useful clarifications.

52 Dammann and Simitris (n 7), at 259-267.

53 Korff (n 12), at 96.

54 For an overview of the different manners in which the Data Protection Directive is implemented in the national laws of the Member States, see Douwe Korff, EC Study on implementation of the Data Protection Directive, Comparative study of national laws, September 2002, Human Rights Centre University of Essex, at 209, to be found at <http://papers.ssrn.com>.

55 Korff (n 54), at Chapter 13, discussing the different legal bases on which damages can be claimed, varying from the ordinary rules on civil and administrative liability rules in a country (as in Finland, France and Luxembourg) to liability in tort (as in Ireland and the Netherlands).

56 Korff (n 12), at 96. See, however, Bing 'Data protection, jurisdiction and the choice of law', Privacy Law and Policy Reporter, [1999] 65, at 9: "According to art 23, the Member States are obliged to 'provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered'. This is, therefore, an obligation under the Directive to include liability provisions for data protection violations, and in this way such provisions may be seen as being 'pursuant' to the

to decide jurisdiction based on their own rules of civil or administrative procedure[57] and the courts further apply their own procedural law. In data protection cases this means that the courts of the Member States will apply the Brussels I Regulation to decide their jurisdiction. It is outside the scope of this dissertation to discuss extensively the possible grounds for jurisdiction of the courts of the Member States in data protection cases. I will limit myself here to discussing briefly the two most common situations. The first is the situation where an individual has some form of contractual relationship with the controller. This will in most cases be a consumer contract or an employment agreement. The Brussels I Regulation provides for a consumer and employee protection regime which entails that in these cases the court of the place where the consumer is domiciled or the place

---

Data Protection Directive. This is, however, a somewhat formal argument. Clauses on liability for data protection violations are related to those applying to the invasion of privacy, which will often have, in national law, a sufficiently broad scope to include violations of the provisions introduced pursuant to the Directive. In my opinion, it may be somewhat artificial to construe such traditional provisions as being introduced pursuant to the Directive, and also apply the 'proper law of data protection' for the choice of law with respect to liability. But this is certainly one possibility for the interpretation of the Directive which should not be omitted." Bing at 10 further points out "that the law relating to liability might vary to a great extent between different countries. The European Directive art 23 requires that member countries implement provisions granting compensation for violations of the data protection provisions following the Directive. It is, however, unclear whether this requires member countries to ensure that there is compensation for non-economic loss, and the co-ordination is limited to this general requirement. There is diversity among countries in the law relating to liability, especially with respect to non-economic damage, which is the probable damage in privacy cases. For instance, many European countries require statutory authorisation to award such damages, while the Common Law countries have a less strict doctrine." Bing at 23, warns that "there may be an advantage in forum shopping in such instances".

57 Kuner (n 22), at 112; Bing (n 56), at 7. See also WP Opinion on applicable law (n 21), at 10: "The provisions of the Directive also determine the scope of applicability of the national laws of the Member States, but they do not affect the jurisdiction of national courts to decide relevant cases before them". See for the French courts: Korff (n 36), at 34. The French courts follow the general rules of the law of administrative and civil procedure in data protection cases. From the case study by Korff it appears that "[a]s far as non-criminal judicial remedies are concerned, the Law itself is largely silent [...] simply because in France, anyone whose rights or interests are or may be affected by unlawful action, such as processing in contravention of the data protection law, can in any case appeal to the courts for redress and/or compensation, also and in particular in speedy interlocutory proceedings (en référé). The "relevant judge" (the judge with competence to rule on the matter) differs according to the controller: Matters relating to processing by public bodies will be decided by the administrative courts; matters relating to processing by private sector bodies or individuals by the civil courts."

where the employee habitually carries out his work (which is often the place of his domicile) has jurisdiction.[58] The consumer and employee protection regime of the Brussels I regulation will be extensively discussed in Paragraph 12.5.

If the data processing is not in connection with a contractual relation, the jurisdiction basis available to individuals in the EU is (amongst others) Article 5(3) of the Brussels I Regulation, which provides for jurisdiction at the place where the "harmful event" occurred or may occur. The place where the harmful event occurred must be understood as covering two distinct connecting factors (used at the option of the plaintiff), namely "the place where the damage occurred" and "the place of the event giving rise to it".[59] In data protection cases, jurisdiction will be generally based on the first connecting factor (as this base generally leads to jurisdiction of the courts of the country of domicile of the individual).[60] The damage occurred may also concern "non-material damage"[61] (as will often be the case in data protection violations). What is required, however, is that the causal event "directly produces its harmful effects upon the person who is the immediate victim of that event". This entails that only the "initial damage" is jurisdictionally relevant, as opposed to the "financial damage following upon".[62] In data protection violations this requirement will be met in the country of domicile of the individual.[63]

---

58 Articles 16 and 19 Brussels I Regulation.

59 Arnaud Nuyts, "Suing At the Place of Infringement: The Application of Article 5(3) Regulation 44/2001 to IP matters and Internet Disputes, Chapter 6, in: International Litigation in Intellectual Property and Information Technology, Kluwer International [2008], at 115, referring to ECJ Case 21/76 [1976] ECR 1735 (*Bier*).

60 The second connecting factor is the "place at the origin of the damage". This may not necessary coincide with the country of the plaintiff (which would be the preferred forum). For instance in internet cases, the causal event will be the place of establishment of the person who uploads the data to the network (as opposed to the place of eventual downloading), see Nuyts (n 59), at 120-121.

61 Nuyts (n 59), at 117, and case law there referred to.

62 Nuyts (n 59), at 121, and case law there referred to.

63 Korff (n 12), at 97: "This also means that, normally, the domestic courts of the Member States will assume jurisdiction over actions by foreign controllers that are alleged to have caused damage or distress to claimants who are nationals or permanent residents of the State to which the court pertains."; Lee Bygrave, 'Determining applicable law pursuant to European Data Protection Legislation' [2000] 16 Computer Law and Security Report 252, at 256, who notes that the forum of the State in which the data subject has his domicile "would parallel existing European rules on jurisdiction and choice of law in case of consumer cases."; Bing (n 56), at 8: "applying this reasoning to data protection, it can be argued that the question whether the victim had an interest in his or her privacy in the country where he or she is domiciled or is

4.10 Evaluation of the overall jurisdiction regime

The jurisdiction regime of the Data Protection Directive does not lead to discernable issues in practice and no case law of the European Court of Justice is available.[64] One of the issues identified in the literature[65] is that in

---

residing (…) and it would seem to follow that the court of the country in which the data subject is domiciled or residing would also have jurisdiction according to the criteria of the (…) Convention". Peter P. Swire, Elephants and Mice Revisited: Law and Choice of Law on the Internet, University of Pennsylvania Law Review [Vol. 153: 2005], at 1982: "In the European Union, the revisions to the Brussels Convention have clarified the law for business-to-consumer transactions over the Internet: jurisdiction will generally exist in the buyer's country, and judgments from that country will generally be enforced in other European countries, referring to: Cindy Chen, Comment, *United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce*, *25 U. PA. J. INT'L ECON. L. 423 (2004).*

64 Korff (n 12), at 98, reports that the theoretical issues he raises in respect of jurisdiction and applicable law have not "yet arisen anywhere in the EU" and further reports that "litigation in the courts by ordinary citizens is extremely rare". Kuner I (n 23), at 1, however, notes that "As the global economy has become more interconnected and the Internet ubiquitous, jurisdictional conflicts involving States, private actors, and regulatory agencies are becoming increasingly common. States also frequently assert their jurisdiction over conduct occurring outside their own territory, particularly with regard to conduct on the Internet". So far, however (as noted by Korff), jurisdiction issues are limited to the rare case (if any). An interesting publication in this respect is Swire (n 63), at 1975-2001. In an earlier publication (Swire (n 22), Swire described 11 areas where choice-of-law issues might arise on the Internet. Swire in his sequel (n 63), at 1975, however, observes the following: "every encounter in cyberspace (…) raises the possibility that diverse laws will apply" and that the "rules for choosing among diverse laws (…) thus appear uniquely important for cyberspace. Surprisingly the number of actual cases addressing choice of law on the Internet is far, far lower than the initial analysis would suggest. Although there is the possibility of diverse national laws in every Internet encounter, some mysterious mechanisms are reducing the actual conflicts to a handful of cases." He subsequently explains the mechanisms that reduce the actual conflicts. See at 1976, where Swire summarises the mechanisms:
"Four significant filters exist before a court must choose among conflicting national laws: technology's ability to trump law; lack of jurisdiction over defendants; the harmonization of diverse laws; and the existence of self-regulatory and other systems that suppress choice-of-law conflicts for transactions. Swire's explanation why there have been few cases in the **data protection area** is the following: "The 1998 article had an extensive discussion of choice-of-law issues under the European Union Data Protection Directive. That discussion highlighted the potential that E.U. Member States would interpret Article 4 of the Directive broadly, to apply even to websites in the United States and elsewhere that did not sell any products inside the E.U. Although there has been no formal statement by regulators forswearing that broad reading,

cross-border cases the situation may arise that a DPA or national court will have to apply the data protection law of another Member State. Due to the many differences between the implementation laws of the Member States[66], issues may arise "if a 'foreign applicable' law were to provide less rights, or wider exceptions, than are provided for in the domestic law of the country concerned."[67] As the right to data protection is a fundamental human right and freedom,[68] and the basis for the Data Protection Directive is to implement these rights and ensure a high level of protection,[69] a number of Member States have chosen the constitutional approach to implementation of the Data Protection Directive[70] or have otherwise provided that their data protection laws are of a mandatory nature.[71] The courts and DPAs of these countries will in all probability apply in such circumstances their own rules as *ordre publique*.[72] The issue of lack of harmonisation of the data protection

---

actual enforcement has not been nearly so broad. Instead, I believe that all of the privacy enforcement actions by E.U. Member States have been predicated on activity that took place within the E.U."

65 Korff (n 12), at 96.

66 See n 54.

67 Korff (n 40), at 96

68 See para. 7.1, in particular n 3 and further para. 12.3.2

69 See Recitals 10 and 11 of the Data Protection Directive.

70 See Korff (n 54), at Chapter 13. Korff lists the Member States (most notably Germany, Spain, Greece, Italy, Portugal and Austria) that have chosen the constitutional approach to implementation of the Data Protection Directive. See also Bert-Jaap Koops, "Conclusions and Recommendations," in: *Constitutional Rights and New Technologies: A Comparative Study*, ed. Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul (The Hague: Asser Press, 2008), p. 271 et seq.), where Koops points out that it is a trend of the past years – either directly, or in the context of the right to privacy, or value of dignity - to recognize the right to data protection as a part of the national constitutional heritage of most Member States.

71 See for instance the legislative history to the Dutch Data Protection Act, Kamerstukken II 1997/98, 25 892, nr. 3, at 10.

72 See in more detail para. 12.3.1, in particular n 22. Korff (n 12), at 96. See also at 98: "We believe that if an issue came before the courts in (say) Germany (or Spain, or Italy) in which, on the basis of the "applicable law" rules, a foreign law (say, the UK Data Protection Act) applied, and if that law failed (from the domestic point of view of the court) to adequately protect such a constitutional right, the domestic court would refuse to give effect to the foreign law - and thus to the "applicable law" rules in the Directive. Specifically, especially also in the light of other rulings on transnational matters - such as rulings by courts in Germany, France and elsewhere on the sale of Nazi memorabilia over the Internet or on holocaust denial websites - it would not be surprising if courts in EU Member States were to issue mandatory or prohibitive injunctions against foreign controllers, including controllers in other EU Member States, in order to protect the constitutional rights of their own citizens." See also Yves Poullet, Jean-Marc Van Gyseghem,

laws in the Member States is a well known issue[73] that the European Commission intends to remedy.[74] If the laws are adequately harmonised, this issue will solve itself. This also applies to other well known issues such as the fact that the enforcement powers of the DPAs have not been adequately harmonised at the right level.[75] For these issues I refer to Paragraph 10.6.5, where I propose to achieve the required harmonisation of EU data protection law by replacing the Directive by an EU regulation in the upcoming revision of the Directive, or, as a next best alternative, to confer the implementing powers in respect of a revised Directive to the European Commission.[76] I will here limit myself to recommending that EU legislators

---

Jean-Philippe Moiny, Jacques Gerard, and Claire Gayrel "Data Protection in the Clouds" in *Computers, Privacy, and data Protection: an Element of Choice*, Serge Gutwirth, Yves Poullet, et al, eds., at 401-402, pointing out that the applicable law may be determined under the so-called 'public order exception clause' "compelling judges to apply national law in some specific cases or when the application of a foreign law leads to unwanted results."

73 It is generally acknowledged that the main shortcoming of the current EU data protection regime is that the level of harmonisation achieved by the Data Protection Directive is unsatisfactory due to (i) the fact that the Directive leaves the Member States too much discretion in implementing its provisions (see Recital 9 of the Data Protection Directive); and (ii) the many instances of incorrect implementation by the Member States. This was already the conclusion of the First implementation report on the Directive, see Commission of the European Communities, First Report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final (**First Report on the Data Protection Directive**), at 11 and action point 6 at 24. See for the same conclusions WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, as adopted on 1 December 2009 (**WP Contribution on The Future of Privacy**), at paras. 18 – 21; and the European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union" (**EDPS Opinion on the revision of the Directive**), at 7 and 12.

74 The European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union,' COM(2010) 609/3 (4 November 2010) (**EC Communication on the revision of the Directive**), at 10.

75 Which also has to be remedied, see on this topic and my recommendations in this respect para. 2.11.

76 Which the European legislators are empowered to do pursuant to Article 291(1) of the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**).

ensure that the jurisdiction regime of the Directive is harmonised in the upcoming revision thereof.

Recommendation 4 Ensure the harmonisation of the jurisdiction regime of the Data Protection Directive.

4.10.1 Country-of-origin principle also extends to jurisdiction

The issue of lack of harmonisation of EU data protection law, also especially presents problems because the applicability regime of the Data protection Directive often results in more than one law being applicable to a data processing (see Paragraph 2.3.6). This issue will be solved if the country-of-origin principle is introduced also for data protection (as per R*ecommendation 2*).[77] As a result of introduction of the country-of-origin principle, one law will apply to, for instance, the cross-border data processing activities of a multinational with establishments in the EU. The law applicable would preferably be the law of the EU headquarters of the multinational (the company having control in the EU of all data processing operations of such multinational). Introduction of the country-of-origin principle also has consequences for the jurisdiction regime of the Directive. In the example above, the DPA of the EU headquarters will have central supervision powers and the other DPAs must assist the DPA and courts of the country-of-origin.[78] This is a form of integral enforcement which will require that the DPA of the country-of-origin of the multinational has supervisory powers to the detriment of other DPAs (i.e. such other DPAs will have to relinquish their supervisory powers as to the secondary establishments in their respective territories). In return such other DPAs obtain central enforcement in respect of the processing activities of multinationals that have their primary establishment in such DPAs' respective territories. To avoid uncertainty in respect of the effect of the introduction of the country-of-origin principle also on jurisdiction of the DPAs, I recommend that EU legislators, when revising the Directive, make explicit that introduction of the country-of-origin principle leads to central jurisdiction of the DPA of the country-of-origin.

77 See para. 2.11.

78 See also Article 19 E-Commerce Directive.

Recommendation 5
Provide that the DPA of the country-of-origin of the controller will have jurisdiction.

In Paragraph 2.10.5, I indicated that in this context thought also has to be given to whether introduction of a country-of-origin principle should also apply to the rights of data subjects, or that data subjects should keep their rights under their national law (as suggested by one author).[79] This is a moot point if the rights of data subjects are properly harmonised and a proper cooperation is ensured between the DPAs in the event of complaints. This will provide a better solution than excluding the rights of data subjects from applicability of the country-of-origin principle altogether.

As discussed in Paragraph 2.11, the country-of-origin principle will become superfluous if the Directive is replaced by an EU regulation. An EU regulation will be directly applicable in all Member States and will not have to be implemented in the national laws of Member States. If there is one uniform EU data protection law, a rule providing that the law of the country-of-origin is applicable is obsolete. Insofar as jurisdiction of the DPAs is concerned, the country-of-origin principle, however, will still have relevance. Multinationals with more establishments in the EU will still have an interest in, for instance, being able to comply with notification or permit requirements under EU data protection law in their country-of-origin only. The same applies for the possibility of central enforcement in respect of the data processing operations of such multinationals. *Recommendation 5* will therefore also have relevance if the Directive were to be replaced by an EU regulation.

4.11 Evaluation of the jurisdiction regime against international jurisdiction principles under public international law

An evaluation of the jurisdiction regimes of the courts of the Member States is outside the scope of this dissertation. Looking at the jurisdiction regime for the DPAs, evaluation is made difficult by lack of any reference points in the international data protection arena. The Data Protection Directive is "the

[79] See J.H.J Terstegge, 'Home Country Control – Improving Privacy Compliance and Supervision', [2002] P&I at 258: "However, not all legal requirements should be exported to other member states. The rights of the data subjects should at all times be addressed under the national law of the subsidiary which collected the personal data or which is responsible for managing the relationship between the company and the data subject."

first and only set of rules in an international data protection instrument to deal specifically with the determination of applicable law" and jurisdiction.[80] This is not because the issue has been "overlooked", but because it was difficult to address or reach consensus on. In Paragraph 4.6, I already noted that the jurisdiction and applicable law provision was dropped in the final version of the Madrid Draft Proposal for International Standards.[81] Also at the time the OECD Privacy Guidelines[82] were adopted in 1981, consideration was given to applicability and jurisdiction, but no principles were formulated, see Explanatory Memorandum to the 1981 OECD Privacy Guidelines:[83]

> "The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions."

Since this statement in 1981, not much progress has been made or may be expected any time in the near future. In 2010, the Hague Conference on Private international Law published a Note on Cross-Border Data Flows and

---

80 Bygrave (n 63), at 252.

81 The Permanent Bureau Hague Conference on Private International Law (a treaty drafting body with 62 member states), was invited to the Madrid Conference where the Madrid Draft Proposal for International Standards (n 31) was adopted. The Permanent Bureau gave a presentation at the Madrid conference on "determining the applicable law in a global world", which apparently lead to the dropping of Article 25 on jurisdiction and applicable law in the final version. See Hague Conference on Private International law, Cross-Border Data Flows and Protection of Privacy, Note submitted by the Permanent Bureau (13 March 2010), to be found at http://www.hcch.net/upload/wop/genaff2010pd13e.pdf (**Note Hague Conference on Cross-Border Data Flows and Protection of Privacy**), at 10: "It is important to note that these provisions had to be removed from the final draft put forth at the Madrid Conference, suggesting that the development of a solution to jurisdictional and applicable law questions is not yet readily apparent ".

82 Recommendation of the OECD Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) (OECD Privacy Guidelines), to be found at www.oecd.org.

83 Organisation for Economic Co-Operation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981), at 35.

Protection of Privacy.[84] In respect of "possible co-ordination of these laws by means of private international law mechanisms", the Hague Conference concluded that:

> "almost 30 years later [counted from the date of the Explanatory Memorandum to the 1981 OECD Privacy Guidelines] States have made relatively little progress to identify an acceptable solution to cross-border transactions involving personal data. It is, admittedly, a very difficult issue that has not become easier to address over time but is rather becoming more acute in light of the growing importance of data processing in the global economy."[85]

Under the heading "Going forward?", rather than suggest solutions, the Hague Conference just states that:[86]

> "Cross-border data protection issues can be addressed from a private international law angle. For example, there is indeed a need to determine how to allocate jurisdiction for protection of privacy in cross-border data flows or which data protection law applies to a particular act of data processing. Concerns about an extraterritorial application of data protection laws and its effects on the recognition and enforcement of decisions abroad have arisen."

In its Conclusions[87] the Hague Conference subsequently just states that "this is an area of law where international co-operation and co-ordination for cross-border cases may be a way forward" and that the Hague Conference is willing to offer assistance with a view to:

- "Identifying possible uncertainties on the applicable law to cross-border data flows necessary to the application of Hague Conventions.
- Assessing the feasibility of tools already successfully implemented by the Hague Conference on transnational co-operation and co-ordination in other contexts as models for cross-border data flow questions.
- Contributing to the ongoing debate whether additional multilateral efforts are feasible and/or desirable and whether it would bring added advantages with respect to existing instruments."

---

84 See n 81.

85 Note Hague Conference on Cross-Border Cata Flows and Protection of Privacy (n 84), at 6.

86 Note Hague Conference on Cross-Border Cata Flows and Protection of Privacy (n 84), at 8.

87 Note Hague Conference on Cross-Border Data Flows and Protection of Privacy (n 84), at 10-11.

> The challenge of drafting international jurisdiction principles is not specific to data protection. Similar jurisdiction issues are encountered in respect of any national right due to the fact that there is no global convention on jurisdiction and the enforcement of a national right in other jurisdictions or for recognition and enforcement of court decisions in other jurisdictions.[88] In 2010 the first in-depth publication on jurisdiction issues in the data protection arena was published, but also this study does not provide for concrete proposals but merely concludes:[89]

---

[88] Illustrative of this is the fact that the Hague Conference has (after more than a decade of work) ceased working on a new Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgements in Civil and Commercial Matters. For the relevant texts and status', see <www.hcch.net>. Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, TILT Law & Technology Working Paper No. 016/2010, October 2010, Version 1.0, at 10, to be found at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483, at 43, comments that it is unrealistic to expect such cross-border enforcement treaties to be forthcoming in the area of data protection as countries recently refused opportunities to enact global legal instruments protecting consumers in electronic commerce. See also Kuner I (n 23), at 16: "In 1999 the Hague Conference on Private International Law considered the issue of jurisdiction and applicable law in data protection in the scope of its 'Geneva Round Table on Electronic Commerce and Private International Law'. However, this work merely resulted in a statement that the subject required further study (referring to "Press Release, Geneva Round Table on Electronic Commerce and Private International Law, http://cuiwww.unige.ch/~billard/ipilec/pressre.html). Swire (n 63), at 1988-1989, gives some background to the breakdown of talks within the Hague Convention: "Particular controversy has accompanied Article 7 of the proposed Convention. Negotiators have put forward a number of variations that seek to compromise between the country-of-destination rule (favoured by European countries and consumer advocates) and rules that give more weight to the seller's country of origin (favoured by the United States and e-commerce companies). One area of possible eventual compromise would be to give country-of-origin treatment to transactions where the seller does not have notice of the location of the buyer. Until this issue is resolved, it appears highly unlikely that there will be formal harmonization for jurisdiction and enforcement of judgments."
See also Corien Prins "Should ICT Regulation Be Undertaken at an International Level?", in Bert-Jaap Koops et. al. (eds.), Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners (TCM Asser Press 2006), at 15.

[89] Kuner II (n 23), at 15. Though Kuner uses the term "jurisdiction", I note that he in fact has evaluated the applicability regime of Article 4 of the Directive rather than Article 28 Directive (see on this n 35). Having studied his publication, I think, however, that his conclusion would be the same as to Article 28 Directive.

> "Data protection law is a combination of so many legal areas, and the differences between different regional and national approaches are so significant, that it would be futile to search for an all-encompassing rule to fit all possible jurisdictional situations. It is also likely to be futile to suppose that every jurisdictional basis for data protection law could be exclusive, i.e., that there should always be one place of jurisdiction to the exclusion of all others. Rather, the broad nature of many important concepts in data protection law, together with the fact that data processing on the Internet has become ubiquitous, means that it is to be expected that there may be several grounds for asserting jurisdiction over a particular act of data processing, and several States that assert such grounds. The key is to find a method of allowing such multiple jurisdictional assertions to co-exist, and of finding a way to measure their international legality."

Despite the lack of reference to other data protection regimes and international guidance in this arena, however, some general starting points for evaluation of the jurisdiction regime for the DPAs can be formulated. First, as a rule of thumb, the jurisdiction regime of the DPAs should preferably be more or less aligned with that of the courts in data protection cases, and if this is not the case, there must be well-reasoned grounds why this is justified. In the second place, it is worth looking at the jurisdiction principles under public international law (and then in relation to **enforcement** jurisdiction)[90], in particular to verify whether the jurisdiction of the DPAs does not prove "exorbitant". As one author puts it: "[t]he examination of 'exorbitant' jurisdiction is particularly illuminating, since by examining forms of jurisdiction which may be excessive, improper, or unreasonable, insights can be gained into appropriate jurisdictional principles".[91]

4.11.1 Aligned with jurisdiction of courts?

The rule that individuals can file a complaint with **any** DPA entails in practice that individuals file complaints with the DPA in their own country. This results in a similar outcome when courts apply the Brussels I Regulation, which in most cases also leads to jurisdiction of the courts of the country of domicile of the individual (see Paragraph 4.9). There is one exception. Complaints can also be filed by persons not domiciled in the EU

---

[90] See n 35. See further Kuner I (n 23), at 5: "While public international law only applies directly to relations between States, its role as the basic limiting standard of the international legal order provides the testing ground for jurisdictional rules affecting private parties in different States as well."

[91] Kuner I (n 23), (n 24), at 5.

(non-EU persons). If the controller is established in the EU, this is still in line with the jurisdiction of the courts, as persons domiciled in a Member State may always be sued before the court of that place. However, it is also conceivable that a non-EU person files a complaint with the DPAs about violation of his rights under EU data protection law by a controller who is not established in the EU. Courts would in that case only have jurisdiction if the damage occurred in its Member State. As non-EU persons will to all probability not be aware of the possibility to sue a non-EU company before the courts of a Member State (or of their rights under EU data protection law for that matter), this possibility has not had discernable relevance in practice. Nevertheless, this basis for jurisdiction cannot be said to be fully aligned with the jurisdiction rules of the courts. The background of the broad jurisdiction of the DPAs is that the Data Protection Directive protects fundamental human rights, which rights should be afforded to any person regardless of his nationality.[92] Whether this is an adequate reason for this broad jurisdiction basis is discussed in the next paragraph on exorbitant jurisdiction.

4.11.2 Exorbitant jurisdiction?

"Exorbitant jurisdiction" is one of the terms used to designate assertions of jurisdiction which are considered to be improper or excessive.[93] The Hague Conference gives the following definition: "jurisdiction is exorbitant when the court seized does not possess a sufficient connection with the parties to the case, the circumstances of the case, the cause or subject of the action, or fails to take account of the principle of the proper administration of justice."[94] In the case of Article 28, the only requirement for a DPA to have jurisdiction is that EU data protection law applies. The individual filing the complaint may be a non-EU person, the controller may be established outside the EU and the data processing itself may take place outside the EU. In Chapters 2 and 3, I discussed that in this virtual world of "big data", this may well be justified, provided the connecting factor for applicability of the Data Protection Directive is based on "virtual territoriality" and not on an unbridled application of Article 4(1)(c) (as presently applied by the Working Party 29). This is an example where rules on applicable law and jurisdiction are interrelated (i.e. if Article 4 is given a broad scope of protection, the

---

92 See on this Paragraph 2.3.7.

93 Kuner II (n 23), at 1-2, gives an overview of the different labels and definitions used in literature.

94 Hague Conference on Private International Law, International Jurisdiction and Foreign Judgments in Civil and Commercial Matters, October 1997, Report drawn up by Prof. Catherine Kessedjian, at 40, http://www.hcch.net/upload/wop/jdgm_pd7.pdf.

scope of Article 28 expands correspondingly) and justifies the comments in the literature that regimes of applicable law and jurisdiction become more difficult to distinguish especially in the online world.[95] This being said, both regimes still have to be evaluated in their own right and cannot be treated or evaluated as one blended concept.[96] In particular, the question that has to be answered here is, if the applicability regime of the Directive is amended as per my *Recommendation 3*, does the jurisdiction basis of Article 28 Directive then (still) constitute "exorbitant jurisdiction"? At first sight the conclusion seems to be that indeed Article 28 seems exorbitant, where it provides for jurisdiction of the DPAs to hear complaints of also non-EU persons against non-EU controllers (see Paragraph 4.11 above). Looking, however, in more detail to which cases Article 28 would be applied in practice, my conclusion is that Article 28 cannot be qualified as exorbitant, again provided that Article 4 is amended as per *Recommendation 3*. Article 4 (as revised) leads to application of EU data protection law:

(i) if the controller processes data in the context of activities **in the territory** of a Member State; or
(ii) if the controller processes data in the context of activities **directed** at the Member State.

If a controller has relevant activities in the Member State (i.e. has an establishment there),[97] and in that context processes data of a non-EU person, jurisdiction of the DPA to hear a complaint of such non-EU person is based on the **territoriality principle**. This is the main and most accepted jurisdiction basis and (as discussed in Paragraph 4.11) would also provide for jurisdiction of the courts and can thus not be qualified as exorbitant. The second connecting factor (the activities of a controller are **directed at the territory**), is based on the effects doctrine, which is more disputed, but is

---

95 Kuner Part I (n 23), at 5, referring to: "F.A. Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 Recueil des Cours de l'Académie de Droit International 9, reprinted in F A Mann, Studies in International Law (Clarendon Press Oxford 2008) 1, at 11, 12, stating that there is a 'deep doctrinal link' between jurisdiction and conflict of laws, and the two areas are 'complementary'; Dan Jerker B. Svantesson, Private International Law and the Internet (Kluwer Law International 2007) 1, at 7, stating that 'the choice of forum determines which court will adjudicate the matter, which in turn decides which choice of law rules will apply, which in turn determines the applicable law, and the substantive law being applied determines which party will win the dispute'; Restatement of the Law (Third), The Foreign Relations Law of the United States (American Law Institute Publishers 1987), vol 1, 237, stating 'in a number of contexts the question of jurisdiction to prescribe resembles questions traditionally explored under the heading of conflict of laws or private international law'.

96 This is in fact how Kuner approaches the concept of jurisdiction (see n 35), which is my main criticism in respect of his publication.

97 See para. 2.5.2.

becoming more common (see in more detail Paragraph 3.12).[98] However, the second connecting factor will in the case of a non-EU person not lead to jurisdiction in the EU as the relevant non-EU person is not physically present in EU territory (but only his data). As a consequence the processing of his data cannot be considered to be "in the context of activities directed at the EU. Article 28 leads in these cases therefore not to jurisdiction of the DPAs as EU data protection law does not apply to the processing of the data of such non-EU person in the first place.

4.12 Does the jurisdiction regime provide for meaningful redress?

That the jurisdiction regime of the Data Protection Directive does not require change or does not lead to discernable issues in practice, does not mean that the jurisdiction and enforcement system (thus) provides for effective cross-border enforcement in practice.

To the contrary, despite the fact that (i) individuals have broad legal rights and remedies; and (ii) DPAs have broad jurisdiction and enforcement powers, the conclusion 16 years after adoption of the Data Protection Directive is that the current enforcement regime does **not** lead to data protection compliance in practice[99] or meaningful redress for individuals.[100] Rather than discussing these issues here in the context of the jurisdiction

---

98 See in particular footnote 101.

99 Korff (n 54), at 209, notes that "the powers now vested in the data protection authorities, as currently exercised, have not been able to counter continuing widespread disregard for the data protection laws in the Member States." See further Rand Europe, Review of the European Data Protection Directive, Technical Report dated May 2009 (**Rand Report**), at 35; and Omer Teme, "For Privacy, The European Commission Must Be Innovative", Center for Democracy & Technology, 28 February 2011, to be found at http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative: "Enforcement is a sore issue for the EU DPD. It is an open secret that the framework is largely not enforced."

100 Korff (n 12), at 98 notes: "Indeed, and we may end this sub-section on this, it appears that litigation in the courts by ordinary citizens is extremely rare. In the UK, the case of Naomi Campbell, briefly set out in section 2.3(b), above, was the first case ever in which compensation was awarded over breaches of data protection law, but remains a very rare case. In other countries there may be more actions, but in most, the cost and effort of formal court proceedings deter most potential claimants. In our Final Report, we will examine if this can be and ought to change. We believe that, especially in the light of the weakness of enforcement by the data protection authorities (as noted in the next sub-sections), possibilities for empowering ordinary citizens should be further explored. We will examine why class actions are still extremely rare in Europe, also on data protection issues, and whether other, non-EU countries have more effective systems of this kind in place."

regime of the Directive (as indicated in my Research Objective for Part I), I have chosen to discuss the specific issues encountered by individuals in the cross-border enforcement of their data protection rights in Paragraph 8.3. The reason is that these cross-border enforcement issues are better understood after a discussion of the challenges posed by the current global data protection regulatory landscape, and a discussion of recent trends and developments which have relevance for data protection. In that Chapter similar cross-border enforcement issues are also discussed as encountered in other areas of law, like consumer protection law. In Paragraph 8.4, I subsequently discuss three possible (partial) solutions to address the cross-border enforcement issues encountered by individuals. One of the solutions is a choice of law and forum in transnational private regulation (such as BCR). How in BCR the applicable law, supervision and enforcement regime may be set up to address these issues is the main topic of Part II of this dissertation (and extensively discussed in Chapter 12).

4.13 Conclusions

Other than a lack of harmonisation, the present jurisdiction regime of the Data Protection Directive does not pose many issues, provided that the applicability regime is amended as per my Recommendations set out in Chapter 2. To ensure that the jurisdiction regime is also aligned with the country-of-origin principle, it is advisable to make explicit that the introduction of the country-of-origin principle leads to central jurisdiction of the DPA of the country-of-origin of the controller. If the Directive is replaced by an EU regulation, the county-of-origin principle becomes superfluous as far as the applicability regime is concerned, but remains relevant insofar as the jurisdiction of the DPAs is concerned. *Recommendation 5* will therefore also have relevance if the Directive were to be replaced by an EU regulation.

Recommendation 4
Ensure an adequate harmonisation of the jurisdiction regime of the Data Protection Directive.

Recommendation 5
Provide that the DPA of the country-of-origin of the controller will have jurisdiction.

5 Conclusions and assessment of Hypotheses Part I

The overall conclusion of Part I is that the especially the applicability regime of the Directive does not cater for the issues presented by the increasing cross-border nature of data processing in the age of "big data". The applicability regime has to be revised to (i) avoid unnecessary cumulation of laws applicable to a data processing activity; (ii) avoid gaps in the protection; (iii) avoid an unbridled application of the Data Protection Directive to data processing by non-EU websites; and (iv) avoid an unbridled application of the Directive to data processed by EU processors on behalf of foreign controllers (without any link to the EU other than the use of an EU processor). An unnecessary cumulation of applicable laws may for EU controllers be avoided by introduction of the country-of-origin principle (as per *Recommendation 2*). If the Directive is replaced by an EU regulation, the country-of-origin principle will become superfluous. The other issues may be addressed by following *Recommendations 1 & 3*. These changes should not be achieved by way of further opinions of the Working Party 29, but by a revision of the Data Protection Directive, which should preferably take the form of an EU regulation or, as the next best alternative, confer in the revised Directive the implementing powers in respect of such revised Directive on the Commission. As far as the jurisdiction regime is concerned, there is lack of harmonisation (which is addressed by *Recommendation 4*), but this does not seem to lead to discernable issues in practice. The jurisdiction regime has to be aligned with the introduction of the country-of-origin principle (see *Recommendation 5*). If the Directive is replaced by an EU regulation, the country-of-origin principle will still be relevant for the jurisdiction regime. The current jurisdiction regime, however, does not lead to meaningful redress for individuals in practice, but will be further discussed in Part II and has not led to recommendations here.

Evaluating the results of my research from the perspective of the Hypotheses I formulated at the start, I conclude as follows:

> ***Hypothesis 1***
> *The present applicability regime of the Data Protection Directive is not adequately harmonised and on the one hand leads to gaps in the protection of personal data (Article 4(1)(a) Data Protection Directive) and on the other hand to an arm's length scope which has little hope of enforcement (Article 4(1)(c) Data Protection Directive).*

Conclusion Hypothesis 1
My conclusion as to Hypothesis 1 is that the applicability regime of the Data Protection Directive is indeed presently not sufficiently harmonised and on the one hand leads to gaps in the protection and on the other hand to an arm's length scope with little hope of enforcement. If *Recommendations 1 & 3* are followed, these issues will no longer present themselves. If Recommendation 2 is followed, an unnecessary cumulation of applicable laws to data processing by controllers established in the EU will further be avoided.

> ***Hypothesis 2***
> *The present jurisdiction regime is adequately harmonised, does not lead to gaps in enforcement or "exorbitant" jurisdiction, but does not provide for meaningful redress in practice.*

Conclusion Hypothesis 2
My conclusion as to Hypothesis 2 is that, other than as assumed in the hypothesis, the jurisdiction regime is presently not adequately harmonised. If *Recommendation 4* is followed this will no longer pose a problem. The jurisdiction regime, however, indeed does not pose gaps in enforcement and if the applicability regime of the Data Protection Directive is amended as per *Recommendations 1-3*, the jurisdiction regime also does not lead to "exorbitant" jurisdiction. The assumption that the jurisdiction regime does not provide for meaningful redress is correct, but will be further discussed in Part II and will not lead to recommendations here.

Overview of Recommendations to EU legislators

Recommendation 1 Ensure an adequate harmonisation of the applicability regime of the Data Protection Directive.

Recommendation 2 Introduce the country-of-origin principle in the revised Data Protection Directive.

Recommendation 3
Delete Article 4(1)(a) and (c) Data Protection Directive and instead provide that the data protection law of a Member State applies:

- to the processing of personal data in the context of the activities of the controller in or directed at the territory of the Member State;
- and if the first ground is not applicable, to the processing of personal data in the territory of the Member State, but only insofar as it implements the obligations of a data processor to ensure that the data processing (i) is adequately secured in accordance with Article 17 of this Directive and (ii) provides for an adequate level of protection for the data processed within the meaning of Article 25(2) of the Directive.

Recommendation 4
Ensure an adequate harmonisation of the jurisdiction regime of the Data Protection Directive.

Recommendation 5
Provide that the DPA of the country-of-origin of the controller will have jurisdiction.

PART II BINDING CORPORATE RULES

6 Introduction

6.1 Data here, data there, data everywhere[1]

At the time of adoption of the European Data Protection Directive (1995)[2] the expectation was that the establishment and functioning of the European internal market[3] would lead to a substantial increase in cross-border flows of personal data between all those involved in economic activity **within** the EU Member States.[4] To facilitate a free flow of these personal data within the EU, the object of the Data Protection Directive was to achieve full harmonisation of data protection laws within the EU. [5] The wish to protect European data also if transferred outside of the EU resulted in a prohibition

---

1 "The Data Deluge: Businesses, governments and society are only starting to tap its vast potential", The Economist, 25 February 2010. The Economist reports that the world is currently undergoing an unprecedented 'information explosion', which transforms our society into a 'data centred economy'. This phenomenon is coined by scientists and computer engineers as 'big data': "Everywhere you look, the quantity of information in the world is soaring. According to one estimate, mankind created 150 exabytes (billion gigabytes) of data in 2005. This year, it will create 1,200 exabytes. Merely keeping up with this flood, and storing the bits that might be useful, is difficult enough. Analysing it, to spot patterns and extract useful information, is harder still. Even so, the data deluge is already starting to transform business, government, science and everyday life (...). It has great potential for good—as long as consumers, companies and governments make the right choices about when to restrict the flow of data, and when to encourage it."

2 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31 (**Data Protection Directive**).

3 The legal basis for the Data Protection Directive is Article 95 (formerly 100a) of the Consolidated Version of the Treaty establishing the European Community, [2002] OJ C325/1 (**EC Treaty**). See further Recitals 1 – 9 of the Data Protection Directive. The EC Treaty has been replaced by the Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/49 (**TFEU**). Article 95 EC Treaty is now Article 114 TFEU.

4 Recitals 5 and 6 of the Data Protection Directive. The Data Protection Directive also foresaw an increase in the exchange of personal data between companies as a result of the increase in scientific and technical cooperation and the introduction of new telecommunication networks in the Community, which would necessitate and facilitate the cross-border flow of personal data, see Recital 5 Data Protection Directive.

5 See Recital 8 Data Protection Directive, indicating that the purpose of the Directive was full harmonisation with the exception of specific discretionary powers in a limited number of areas (for instance it is left to the individual Member States to provide in which cases controllers are authorised to process sensitive data). See also Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, paras. 95-96.

of data transfers to non-EU countries[6] without an adequate level of data protection.[7] It is clear that the EU data transfer rules date from the time the internet was not yet widely used. The EU transfer rules were devised when transborder data flows were still typically point-to-point transfers (via fixed telecommunication lines), for instance if a company transferred an employee abroad to another group company and provided the employee's file and other employee records to such other group company or in the case of a cross-border takeover.[8]

---

6 The three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway) have ratified the Data Protection Directive in the EEA agreement (cf. Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, OJ L 296/41, of 23.11.2000). The free flow of information extends to these countries. References to the EU should be understood to include the EFTA countries, i.e. they also concern the European Economic Area (**EEA**).

7 Recitals 56 and 57 of the Data Protection Directive. See also European Commission, Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final, 15 October 1992, at 34, indicating that without restrictions on international data transfers, "the Community's efforts to guarantee a high level of protection for individuals could be nullified by transfers to other countries in which the protection provided is inadequate". See Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos 1997), at 270 (translation by the author): "The corresponding regulations have to guarantee that the protection guaranteed within the territory of the EU will not be nullified by a transfer to a territory, where there is no or no equivalent level of data protection."

8 Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*. TILT Law & Technology Working Paper No. 016/2010, October 2010, Version 1.0, at 10, to be found at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483>. See also Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169) at para. II.2, pointing out that "when Directive 95/46/EC was adopted, the context of data processing was still relatively clear and straightforward, but that is no longer the case "due to a growing tendency towards organisational differentiation, development of Information and Communication Technologies (ICTs), and globalisation. See further Vodafone, Privacy – an evolving challenge, to be found at http://www.vodafone.com/content/dam/vodafone/about/public_policy/future_ofprivacy/privacy_an_evolving_challenge_update.pdf, at 2: "Back in 1995, when the Data Protection Directive was adopted, only 18%1 of Europeans had access to a PC, and the percentage of people with a mobile phone in Europe was 4%2. Only 1%3 had access to the internet and, even within industry, IT use was relatively basic. People didn't have "online profiles"; indeed when it came to the use of personal information the individual was essentially passive. Large organisations, like banks, hospitals, government departments, were the only bodies with the capacity to process large amounts of information. This information was seldom shared as it was, in general,

The EU transfer rules prompted many non-EU countries to follow suit in adopting comprehensive data protection legislation in order for their companies to maintain access to the EU market.[9] Though these laws all regulate more or less the same subject matter, their governments have chosen substantially different solutions to do so. In the EU the rights of individuals in respect of processing of their personal data became a fundamental human right and freedom,[10] but in many other jurisdictions another form of protection was chosen. Also, there are still many countries with no data protection laws at all as well as countries (most notably the US) with a limited regime, where public regulation of data processing in the private sector is targeted at certain sensitive industries and further provides for data breach notification obligations in respect of specific categories of personal data only.[11] The result at present is a worldwide data protection regulatory landscape consisting of at best a patchwork of very diverse national data protection laws.

Though the Data Protection Directive foresaw an increase in data flows within the EU, the digital era has resulted in an unprecedented continuous **worldwide** flow of data both within multinational companies[12] as well as

---

kept in discrete segregated silos on local servers.", see Vodafone, Privacy – an evolving challenge, to be found at http://www.vodafone.com/content/dam/vodafone/about/public_policy/future_ofprivacy/privacy_an_evolving_challenge_update.pdf.

9 This puts the situation in a positive light. However, at the time of introduction of the Data Protection Directive, it was clear that the EU dictated its standard on the rest of the world based on the concept of reciprocity: EU personal data may only be transferred to a country that provides equivalent protection. Representatives from outside the EU argued that the Data Protection Directive thus had an improper extraterritorial effect and was protectionist. The complaints however did not stick and the export of the EU model has been very successful. Even the US capitulated by agreeing to implement the Safe Harbor Framework (see n 68 below). See also Corien Prins "Should ICT Regulation Be Undertaken at an International Level?", in Bert-Jaap Koops et. al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), at 172.

10 See e.g. Art. 16 TFEU and Art. 8 EU Charter of Fundamental Rights (annexed to the TFEU and legally binding for EU Member States since December 2009), both recognising the right to data protection.

11 See on data breach notification legislation in the US para. 9.3.

12 The term 'multinational company' refers to corporate enterprises with establishments across the world (typically in serveral or all continents). In literature, many acronyms are used such as MNCs (Multinational Corporations), MNEs (Multinational Enterprises) or TNCs (Transnational Corporations). For readability, I use only the term multinational.

with their external outsourcing service providers. Multinationals process personal data in the course of business.[13] Employee data are processed, for instance, for purposes of execution of the employment agreement (salary payment, performance evaluation, succession planning). Multinationals selling consumer products further process personal data of their customers. But multinationals involved in business-to-business transactions also process personal data of the contact persons within their suppliers, corporate customers and other business partners. Specific industries like the pharmaceutical sector may in addition process specific categories of personal data for instance in the course of performing scientific research involving patients. Due to the globalisation of the activities of these multinationals, these data are not relevant to one group company only (for instance, the group company employing the relevant employee), but are relevant to many other group companies. An example is performance evaluations and succession planning. Most multinationals have matrix organisations, which entails that their business is managed not so much on a country-by-country basis but per business unit, which may extend over many countries. It is therefore possible that the manager of an employee is not located in his own country. Evaluation of the employee's performance will then require a transfer of his performance data to the country of his manager and ultimately to central management of the relevant business unit, which may be located yet somewhere else. The same applies to supplier data. Multinationals more and more centralise their purchasing to achieve

[13] For a description of the magnitude of the recent worldwide explosion of data collection and sharing, see "A special report on managing information: Data, data everywhere. Information has gone from scarce to superabundant. That brings huge new benefits, but also big headaches," The Economist 25 January 2010, stating that "Wal-Mart, a retail giant, handles more than 1m customer transactions every hour, feeding databases estimated at more than 2.5 petabytes—the equivalent of 167 times the books in America's Library of Congress (...). Facebook, a social-networking website, is home to 40 billion photos. And decoding the human genome involves analysing 3 billion base pairs—which took ten years the first time it was done, in 2003, but can now be achieved in one week. All these examples tell the same story: that the world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly. This makes it possible to do many things that previously could not be done: spot business trends, prevent diseases, combat crime and so on. Managed well, the data can be used to unlock new sources of economic value, provide fresh insights into science and hold governments to account. But they are also creating a host of new problems. Despite the abundance of tools to capture, process and share all this information—sensors, computers, mobile phones and the like—it already exceeds the available storage space (see chart 1). Moreover, ensuring data security and protecting privacy is becoming harder as the information multiplies and is shared ever more widely around the world."

cost savings. This requires the centralisation of their supplier data which are subsequently shared with many other group companies.

Another development is that these transfers are no longer point-to-point but between multiple computers communicating through a private network or the Internet. Multinationals have further started to integrate their various local IT systems and now process their employee and customer data in central IT systems, which entails a continuous worldwide transfer of data between their group companies. These central IT systems may subsequently be outsourced to third-party service providers.[14] For cost reasons these service providers often provide their services from offshore locations outside the EU.[15] Such offshoring may involve transfers of the data of the multinational to all service centres of the outsourcing supplier in the countries involved. Transfers of data within the multinational and offshoring to third countries may be subject to a multitude of applicable data protection laws. The data transfer issues are further multiplied by recent technical developments such as dynamic routing[16] and cloud computing.[17] As a result of these developments it is no longer predictable how data will be routed over the internet and where the data will be ultimately stored. This proliferation of transborder data flows has triggered the application of the EU transfer rules on an unprecedented scale.

Multinationals (whether with headquarters within or outside the EU) find compliance with all applicable national data protection laws[18] a "challenge" as the present regulatory environment features many overlaps of applicable

---

14 For instance with server management, the outsourcing supplier hosts the servers of a customer on which the customer's IT applications operate (varying from HR to CRM applications).

15 Favourites include the 'BRIC' countries (Brazil, Russia, India and China).

16 Dynamic routing is the opposite of static routing, where data are processed through a network by a fixed path. With dynamic routing it cannot be predicted how data will be routed over the internet.

17 Cloud computing is defined by The National Institute of Standards and Technology (NIST) as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." <http://en.wikipedia.org/wiki/Cloud_computing - cite_note-5#cite_note-5>. The key characteristic of cloud computing is that the computing is 'in the cloud' i.e. the processing and the related data are not in a specified, known or static place. This is in contrast to a model in which the processing takes place in one or more specific servers that are known.

18 Kuner estimates that of the 192 Member States of the United Nations about 50-60 currently have a legal framework for data protection. See Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects", [2009] Computer Law and Security Review, 307, para III.

laws, which laws often vary or are even in outright conflict.[19] Many countries[20] have followed the EU in imposing restrictions on the outbound transfer of personal data from their territories. These restrictions require multinational companies to track and comply not only with the material data protection rules of each jurisdiction but also with all requirements relating to data transfers between specific countries.

The existing regulatory minefield in the data protection area has led many multinationals to implement worldwide corporate privacy policies.[21] These company-wide data protection rules aim to provide for a uniform adequate[22] level of data protection throughout the relevant group of companies rather than strive for compliance by the multinational on a country-by-country basis. The multinationals accept the risk of possible non-compliance with any stricter rules at the national level. Furthermore, given the administrative burden involved with complying with the various national transfer rules[23], most multinationals just ignore these transfer rules insofar as their intra-company transfers of personal data are concerned. They may also ignore the data transfer rules in the case of offshoring and the use of cloud computing.[24]

---

19 Even in the EU, where data protection laws are harmonised such conflicts do present themselves. For instance, in Germany it is required for employers to register the religious faith of employees (as employers pay church tax on behalf of employees), while in most other countries it is expressly prohibited to process the religious faith of an employee.

20 About 60 countries have some form of data transfer restriction. See for a comprehensive overview, see Kuner (n 8), at 55-89.

21 This is based on my observations as a practitioner advising multinationals on their worldwide data protection compliance. Part of the HiiL Program is to perform empirical research in this respect.

22 The term 'adequate' is not used in the meaning of Article 25(1) Data Protection Directive, but is here used to express that the multinational does not attempt to make the global policy compliant with all applicable national data protection laws in order to ensure compliance on a world wide basis. This would entail that the strictest provisions of all national laws would be cumulatively applicable throughout the world. The multinational therefore makes choices between different features of different systems to come to an overall adequate level of protection.

23 For the EU administrative requirements, see para 7.1.1 below, which include in many Member States authorisation of such transfers by the DPAs of the Member States from which the data are exported and notification of the data processing to the DPAs.

24 This is not only my own observation as a practitioner, but is confirmed by research performed on behalf of the European Commission, see n 26 and 27.

Data protection authorities in the various EU Member States (**DPAs**)[25] are well aware of the fact that multinational companies exchange personal data on a worldwide basis and outsource their IT to countries without an adequate system of data protection.[26] Practice shows that the enforcement tools of the DPAs are at present not sufficient to force compliance, whether due to lack of cooperation between national states, lack of enforcement tools at the disposal of the DPAs, lack of resources or the sheer volume of non-compliance.[27]

---

[25] References to the DPAs should be understood to include data protection authorities of the EEA countries: see n 6.

[26] See Commission of the European Communities, First Report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final (**First Report on the Data Protection Directive**), at 19. National DPAs are supposed to notify the Commission when they authorise a transfer under Article 26(2) Data Protection Directive. The Commission notes that it has received only a "derisory number of notifications compared with what might reasonably be expected." The Commission further notes that "combined with other evidence pointing in the same direction, this suggests that many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection."

[27] Rand Europe, Review of the European Data Protection Directive, Technical Report dated May 2009 (**Rand Report**) at 35. Douwe Korff, *EC Study on implementation of the Data Protection Directive, Comparative study of national laws*, September 2002, Human Rights Centre University of Essex, at 209, to be found at <http://papers.ssrn.com>, notes that "the powers now vested in the data protection authorities, as currently exercised, have not been able to counter continuing widespread disregard for the data protection laws in the Member States." See further Omer Teme, "For Privacy, The European Commission Must Be Innovative", Center for Democracy & Technology, 28 February 2011, to be found at http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative: "Enforcement is a sore issue for the EU DPD. It is an open secret that the framework is largely not enforced. Indeed, implementation of the EU DPD is probably highest among US based multinationals, which implement strict compliance programs for risk management purposes and as part of overall corporate governance schemes"; and "Commentary in Response to the European Commission's Communication on 'A comprehensive approach to personal data protection.'" Centre for Information Policy Leadership, January 2011, to be found at <www.huntonfiles.com> (**Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive**), at 12: "Articles 25 and 26 of the existing Directive have been simultaneously its most controversial and most burdensome provisions. It is also arguable that they have been the least effective if full account is taken of current volumes of international transfers. (…). The result is the paradox that substantial resources are expended by some organisations to try "to get it right" whilst there is an unmeasured non-compliance by other organisations which ignore the requirements."

Especially the complications with the EU data transfer rules have led multinationals to put pressure on the DPAs to recognise their corporate privacy policies as providing an adequate level of protection for the processing of personal data throughout their groups of companies. Insofar as such processing involves transfers of personal data to a group company in a country without an adequate level of data protection, 'adequate safeguards' are provided for by the corporate privacy policy.[28] The advisory committee to the European Commission on data protection (**Working Party 29**)[29] recognises the added value of such transnational private regulation in the data protection area in light of the gaps and deficiencies of the present EU data transfer regime. The Working Party 29 has set criteria for these corporate privacy policies in order to ensure a minimum level of protection for the processing of personal data throughout the group of companies. One of these requirements is that these privacy policies should be "internally binding" within the organisation (on all group companies and employees) and "externally binding" for the benefit of individuals (i.e. must create third-party beneficiary rights for the individuals).[30] To express this binding character of these corporate privacy policies the Working Party 29 calls them "Binding Corporate Rules" (**BCR**). The BCR regime set by the Working Party 29 introduces the possibility of central supervision of worldwide compliance with such BCR by one of the DPAs of the EU Member States. With BCR, the Working Party 29 introduced a complex hybrid system of regulation of cross-border data transfers combining transborder self-regulation (corporate privacy policies) with public arrangements (the DPAs validating such corporate privacy policies and providing supervision and enforcement). Despite the opinions issued by the Working Party 29 on the concept of BCR, some DPAs still do not agree to these requirements and refuse to recognise

---

[28] As required for the transfer of data to countries without adequate protection, pursuant to Article 26(2) Data Protection Directive.

[29] The Working Party 29 was established as an advisory body to the European Commission under Article 29 of the Data Protection Directive. The Working Party 29 has advisory status only and acts independently, see Article 29(2) Data Protection Directive. Members are representatives of each of the DPAs, of the European Data Protection Supervisor and of the European Commission. The tasks of the Working Party 29 are clearly formulated and are publicly available. It issues opinions to "contribute to the uniform application of the Data Protection Directive and advises on proposals for EU legislation having an impact of data protection. See the Document "Tasks of the Working Party 29", as published at <www.ec.europa.eu>. Though the opinions of the Working Party 29 are non-binding, they are followed in practice by the DPAs and *de facto* set the rules for application of the Data Protection Directive. See on the Working Party 29, its tasks and procedural rules in more detail para. 14.7.2 - 14.7.4.

[30] See on this requirements in detail para. 11.2 - 11.3.

BCR or set additional requirements in this respect.[31] In any event uncertainty exists as to whether BCR will also be accepted as a valid data transfer tool by non-EU jurisdictions that have their own data transfer restrictions. As a consequence it is at present still uncertain whether the BCR concept will work on an EU-wide basis, let alone at a global level, and the timeframe within which this may ultimately be achieved.[32]

The Working Party 29 acknowledges the shortcomings of the EU data transfer rules and of the present BCR regime and has advised the European Commission to address these in the upcoming revision of the Data Protection Directive[33] which was launched by the European Commission on 1 July 2009. Subsequently, the European Commission in its communication of November 2010 on the revision of the Data Protection Directive[34] announced that it will indeed "improve and streamline the current procedures for international data transfers, including (…) Binding Corporate Rules".[35] It is therefore to be expected that the BCR regime will become one of the standard tools for intercompany data transfers.

---

31 See for examples n 38 and n 41 below.

32 See in more detail para 10.5.

33 See WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, as adopted on 1 December 2009 (**WP Contribution on The Future of Privacy**), at para 38, listing: "Recognising BCR as appropriate tool to provide adequate safeguards"; and "Defining the main substantive and procedural elements of BCRs, following the WP29 Opinions on the subject". What is noteworthy here is that the Working Party 29 (apparently) is not even sure that BCR can indeed be a tool for the transfer of data to countries without adequate protection under Article 26(2) of the Data Protection Directive. See further the WP Opinion on the principle of accountability (n 15), at para. 56.

34 See European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union,' COM(2010) 609/3 (4 November 2010), at para. 2.2.1. and 2.2.3 (**EC Communication on the revision of the Directive**). Commissioner Viviane Reding, who is in charge of Justice, Fundamental Rights and Citizenship, had announced that a proposal for the revision of the Data Protection Directive would be presented in November 2010. However, several DPAs urged the Commissioner not to rush through the revisions. Accordingly, the European Commission has decided to postpone the release of a proposal, noting that it will instead issue a statement in November 2010, and will present proposed revisions in the latter half of 2011. See the press release of the French DPA at <www.cnil.fr>.

35 EC Communication on the revision of the Directive (n 34), at 16; Viviane Reding, "The Upcoming Data Protection Reform for the European Union," in: [2011] 1 International Data Privacy Law, at 5. This was already the recommendation in the First Implementation Report

6.2 Relevance of BCR as a data transfer tool at global level

For a number of reasons the introduction of the BCR regime is an important development and is expected to gain further relevance in the coming years.[36]

6.2.1 No global standard

International data transfers are generally considered essential to the advancement of global trade[37] and the economic and social development of individual countries.[38] At the same time, concerns about data processing risks in certain countries have led many countries to introduce restrictions on outbound data transfers.[39] Recently, these concerns have increased due to certain countries expanding their state policing powers to access data of foreign citizens.[40] The growing number of incidents recently where foreign

---

(see First Report on the Data Protection Directive (n 26), at 18), and is further in line with the recommendations of the Rand Report (see Rand Report (n 27), at 42) and of the EPCD in European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union" (**EDPS Opinion on the revision of the Directive**), at para. 127. See in detail para 10.6.

36 See also Kuner (n 8), at 24.

37 As already acknowledged at the time the Data Protection Directive was enacted, see Recital 56: 'Whereas cross-border flows of personal data are necessary to the expansion of international trade (...)'. See also Kuner (n 8), at 34 - 35, however also concluding that more 'hard research has to be done to confirm the effects of transborder data flows'.

38 Recommendation of the OECD Council Concerning Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data (23 September 1980) (**OECD Privacy Guidelines**), preamble, to be found at <www.oecd.org> and **APEC Privacy Framework (2005)**, to be found at www.apec.org, preamble at para. 2; Kuner (n 8), at 8 and 34. At 8, Kuner indicates that the economic, legal and social importance of transborder data flow is at present not adequately recognised at the highest levels of government, and that more research has to be undertaken to measure the economic benefits and costs of regulation of trans-border data flows.

39 See for a comprehensive overview of the various perceived risks that underlie regulation of transborder data flows: Kuner (n 8) at 30 -33.

40 The US Patriot Act (see para 8.1 below) is an example of a recent expansion of state control powers which triggered data transfer restrictions in other countries. See Kuner (n 8), at 31-32, giving the example that Canadian provinces have enacted a restriction of the outsourcing of data of Canadian public bodies based on concerns about access to such data by the US government under the US Patriot Act. The increase in surveillance is not limited to the US. This is also an issue within the EU. For an overview of the EU security data exchange policies and the data

governments use their state control powers and demand access to foreign data[41] only strengthens the data protection concerns of countries that

---

protection implications, see Tenth Annual Report of the Article 29 Working Party on Data Protection, at 7-8 (to be found at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm>).
In 2004, the EU and US finally entered into an agreement on the much debated data transfers to the US Department of Homeland Security of 'passenger name records (**PNR**) of air passengers' travelling from Europe. Until this point, these transfers lacked a legal basis under the Data Protection Directive. Another source of tension was the revelation in 2006 that, since 2001, US authorities repeatedly enforced the disclosure of payment transaction data processed by SWIFT (Society for Worldwide Interbank Financial Telecommunication) for the purpose of fighting terrorism, based on government subpoenas, in violation of the EU transfer rules. To avoid further violations of data protection, SWIFT transferred its data processing facilities from the US to Switzerland. The violation has been recently remedied in the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, [2010] OJ L8/11, as approved on behalf of the Union by the Council Decision 2010/412/EU of 13 July 2010 OJ L195/3. This approval followed the proposal from the European Commission, and gained the consent of the European Parliament (European Parliament legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE) (**Agreement on Transfer of Financial Messaging Data**).

[41] Examples are the refusal of India to allow Blackberry handheld devices because the data are encrypted, demanding that entities offering communication services in India should also maintain communications equipment there, facilitating real-time access to corporate messages. See Daniel Emery, "India threatens to suspend Blackberry by 31 August," BBC News Online, 13 August 2010, available online at <http://www.bbc.co.uk/news/technology-10951607>. Another example is China which requires service providers doing business in China to reveal data to Chinese law enforcement authorities. E.g. in January 2010 Google threatened to withdraw from China referring to China-based cyber attacks on its databases and the e-mail accounts of some users, and China's attempts to 'limit free speech on the Web,' as the reasons for its decision. See The New York Times Google Inc. profile at <http://topics.nytimes.com/top/news/business/companies/google_inc/index.html?scp=2&sq=china%20google%20yahoo&st=cse>. A more recent example is a US court order from 14 December 2010, demanding release of details about the accounts of WikiLeaks founder Julian Assange and other WikiLeaks activists, including Birgitta Jonsdottir, an Icelandic parliamentarian (see http://www.bbc.co.uk/news/world-us-canada-12141530).

underlie their data transfer rules.[42] As a result we may expect that increasingly more countries will introduce data protection legislation[43], which in most cases will also include outbound data transfer rules. It is only when data protection laws are harmonised on a global basis that the need to adopt data transfer rules will be eliminated.[44] Although there is a persistent call for a legally binding global standard for data protection and there are some concrete initiatives in this respect, it is not expected that such a global standard will indeed be realised within the coming 10 years.[45] The present regulatory landscape is still too diverse for such a standard to be adopted on a global level. Therefore, at least for the near future, the existence of data transfer rules is a given and even on the increase. Data transfer instruments such as BCR therefore are expected to gain importance as instruments in facilitating cross-border data transfers.

6.2.2 Bridging function of BCR between different legal systems

Governments choose very different rationales for their data protection legislation: EU legislation is based on protecting fundamental rights and freedoms whereas, for instance, the APEC Privacy Framework is aimed at securing economic benefits of e-commerce.[46] The rationales underlying the regulation of outbound data transfers are also very different. Broadly speaking, there are two approaches to data transfer rules to be distinguished: territory-based rules and organisation-based rules.[47] The EU data transfer rules are an example of the first approach and allow data transfers when the country of destination provides for "adequate" data

---

42 As a practitioner, I see a trend for multinationals to avoid having data processing facilities in countries with excessive state control powers. After introduction of the US Patriot Act, many multinationals relocated their central IT facilities (which were initially transferred to the US mainly for cost reasons) back to the EU. A public example is the Society for Worldwide Interbank Financial Communications (SWIFT) which relocated its central processing facilities in the US to Switzerland for reasons of US state control powers under the US Patriot Act. See press release of 4 October 2007 to be found at www.swift.com and n 40 above.

43 Kuner (n 8), at 42.

44 See Spiros Simitis (ed.), Bundesdatengeschutzgesetz (Nomos 2006), at 123.

45 See in detail para 8.2.

46 APEC Privacy Framework (n 38), at 3: "APEC economies realise that a key part of efforts to improve consumer confidence and ensure growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region". See also Kuner (n 8), at 27.

47 See for this categorisation Kuner (n 8), at 28.

protection.[48] The APEC Privacy Framework is an example of the second approach, and holds organisations accountable for the protection of personal data also after they transfer such data to other organisations (wherever located).[49] Though the starting points of these two approaches may seem very different, in practice the two systems in their application to a large extent converge. For instance, the Data Protection Directive also facilitates "organisational based" data transfer tools, legitimising data transfers between organisations if the EU Standard Contractual Clauses are used or if US companies have adhered to the US Safe Harbor scheme. Introduction in the EU of the BCR regime, making a multinational an adequate "safe haven" for data protection purposes wherever its group companies are located, is a further prime example of an "organisational based" tool for data transfers. APEC through its Privacy Framework also intends to facilitate a similar organisational tool, providing that Member Economies shall endeavour to ensure that organisations adopt "Cross Border Privacy Rules" (**CBPR**) as a manner to facilitate their cross-border data transfers.[50]

The APEC Privacy Framework also incorporates elements of the territory-based approach, where it encourages Member Economies to develop cooperative bilateral or multinational arrangements so that the participating countries will cooperate in the investigation and enforcement of data protection violations. The APEC Privacy Framework explicitly provides that

---

[48] Another example is Article 2(1) of the Additional Protocol to the Convention for the protection of individuals with regard to the automatic processing of personal data regarding Supervisory Authorities and transborder data flows, 8 November 2001 (**Additional Protocol to Convention 108**), to be found at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=1&CL=ENG, which provides that each party shall allow transfers of personal data to a non-party only if an "adequate level of protection is assured". Other examples (athough here the starting point is reversed in the sense that transfers are in principle allowed but may be blocked or restricted in certain circumstances) are: the OECD Privacy Guidelines, which allow restriction of outbound data transfers in case the country of destiny does not provide for 'equivalent protection', see OECD Privacy Guidelines (n 38), at para. 17; the UN Guidelines concerning Computerized Personal Files of 14 December 1990 (UN Doc E/CN.4/1990/72), at para. 9, allowing restrictions in case the other territory does not provide for 'reciprocal safeguards'; and Article 12 of Convention 108 which allows restrictions "except where the regulations of the other party provide an equivalent protection."

[49] See para 7.4 on the APEC Privacy Framework, and in particular for the accountability rule in respect of data transfers (n 38).

[50] APEC Privacy Framework (n 38), at III Cooperative Development of Cross Border privacy Rules, para. 46 -48.

such cooperation may be declined or limited by a Member Economy where cooperation would lead to violation of the national laws or policies of a Member Economy. Thus, if the laws of the counterpart are not considered "equivalent" to a country's national law, cooperation may be declined; a result very similar to the EU adequacy rule.[51] This is a clear example of a territory-based arrangement. Though it is expected that the EU and APEC systems of data transfer rules will converge further[52], it is clear that BCR and CBPR will be an important common factor of the two systems.[53] BCR will thus fulfil a bridging function between the two systems facilitating international data transfers even where (in this case) the EU and the APEC Member Economies cannot agree on what the appropriate universal level of data protection should be.[54]

6.2.3 Limitations of state legislative and enforcement powers

Territoriality is a key factor for the applicability and enforcement regimes of the data protection laws across the world.[55] However, in a globalised society where companies operate on a cross-border basis and technology facilitates

---

51 See also Kuner (n 8), at 30.

52 Kuner (n 8), at 40 concludes that neither the geographical nor the organisational approach is inherently better than the other, each having advantages and disadvantages. What is needed is for the two approaches to co-exist, whereby the solution selected by a country should be accompanied by measures to avoid its inherent disadvantages, as otherwise the first approach will tend to be excessively bureaucratic and the second too reactive. A solution is also to mix the two approaches. Examples given are Canada, where for the decision whether a company has implemented sufficient organisational and contractual measures as part of its accountability obligations, the location to which the data are to be transferred is taken into account. See Christopher Kuner, 'Developing an adequate legal framework for international data transfers', in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), at 271. The Australian Government, Australian Privacy Principles, Exposure Draft of 24 June 2010, at 15–17, to be found at http://www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/exposure_draft.pdf (Draft Australian Privacy Principles also seek to combine the geographical and organisational approach.

53 In general it is the expectation that private sector instruments will likely assume increasing importance in coming years. See Kuner (n 8) at 24; and Prins (n 9), at 173: "A final remark is that the case of personal data protection is also a fine illustration of the role that soft law (codes of conduct, privacy policies, corporate rules, privacy seals and trust marks) and the actors involved therein can play in establishing a certain degree of international protection."

54 For a critique of the 'adequacy' of data protection expected to be provided , see the APEC Privacy Framework, (n 38).

55 See paras. 2.3.7 and 3.2 Kuner (n 8), at 11 and 41.

seamless cross-border data flows, reliance on territoriality as an organising principle to regulate these data flows is inherently flawed.[56] Most state regulation is aimed solely at protecting individuals in a relevant state territory, whether the offensive acts are performed in the territory or aimed at the citizens in the relevant territory (think of media and advertising laws). Specific to data protection is that protection of data of an individual in the territory itself is not sufficient as data of individuals may also flow outside the territory. Data protection is one of the few legal fields that aims to protect individuals also outside their territory[57], when their data are

[56] See para. 3.11: "The underlying principle of territoriality whereby a physical connection is required to a territory is no longer suited to be applied in the current day reality;" or as phrased by Stephen J. Kobrin, 'The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance', Working Paper Series , The Wharton School (November 2002), at 23: "Extraterritorial reach not only becomes the norm, the concept itself looses meaning as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system." See also Kobrin (above), at 28: 'Transnational integration, however, is increasingly relational rather than geographic; the new political space from which effective and legitimate governance must emerge takes the form of relational networks rather than territory, a 'space of flows' rather than a 'space of spaces'. '

[57] A parallel can be made with export control regulations, where the export of technology that may endanger state security (as it may enable foreign governments in developing weapons etc) is restricted. Though not identical, parallels can also be found with corporate social responsibility regulation. This aims to protect citizens in a territory against products that are manufactured in ways which violate human rights abroad. In the criminal arena, a parallel may be made with the 'passive personality principle' of public international law. This principle allows a sovereign state, in limited cases, to claim jurisdiction to try foreign nationals for offences committed abroad on the basis that the crime affects their own nationals. On this concept, see Alina Kaczorowska, *Public International Law*, 4th ed. (Routledge, New York 2010), at 322: "According to the passive personality principle a State has jurisdiction to punish aliens for harmful acts committed abroad against its nationals;" and Tim Hillier, *Sourcebook on Public International Law* (Cavendish, London 1998) at 279: "Under this principle, jurisdiction is claimed on the basis of the nationality of the actual or potential victim. In other words, a state may assert jurisdiction over activities which, although committed abroad by foreign nationals, have affected or will affect nationals of the state." The passive personality principle has been rejected as a ground of jurisdiction by the International Court of Justice in the SS Lotus case (France v Turkey 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7)) and has been described as "the most difficult principle to justify in theory" (Kaczorowska at 322, see also Hillier at 279). Of this principle, it has also been said that "while many civil law countries claim jurisdiction on this ground, others such as the UK and the US, tend to regard it as contrary to international law so far as ordinary torts and crimes are concerned but not in respect of terrorist killings and the taking of hostages etc." (see Kaczorowaka at 322).

transferred abroad (and such other country does not provide for protection of such data). This is the main motivation for the introduction of data transfer rules. In addition to data transfer rules, many countries have tried to protect the data of their citizens when transferred abroad by expanding the long-arm reach of their data protection laws (i.e. by expanding the scope of their applicability regimes).[58] This poses many questions under private international law (**PIL**). Though data protection regulations may be of relatively recent times, the concepts of applicable law, jurisdiction and enforcement are embedded in a long tradition of PIL, whereby laws that over-extend their jurisdictional reach are considered to be an unacceptable form of 'hyper-regulation' if they apply so indiscriminately that there is no hope of enforcement.[59] Enforcement powers of states and the jurisdiction of their courts are also subject to limitations set by PIL.[60] Applicability and enforcement regimes are therefore inherently delineated and cannot be instrumental in filling the gaps in the protection of personal data and the enforcement of protection.[61] At present, the main tool available to the authorities to try to solve any gaps in the international patchwork of applicable laws and enforcement is seeking cooperation with other data protection authorities in the event of cross-border data protection violations (the 'network approach', where each DPA enforces its own rules in its own territory).[62] In practice seeking such cooperation is increasingly common.[63]

---

58 Kuner (n 8), at 7 comments that the rules of applicable law and data transfer are often intertwined, whereby countries use rules on applicable law to protect data across their borders, "thus using applicable law to serve the same purpose as regulation of transborder data flows."

59 An example is the interpretation by the Working Party 29 of Article 4(1)(c) Data Protection Directive as a result of which the Data Protection Directive already applies if a non-EU website uses cookies to process personal data of EU citizens, by taking the position that the sending by a non-EU based website of cookies to the computers of internet users in the EU constitutes the use of 'equipment' in the EU, triggering the applicability rule of Article 4(1)(c). See Working Document on determining the international application of EU data protection law to personal data processed on the Internet by non-EU based websites (WP 56, 30 May 2002) (**Working Document on Non-EU Based Websites)**, at 11. See para 3.7.3, in particular n 64.

60 See Christopher Kuner*, European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2007), at 125 and Kuner (n 52), at 271.

61 See Chapters 2 and 3 where I discussed the delineations of the present applicability and jurisdictional regime of the Data Protection Directive, and Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)," in [2010] International Journal of Law and Information Technology, at 183.

62 Pursuant to Article 28(6) and (7) of the Data Protection Directive, DPAs are required to cooperate with one another, exchange useful information and may be requested to exercise their powers by a DPA of another Member State (i.e. enforcement is based on a 'network approach'). See for the APEC Privacy Framework (n 38). See further para 8.3.

However, until such time as all jurisdictions have adequate data protection laws and supervision of these laws, this network approach cannot adequately solve all gaps in applicable laws and enforcement issues presently faced by data protection regulators.

At first glance the absence of a global data protection regime may seem to be to the advantage of multinationals, being able to benefit from any gaps in protection and avoid liability for doing so. This is, however, not the case. As multinationals benefited from harmonisation of the data protection laws in the EU by the introduction of the Data Protection Directive[64] and will benefit from further approximation of the EU data protection laws in the upcoming revision of the Data Protection Directive[65], multinationals operating on a global basis would also benefit from global norms and central supervision and related enforcement. This would enable them to streamline their data processing operations not only on an EU-wide basis but also on a global basis and further ensure a consistent and predictable interpretation and

---

63 Kuner (n 8), at 32 and 42.

64 Prior to the adoption of the Data Protection Directive, the data protection laws in the Member States were very diverse with some Member States having no data protection laws at all (see n 15). According to Recital 7 of the Data Protection Directive, the main consideration for introduction of the Data Protection Directive was "the existence of a wide variety of national laws, regulations and administrative provisions" which were considered to "constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law". See further Recital 8: "whereas, in order to remove the obstacles to flows of personal data, the level of [data protection] must be equivalent in all Member States". See on the economic and social benefits of free cross-border data flows, Kuner, (n 8), noting (at 6) that "[p]ersonal data are now crucial raw materials of the global economy"; and (at 9) that "confidence in data processing and privacy protection have become important factors to enable the acceptance of electronic commerce". While at the same time noting (at 8) that the "economic, legal and social importance of transborder data flows is not adequately recognised at the highest levels of government" and that "important research remains to be done in areas such as measuring the economic effects of transborder data flows".

65 It is generally acknowledged that the main shortcoming of the Data Protection Directive is that the level of harmonisation under the current framework is unsatisfactory due to (i) the fact that the Directive leaves the Member States too much discretion in implementing the provisions thereof (see Recital 9 of the Data Protection Directive) and (ii) the many instances of incorrect implementation by the Member States. This was already the conclusion of the First Implementation Report on the Directive (n 26), at 11 and action point 6 at 24. See for the same conclusions the WP Contribution on the Future of Privacy (n 33), at para. 18 – 21; the EC Communication on the revision of the Directive (n 34), at 10; and the EDPS Opinion on the revision of the Directive (n 35) at 7 and 12. See para. 5.3 for areas that according to the EDPS require further harmonisation.

application of the data protection rules. As this is not yet achievable by global public regulation, BCR may play a role here. If it is possible to make a choice of law and forum in BCR, it would be possible to have BCR supervised and enforced by one "lead" DPA only, preferably the authority of the place of establishment of the headquarters of such multinational. BCR may thus function as a private regulatory response to the inherent limitations of rules on applicable law and jurisdiction.

6.2.4 Stepping stone to further harmonisation

The application of BCR by multinationals also to group companies in countries where no (or less) data protection exists may have an important example function in those countries, as their nationals also benefit from this protection.[66] Though no hard research has been carried out in this respect, in general it can be said that transnational private regulation (**TPR**) that is based on non-binding "soft law" is often a stepping stone to hard law.[67] A similar influence may be expected of implementation of BCR on a large scale. This being said, it should be noted that at the time the Safe Harbor Framework[68] was introduced in the US, it was the expectation that this

---

66 Kuner, (n 8), at 6 indicates that this is a benefit of data transfer rules.

67 Application of TPR on a worldwide basis has the potential to import the rule of law and developed countries' business norms into the world of emerging economies, which in itself may be a bottom up driver for the ultimate acceptability of an international standard. For such an effect of TPR, see John M. Conley and Cynthia A. Williams, *Global Banks as Global Sustainability regulators: the Equator Principles*, at 5, available at www.hill.org, and literature therein referred to. See further Fabrizio Cafaggi, *New Foundations of transnational private regulation*, EUI Working papers RSCAS 2010/53, at 15; Deirdre Curtin and Linda Senden, "Public accountability of Transnational Private regulation", in: [2011] 38 Journal of Law and Society, at 185; and Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins, Maurice Schellekens, "Should Self-Regulation Be The Starting Point?", in: Bert-Jaap Koops et. al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), Chapter 5, at 140. Cafaggi (above) at 17 signals that if soft law is in place TPR also "operates as a vehicle to harden soft law, providing binding force" and "confers higher legitimacy" to such soft law. This is based on the conclusion of Cafaggi (at 1) that TPR is generally voluntary, but after it has been adopted it becomes binding: "Parties who wish to join the regulatory bodies participating to the regime are free to do so, however, once they are in, they are legally bound and violation of the rules is subject to legal sanctions".

68 The Safe Harbor Framework consists of a set of seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision regarding data protection in the US, the exchange of letters between the US Department of Commerce and the European Commission, and letters from the Department of Transportation and Federal Trade Commission on their enforcement powers. As explained in the Safe Harbor Privacy Principles

would ultimately lead to elevation of the overall level of data protection in the US. It seems that this expectation has not (fully) materialised.[69] Rather

issued by the US Department of Commerce on 21 July 2000, (ANNEX I to 2000/520/EC Commission Decision of 26 July 2000 on the adequacy of the protection provided by the safe harbor privacy principles), the principles are intended for the purpose of qualifying for the safe harbor and the presumption of 'adequacy' it creates. To qualify for the safe harbor scheme, an organisation must comply with the requirements of:
1) notice (inform an individual as to the purpose of processing, contact information of the organisation and complaint procedure, etc.):
2) choice (opt-out regarding disclosure to a third party or use incompatible with the purpose for which the data was initially collected, and op-in regarding sensitive information);
3) onward transfer (permitted only if the notice and choice requirements are respected; an organisation must ensure that its agent complies with these principles, the Data Protection Directive or another adequacy finding);
4) security (reasonable precautions must be taken to ensure data security);
5) data integrity (data should be reliable, accurate, complete and current and processing is not excessive with regard to the purposes for which the data was collected);
6) access (an organisation must ensure individual access rights); and
7) enforcement ('mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed').

69 See Duncan H. Brown and Jeffrey Layne Blevins, "The Safe Harbor Agreement between the United States and Europe: A Missed Opportunity to balance the Interests of E-Commerce and Privacy On-Line," Journal of Broadcasting and Electronic Media 46, no. 4 (2002) available on-line at <http://www.allbusiness.com/legal/laws/384290-1.html>. Brown and Blevins are of the opinion that the Safe Harbor Framework did not live up to its potential to elevate the level of US data protection: "The "ratcheting up of national standards" for personal data privacy protection in the U.S. (…) might happen in response to the safe-harbor provisions did not transpire. (…S)everal years before (…) a number of analysts (…) had believed that the proposed Data Protection Directive "might open a 'policy window' leading to the strengthening of privacy laws in the United States and the establishment of some form of commission" (…). In the earlier case, there was certainly no change, and it now appears likely that the status quo will again be maintained in the U.S. despite the existence of the safe harbor." See, however, Peter P. Swire, Elephants and Mice Revisited: Law and Choice of Law on the Internet, University of Pennsylvania Law Review [Vol. 153: 2005], at 1987: "the Safe Harbor has been fairly successful at meeting two strategic goals: avoiding a trans-Atlantic trade war and providing a reasonable baseline for privacy protection in transborder activities (…).Agreement on the Safe Harbor can also be defended as a "soft" harmonization of privacy law. Both for organizations who have formally enrolled in the Safe Harbor, and for the larger group of organizations who are aware of the Safe Harbor, the Safe Harbor principles give a widely known set of rules for what is considered appropriate corporate action. Even though most companies will never face an enforcement action or a privacy audit, any organization that deviates substantially from the Safe

than increasing the overall level of data protection, introduction of the Safe Harbor Framework often led in practice to US companies introducing a higher standard only for EU customers.[70]

6.3 Evaluation of the BCR regime from different dimensions

In light of the above it is worth looking at the BCR regime as introduced by the Working Party 29 in more detail in order to determine whether this co-regulatory[71] tool is indeed suitable to achieve protection of one of the fundamental rights and freedoms of EU nationals in a transnational environment. For that purpose the BCR regime may be seen and evaluated in the context of a number of different dimensions:

6.3.1 Evaluation of BCR as a form of transnational private regulation

Legislators (including EU legislators)[72] that wish to regulate global corporate conduct opt for "regulating" TPR rather than introducing public regulation with its inherent limitations as to jurisdictional and authoritative scope of state competence. The discipline of how to best regulate (the rules for rule

---

Harbor principles runs the risk of exposure and enforcement. The potential number of choice-of-law cases involving privacy is greatly reduced under this soft version of harmonization that gives notice to organizations about key, expected privacy protections."

70 See Vera Bergelson (2003), "It's personal but it is mine?" U.C. Davis L. Review 37:379 at 396. Bergelson, acknowledges the role of the Safe Harbor Framework as "an important step in establishing a data protection regime in this country," but considers the framework "just an emergency measure designed to deal with the ultimatum issued by the EU to the United States" and states that "the "Safe Harbour" approach creates an incentive for U.S. participants to maintain two privacy standards – the higher one for European consumers and the lower one for the domestic consumers (this referring to Robert Gellman, "Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete," available at <http://www.epic.org/reports/dmfprivacy.html#2> (March 2002)).

71 Co-regulation is "the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)" (Article 18 of the 2003 Inter-Institutional Agreement on Better Lawmaking concluded between the European Parliament, the EU Council of Ministers and the European Commission of 16 December 2003 (2003/C321/01), [2003] OJ C321/1, in particular Article 18 (**2003 Inter-Institutional Agreement on Better Law Making**).

72 See European Commission, White Paper on European Governance (2001) COM 428 final (**White Paper on European Governance**), at 21; and the 2003 Inter-Institutional Agreement on 'Better Lawmaking' (n 71).

making, the search for meta-norms) has come to be known in the EU as "Better Regulation" (**BR**). In the substantial body of research concerning the concept of BR and TPR, questions are raised as to:

- the suitability of TPR to regulate human rights[73];
- how to best regulate TPR, which of the different forms of regulation would be most suitable to regulate TPR;
- the legitimacy of TPR as compared to public regulation;
- how to align TPR with conventional principles of contract law (TPR raises questions of enforceability by third-party beneficiaries of such TPR)
- TPR is often effectuated through contractual "supply chain management", which solution is also part of the BCR regime. Supply chain management also raises issues of enforceability by the beneficiaries of these contracts, which are of equal relevance to BCR.
- TPR further raise several questions of PIL if the third-party beneficiaries are employees and consumers. The European rules of PIL entail that a choice of law and forum in the BCR may not affect the substantive rights and remedies or the dispute settlement procedures which are available to EU employees or EU consumers.

6.3.2 Evaluation of BCR as implementation of corporate accountability

In some areas of law legislators (including the European Commission) introduce in some areas of law the "principle of accountability" in respect of compliance with the relevant legal requirements. The main purpose of "accountability" is to use the law to hold businesses accountable for taking their responsibilities seriously by using various mechanisms to encourage or force businesses to put internal governance structures and management systems in place. The Working Party 29 has proposed that the accountability principle be included in the revised Data Protection Directive. The European Commission has recently communicated that it indeed intends to include the accountability principle in the revised Directive.[74] This will entail that in addition to the obligation to comply with the EU data protection requirements, an independent obligation will be introduced to implement a proper data protection compliance program. The BCR regime is mentioned by the Working Party 29 as the prime example where the principle of

---

73 Also the European Commission seems to be of the opinion that transnational private regulation is not suitable to regulate human rights. See White Paper on European Governance (n 72), at 21 and the Inter-Institutional Agreement on Better Lawmaking (n 71), at 3. See for a critical discussion of the position of the European Commission and the other EU institutions, Paragraph 14.5.

74 EC Communication on the revision of the Directive (n 34), at 11-12.

accountability has already been implemented. This being said, the BCR regime should be evaluated against:

- the proposal of the Working Party 29 on the accountability principle;
- other data protection legislation that incorporates the accountability principle; and
- the general body of research in respect of the principle of accountability as introduced in other fields of law.

6.3.3 Evaluation of BCR in the context of Corporate Social Responsibility

Many multinationals voluntarily adopt "Corporate Social Responsibility" (**CSR**) codes to overcome differences in regulations and regulatory approaches between countries and as part of their global reputation management. Typically, CSR codes involve a commitment by multinationals (usually in their Code of Ethics or Business Principles) to respect human and civil rights, to protect the environment, to oppose bribery and corruption and to commit to fairness to their customers and suppliers. The range of issues brought under the umbrella of CSR is constantly expanding and often now also includes a commitment to protect the privacy of employees and customers. Various topics concerning CSR are also of relevance to BCR. In the substantial body of research concerning CSR, similar issues are raised as set out above in respect of TPR (CSR being a form of TPR). Additional issues that are raised which equally apply to BCR are:

- Various international non-governmental and intergovernmental organisations have issued instruments with guidelines for CSR codes (so-called soft law). Relevant for BCR is to what extent the right to data protection of the stakeholders of a company is covered by these soft law instruments and whether this has any repercussions for the BCR regime as it presently stands.
- CSR codes are voluntarily unilateral undertakings, but global legal practice shows how the law is being used to hold multinationals legally accountable for application of their CSR codes, which is of relevance to BCR as well.

6.4 The quest for meta-norms for BCR

As TPR operates in a plurality of public and private normative orders and with a plurality of actors, TPR has to function within many different spheres.[75] For TPR to be acceptable, TPR has to "construct relationships of

[75] Jacco Bomhoff and Anne Meuwese, "The Meta-Regulation of Transnational Private Regulation," Journal of Law and Society, Vol. 38, number 1, March 2011, at 160.

recognition with the different public and private orders it comes into contact with."[76] This will not be different for BCR. Also BCR have to operate within many different spheres: the national jurisdiction where the multinational has its primary establishment, the national jurisdictions where the multinational has secondary establishments, the contractual relationships the multinational has with its employees, its customers, its suppliers, its sub-contractors and many supra-national spheres (at the EU, APEC, global level, etc). For BCR to be acceptable in all different public and private spheres it touches upon, it must be aligned with the existing legal disciplines and other bodies of thought it interacts with.[77] This is not so much to say that BCR, for instance, should be in compliance with rules of PIL or that BCR should observe rules of contract law, though these obviously cannot be ignored.[78] The different disciplines (or perspectives) from which BCR may be evaluated, however, also potentially provide a source of "meta-norms" for BCR.[79] "Meta-norms", are defined by one author as "norm[s] to which parties can commit without betraying their loyalty to their own legal systems".[80] BCR will also have to accommodate this duality. Multinationals implementing BCR cannot ignore the national rules of the jurisdictions in which they operate, but they also have to operate on a global level which sets its own demands. For BCR (operating at the global level) to be acceptable at the national level, BCR will have to "build on the assumption of common reference points"[81] between national jurisdictions and different disciplines. For example if BCR are reviewed from the perspective of the discipline of "ethics" of law, we have to look for:

> "the set of social norms commonly accepted on the basis of agreements and conventions, and therefore sustained by rational choices of multiple agents. Once those norms have passed the universalizability test, which is what meta-ethically distinguishes them from rules of mere prudence or from social norms

---

76 Bomhoff and Meuwese (n 75), at 160.

77 Bomhoff and Meuwese (n 75), at 170 and 172.

78 This is also called the function of PIL as a "mechanism" or the "touch down" function thereof, as due to rules of PIL, state laws becomes relevant again for TPR (for instance as to questions whether a choice of law may be made in TPR, enforcement of TPR etc). See Bomhoff and Meuwese (n 75), at 171.

79 Especially as to the socio-economic and political implications behind private international law instruments and doctrines. See Bomhoff and Meuwese (n 75), at 172.

80 Bomhoff and Meuwese (n 75), at 164 (citing C. Joerges, Constitutionalism in Postnational Constellations: Contrasting Social Regulation in the EU and in the WTO, in Constitutionalism, Multilevel Trade Governance and Social Regulation, eds. C. Joerges and E.-U. Petersmann (2006)).

81 Bomhoff and Meuwese (n 75), at 165.

> not susceptible to moral meaning, they are effective by dint of their social function of solving cooperation and coordination problems".[82]

The quest for universality of BCR seems a bit daunting, but a first attempt at identifying common reference points (meta-norms) for BCR is undertaken in this dissertation by evaluating the concept of BCR from the different dimensions and perspectives set out above. Perhaps not so surprisingly, such evaluation will indeed show many common denominators across the disciplines. Though at present there are no hard and fast rules against which TPR (let alone BCR) should be evaluated, I will take these common denominators of the different disciplines as meta-norms for evaluating BCR. On this basis I will make suggestions for improvements of the BCR regime, as well as suggestions how to fit the BCR concept into the regulatory data protection regimes of other countries or regions like the APEC Privacy Framework. The objective is to achieve that BCR can be accepted as a mainstream global solution to regulate global corporate conduct in the area of data protection, also in countries where at present no (or insufficient) data protection is afforded. BCR may then indeed provide a solution to avoid the present gaps in protection and enforcement as presented by the current patchwork of national data protection laws.

[82] Lorenzo Sacconi, "Corporate Social Responsibility (CSR) as a Model of 'extended' Corporate Governance: an Explanation Based on the Economic Theories of Social Contract, Reputation," in Fabrizio Cafaggi, *Reframing Self-Regulation in European Private Law* (Kluwer Law International 2006), Chapter 12, at 294.

7 The worldwide data protection regulatory landscape

In the digital age, data protection is of increasing concern to governments, individuals and companies alike. All advanced industrial societies face essentially the same dilemma of how to regulate these vast flows of personal information, but their governments have chosen substantially different solutions to do so.[1] [2] Any government regulation in the area of data protection needs to balance the interests of organisations that use personal data against the potential harm such use could cause individuals.

7.1 EU data protection regime

Within the EU the protection of individuals prevailed and the rights of individuals in respect of processing of their personal data became a fundamental human right and freedom.[3] Despite the fierce resistance of

---

1 See Joel Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," in: [2000], Stanford Law Review, at 1315, 1318.

2 For a comprehensive overview of different data protection regimes, see Abraham L. Newman, *Protectors of Privacy, Regulating Personal Data in the Global Economy* (Cornell University Press 2008). The distinction between 'comprehensive regimes' and 'limited regimes' as used in this paper was initially introduced by Newman. See also Prins (Chapter 6, n 9), para 6.4.3.

3 The Council of Europe recognised (certain aspects) of data protection as a fundamental human right in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (**ECHR**) as further specified in Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 28 January 1981 (**Convention 108**), both to be found at <www.conventions.coe.int>. According to its Recital 11, the Data Protection Directive gives substance to and amplifies the data protection principles of Convention 108, which was considered not specific enough to provide for sufficient protection. After adoption of the Data Protection Directive, an additional protocol to Convention 108 was considered necessary as it was thought there were missing elements which the Convention did not provide for, such as (i) a data protection supervisory system and (ii) restrictions on transfer to countries not party to it (see Additional Protocol to Convention 108 (Chapter 6, n 48)). See further Article 8 of the Charter of Fundamental Rights of the European Union (n 10) where the right to data protection was recognised as a separate right (alongside the right of respect for private and family life laid down in article 7).
In *Promusicae (*Case C-275/06 *Promusicae* [2008] ECR I-271), the ECJ acknowledged this status of "a further fundamental right," namely the "right that guarantees protection of personal data and hence of private life." According to the ECJ, "this right is however not absolute but must be balanced against other fundamental rights," see paras. 63, 65 and 68. The status of data protection as a fundamental right and freedom is given a legally binding basis in the recently adopted TFEU (Chapter 6, n 3). The TFEU abolishes the pillar structure and introduces, in Article 16, a provision on data protection with general application, which means that all areas of

many interest groups across the industry[4], the EU subsequently adopted the Data Protection Directive.[5]

7.1.1 Material processing principles

The Data Protection Directive provides for comprehensive data processing rules governing both (part of) the public[6] and the private sector throughout

---

EU law are covered (i.e. also the second and third pillars which are presently excluded from the scope of the Data Protection Directive pursuant to Article 3(2) thereof). Article 16 TFEU is designed to be the central source of data protection within the EU. It mirrors Article 8 of the Charter of the Fundamental Rights of the Union. The constitutional character of data protection therefore now has been made part of the legal framework of the EU. On the development of data protection as a constitutional right in the EU, see P. De Hert and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 1, at para. 1.1.2.

4 See Newman (n 2), at 13, reporting that companies expected at the time that the implementation of comprehensive processing rules would have serious financial implications. Further, nationally oriented companies that relied on information exchange (insurance providers and direct marketers) expected to lose from a reduction in data sharing and to benefit little from the free data transfers which would be created within the EU by harmonisation of the various national laws. Also, multinational companies opposed the new laws as they feared that the data exchange between their EU and non-EU companies would be hindered. Non-EU multinationals feared exclusion from the EU market.

5 Hereafter I will discuss the Data Protection Directive, which forms the main building block of data protection law within the EU. The Data Protection Directive is, however, not the only directive that regulates data protection in the EU. Other EU legislative instruments for regulating data protection are:

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (**e-Privacy Directive**).
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ 2008 L 350.

6 Pursuant to Article 3(2) of the Data Protection Directive, processing operations concerning public safety, defence, state security, and the activities of the state in areas of criminal law, are excluded from the scope of the Directive. The TFEU abolishes the pillar structure and in Article 16 introduces a provision on data protection with general application (see n 3).

the EU. The Data Protection Directive imposes requirements on the "controller" of a data processing.[7] Any processing of personal data has to comply with certain material processing requirements. Though the recitals to the Data Protection Directive do not indicate so, the processing requirements of the Data Protection Directive are clearly inspired by those of the OECD Privacy Guidelines.[8] Personal data must be processed fairly and lawfully[9], collected for specified and legitimate purposes only[10], and the processing of these data must be adequate, relevant and not excessive in relation to the purposes for which the data were collected or further processed.[11] Other fundamental principles of the Data Protection Directive are that individuals should be informed about processing of their data[12], personal data must be adequately secured[13] and individuals should be granted rights of access, rectification and objection to processing.[14]

---

7 Controller means the "(legal) person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of the processing of personal data," (Article 2(d) Data Protection Directive); WP 169 Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010 (**WP Opinion on controller and processor**).

8 OECD Privacy Guidelines (Chapter 6, n 38). The Guidelines prescribe that: Collection of data should be limited, lawful and fair, with knowledge or consent of a data subject (para. 7); data collected should be relevant to the purposes of collection, accurate, complete and up-to-date (para. 8); the purposes of collection should be specified at the time of or prior to data collection and subsequent use should not go beyond declared purposes (para. 9); data should not be disclosed, made available or used for purposes other than those specified unless there is a data subject consent or a requirement of law (para. 10); reasonable security safeguards should be taken against loss or unauthorised access, destruction, use, modification or disclosure of data (para. 11); developments, practices and policies with respect to personal data should be open. Establishing the existence and nature of personal data, and the main purposes of their use, the identity and usual residence of the data controller should be facilitated (para. 12); an individual should have the right to obtain a confirmation from a controller in an accessible manner whether or not the data controller has data relating to him; challenge data related to him, have it corrected, erased, rectified, completed or amended (para. 13); the data controller should be accountable for compliance with the data protection measures (para. 14).

9 Article 6(1)(a) Data Protection Directive.

10 Article 6(1)(b) Data Protection Directive.

11 Article 6(1)(c) Data Protection Directive.

12 Article 10 Data Protection Directive.

13 Article 17 Data Protection Directive.

14 Article 12 and 14 Data Protection Directive.

7.1.2 Scope of applicability

The Data Protection Directive has harmonised various national data protection laws already in force in some EU Member States.[15] The aim of the Data Protection Directive was to work as a single market measure to facilitate the free flow of data within the EU.[16] The wish to avoid gaps in the protection of personal data and to prevent circumvention of the protection of the Data Protection Directive has led EU legislators to provide for a very broad scope of applicability of the Data Protection Directive ("long arm reach"). The main applicability rule of the Data Protection Directive[17] prescribes that the national data protection laws apply in the event a controller processes data 'in the context of the activities of an establishment (of such controller) in the EU'. For applicability of the national data protection laws it is not required that the controller itself is established within a Member State. To avoid the circumvention of the protection of the Data Protection Directive, a second applicability rule[18] was introduced, which provides that the national data protection laws also apply if the controller has no establishment in a Member State at all but "makes use of equipment located within the EU for the processing of data", unless such equipment is used for mere transit purposes only.

7.1.3 EU transfer rules

The wish to also regulate the trans-European data streams has resulted in a further extension of applicability of the Data Protection Directive, where it prohibits data transfers from the EU to countries outside the EU without an adequate level of protection[19] (**EU transfer rules**).[20] The EU transfer rules are not considered to be one of the material processing principles (listed in Paragraph 2.1.1. above), as the transfer rules are a mechanism to ensure that these material processing principles will be observed, rather than being a fundamental processing principle itself.[21] This being said, the transfer rules

---

15 Notably France, Germany and Sweden already had comprehensive data protection laws. On the other hand, Spain, Italy, Portugal, Greece and Belgium had no data protection laws at all.

16 The legal basis for the Data Protection Directive is Article 95 (formerly 100a) EC Treaty (n 3). See further Recitals 1- 9 of the Data Protection Directive.

17 Article 4(1)(a) Data Protection Directive. See on the scope of this applicability rule, Chapter 2.

18 Article 4(1)(c) Data protection Directive. See on the scope of this applicability rule, Chapter 3.

19 Article 25(1) Data Protection Directive.

20 Given the equivalent protection in the Member States resulting from implementation of the Data Protection Directive, the EU transfer rules were not made applicable to transfers of personal data within the EU. See Recital 9 to the Data Protection Directive.

21 This is evidenced by the fact that in the Directive the EU transfer rules are not included in Chapter II (The General Rules on the Lawfulness of the Processing of Personal Data), but in a

are crucial in their own right to guarantee the protection provided by the Data Protection and therefor are a key cornerstone of the Directive.[22] The Directive contains only a limited number of derogations from the EU transfer rules.[23] The European Commission can issue a finding that a certain country provides for an adequate level of protection as a result of which the data transfer rules do not apply to such country (**adequacy finding**).[24] In practice only a limited number of countries have obtained such an adequacy finding.[25] As multinationals typically transfer data worldwide, this derogation is therefore of limited relevance only. The European Commission has further approved specific mechanisms for the regulation of data flows

---

separate Chapter IV (Transfer of personal Data to third Countries). For a similar separation of the basic principles and the transfer rules see the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (**Madrid Draft Proposal for International Standards**), as adopted on 5 November 2009 at The International Conference of Data Protection and Privacy Commissioners in Madrid by the participating data protection authorities, to be found at www.agpd.es, where the transfer rules are included in section 15 and the basic principles of data protection in Part II. See also the OECD Guidelines (Chapter 6, n 38), where the rules on transborder data transfer are included in Part III ('Basic principles of international application: free flow and legitimate restrictions') and the basic principles in Part II ('Basic principles of national application'). Further, see Kuner (Chapter 6, n 8), at 27.

22 See WP 12, Working Document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24 July 1998 (**WP 12**), at 6, where the Working Party 29 lists "six content principles" of which the 6th is: "restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive." Since a restriction on onward transfers was at the time missing from Convention 108, the Working Party 29 considered the protection provided by the countries that had at the time ratified Convention 108 was insufficient (see WP 12, at 8). This led to adoption of a transfer rule similar to the Data Protection Directive in Article 2 of the Additional Protocol to Convention 108 (n 3).

23 For the derogations to the EU transfer rules, see Articles 25 – 26 Data Protection Directive.

24 Articles 25(6) and 31(2) Data Protection Directive.

25 For the countries that have obtained an adequacy finding, see <http://ec.europe.ec/home/fsj/privacy/thirdcountries/index_en.htm>. These are presently: Argentina; Canadian organisations subject to the Canadian Personal Information Protection and Electronic Documents Act (**PIPED Act**); Switzerland; the Bailiwick of Guernsey; the Bailiwick of Jersey; the Isle of Man; Israel; and Andorra. The Working Party 29 issued an opinion that it considers New Zealand as providing for an adequate level of protection. See Opinion 11/2011 on the level of protection of personal data in New Zealand dated 4 April 2011(**WP 182**). The European Commission decision confirming this has not been issued yet.

between the EU and the US. For instance, the Commission has approved data transfers from the EU to the US when an organisation in the US has voluntarily adhered to the US Safe Harbor Framework.[26]

Another ground for allowing a data transfer is obtaining the consent of the individual for such transfer.[27] For consent to be valid it should be "freely given".[28] This requirement entails that an individual should be able to refuse his consent or withdraw it any time.[29] In the case of cross-border transfers of

---

[26] See the European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L215/7. For the US Safe Harbor Principles see <http://www.export.gov/safeharbor/eu/eg_main_018493.asp> (**US Safe Harbor Framework**). Other examples are the agreement between the EU and the US regarding transfers of air passenger name records data (Council Decision 2007/551/CFSP/JHA of 23 July 2007), and the Agreement on Transfer of Financial Messaging Data, n 40.

[27] Article 26(1)(a) Data Protection Directive.

[28] Article 2(h) Data Protection Directive defines consent as "any freely, given specific and informed indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed." Consent implies that the data controller has given the relevant information about the purposes and extent of the data processing for which consent is given.

[29] See WP Opinion 8/2001 on the processing of personal data in the employment context adopted on 13 September 2001 (**WP 48**), at 23: "Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice." That data subjects have the right to withdraw consent is further generally assumed in literature: see Waltraut Kotschy, 'Directive 95/46/EC, General Rules on the Lawfulness of the Processing of Personal Data' in Concise European IT law, Bullesbach, A., Poullet, Y., Prins, Corien, eds., (The Hague, Kluwer Law International, 2006), at 47. In some Member States, the right to withdraw consent has been provided for in the national law. For instance, see Article 5 (1) para. 2 of the Dutch Data Protection Act: "The data subjects or their legal representative may withdraw consent at any time." Along the same lines, in respect of consent of consumers, see Opinion 2/2010 on online behavioural advertising Adopted on 22 June 2010 (WP 171), at 21: "If/when an individual asks for a deletion of his/her profile or if he/she exercises his/her right to withdraw the consent, these actions require the ad network provider to erase or delete promptly the data subject's information insofar as the ad network provider ceases to have the necessary legal grounds (i.e. the consent) allowing the processing." ; Liam Curren and Jane Kaye (2010) "Revoking consent: A 'blind spot' in data protection law?'", Computer Law & Security Review, 26(3), at 278 acknowledge that "it is generally assumed that individuals have a right to withdraw, or revoke, their consent to the processing of their personal data by others," but indicate that there are arguments that the Data Protection Directive may not include such a right." At 282, Curren and Kayne indicate that the UK DPA (the ICO) also interprets the right to withdraw consent narrowly, stating that the latest data protection guide states that it is possible for consent to be

employee data between group companies, obtaining consent is hardly ever an option because employee consent is presumed not to be "freely given" as it is given in the context of a relationship of authority.[30] Also in the consumer context, the validity of consent can be questioned in case of repeated or even structural transfers or if the transfer in question is disproportionate.[31] More in general there is a growing concern that

withdrawn "depending on the nature of the consent given and the circumstances in which [the data controller is] collecting or using the information." However, their subsequent conclusion is that data subjects should have the right to revoke consent, as the lack of such a right "could amount to a major shortcoming if individuals should actually be empowered to exercise control of their privacy in a meaningful way" (at 279 et seq).

[30] See also WP 48 (n 29), at 23: "Where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal information, it is misleading if an employer seeks to legitimize this processing through consent. Reliance on consent should therefore be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment".

[31] See Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 25 November 2005 (**WP 114**), at 11: "Consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question." Even if consent is obtained, the processing by a controller still has to meet the proportionality principle. Though the proportionality principle is not included in the material processing principles (see para. 7.1.1 above), this principle is considered to be inherent in the bulk of these principles (especially in the requirements of Article 6(1) Data Protection Directive that data have to be processed fairly, collected for legitimate purposes only, and must be adequate, relevant and not excessive). Consent may be considered invalid if the processing for which consent is requested is disproportionate. On how the fundamental right to data protection safeguards data subjects and leads to the conclusion that consent has (and should have) a limited value as an independent legal ground for data processing, see Antoinette Rouvroy and Yves Poullet, "The right to Informational Self-Determination and the Value of Self-Development. Reassessing the Importance of Privacy for Democracy," in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 2, at 72–76; and Lee A. Bygrave and Dag Wiese Schartum, "Consent, Proportionality and Collective Power," in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), at paras. 9.3 and 9.4. The Working Party 29 in its WP Contribution on The Future of Privacy (n 33), at 17, recommends to the Commission to specify the requirements of consent taking into account inter alia the following observations: 'There are many cases in which consent cannot be freely given, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when data must be provided to public authorities). In addition, the requirement that consent has to be informed starts from the assumption that it needs to be fully understandable to the data subject what will happen if he decides to consent to the processing of his data. However, the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or

individuals may not understand what they are consenting to,[32] that there is no meaningful default option available if they do not wish to provide consent,[33] and that the granting of consent becomes a mechanical matter of "ticking the box", i.e. becomes subject to 'routinisation' and therefor meaningless.[34] Consent as a structural basis for data transfers within a multinational group of companies is therefore often not feasible.

The main other derogation to the EU transfer rules is that a Member State may authorise a certain transfer of data to a third country which does not provide for an adequate level of data protection, if the controller "adduces adequate safeguards with respect to the protection of personal data".[35] The European Commission has approved the use of EU standard contractual clauses (**EU Standard Contractual Clauses**)[36] for this purpose, which Clauses have to be entered into between the EU data exporting company and the non-EU data importing company.

7.1.4 Third-party processors

If a controller involves a processor[37] to process personal data on its behalf, the controller has to enter into a written[38] data processing agreement with the processor and impose a number of mandatory processing conditions[39]:

---

willingness to make decisions to control the use and sharing of information through active choice" (this is in reference to 'Data Protection Accountability: The essential Elements – A Document for Discussion', Centre for Information Policy Leadership, as Secretariat to the Galway Project, October 2009, at 4). In its turn, the Commission announced that the controls of consent will indeed be strengthened in the revised Directive. See EC Communication on the revision of the Directive (Chapter 6, n 34), at 6 and 9. The EDPS supports this position of the Commission, see EDPS opinion on revision of the Directive (Chapter 6, n 35), at para. 82 at 18.

32 Roger Brownsword, "Consent in Data protection Law," in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 2, at 90, rightfully notes that "until background rights, including the background informational rights have been established, consent has no reference point."

33 Kuner (Chapter 6, n 8), at 20 and 30.

34 On the risks of routinisation of consent, see Roger Brownsword (n 32), Chapter 2, at 90.

35 Article 26(2) Data Protection Directive.

36 The approved EC Standard Contractual Clauses may be found at <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm>.

37 Article 2(e) Data Protection Directive defines a processor as "a (legal) person, public authority, agency or any other body that processes personal data on behalf of the controller."

38 Or other equivalent form. See Article 17(4) Data Protection Directive.

39 Article 17(2) and (3) Data Protection Directive.

(a) the processor may only act on instructions from the controller;
(b) the processor must implement appropriate technical and organisational security measures as defined by the law in which the data processor is established[40] ;
(c) the controller must be entitled to review the security measures taken by the processor and the processor must submit its data processing facilities to audits conducted by the controller in connection therewith.[41]

If a controller in the EU transfers data to a processor in a non-EU country, the EU transfer rules apply. For these transfers the European Commission has approved specific controller-to-processor EU Standard Contractual Clauses.[42]

7.1.5 Jurisdiction and enforcement

Each of the Member States has established a DPA to monitor and enforce compliance with its national data protection law.[43] The DPAs exercise their function with complete independence.[44] The Data Protection Directive has further ensured that each of these DPAs has been endowed with: investigative powers, effective powers of intervention and the power to engage in legal proceedings.[45]

---

40 Article 17(3) Data Protection Directive.

41 This is an implementation of the requirement in Article 17(2) Data Protection Directive that the controller must ensure compliance by the processor with the security measures.

42 The approved EC Standard Contractual Clauses for controller-to-processor transfers are also to be found at <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm>. The latest EU Standard Contractual Clauses for controller-to-processor entered into force on 15 May 2010 and now also facilitates the onward transfer by the non-EU based processor to non-EU based sub-processors (**EU Standard Contractual Clauses for Processors**). On these new EC Standard Contractual Clauses, see Christopher Kuner, "The New EU Standard Contractual Clauses For International Data Transfers to Data Processors," Privacy & Security Law Report, 19 April 2010, at 1-7.

43 Article 28(1) Data Protection Directive.

44 Recital 62 and Article 28(1) Data Protection Directive. See further Article 8(3) TFEU. See in more detail on the requirement of independence of DPAs (and the lack thereof in some Member States), para. 14.7.5.

45 Article 28(3) Data Protection Directive.

Jurisdiction to hear claims

The jurisdiction system under the Data Protection Directive for hearing claims by the DPAs is based on the protection principle. Any person (regardless of nationality) who wishes to file a claim concerning his rights under the Data Protection Directive may do so with any DPA, regardless of the applicable law.[46] If the relevant DPA requires the assistance of another DPA to decide on the claim (for instance as the claim is governed by the law of another Member State or if the actual processing takes place in another Member State), such other DPA has to provide all relevant information and assistance.[47]

Decisions by the DPAs may be appealed before the courts.[48]

Jurisdiction to enforce

Concerning the enforcement powers of the DPA, the rule of jurisdiction is based on the territoriality principle: each DPA has jurisdiction in its own territory. Conversely, DPAs cannot enforce their powers outside their territory. The Data Protection Directive provides jurisdiction regardless of the applicable law (this may even be non-EU law).[49] This is relevant as the applicability regime of the Data Protection Directive (see Paragraph 7.1.2 above) may well lead to the applicability of the laws of another Member State than the Member State where the data processing takes place.[50] As a result, whenever these powers may be exercised (i.e. because a processing takes place in the relevant territory or if a controller is established in the relevant territory), the DPA of the relevant Member State has jurisdiction. By this provision the Data Protection Directive ensures that there is always one DPA that can actually exercise its powers. Otherwise the DPA where the individual has filed his claim cannot exercise its powers, as for instance the

---

46 Article 28(4) Data Protection Directive: "Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim."

47 Article 28(6) Data Protection Directive: "The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."

48 Article 28(3) Data Protection Directive.

49 Article 28(6) Data Protection Directive: "Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with para. 3. Each authority may be requested to exercise their powers by an authority of another Member State."

50 For instance, if the controller is established in one Member State and involves a processor in another Member State to process data on its behalf.

relevant processing or assets are not in its territory. By ensuring that such DPA can request the assistance of the DPA that can exercise[51] its powers, effective enforcement is ensured throughout the EU (i.e. enforcement is based on a "network approach").

Redress to the courts

The Data Protection Directive has further ensured that all Member States allow for the possibility of individuals to seek redress, and corrective action, though the courts.[52] This includes both the possibility for individuals to obtain damages by means of court action, and the possibility to obtain a court order to remedy a breach or refrain from further violations. These judicial remedies are without prejudice to the enforcement powers of the DPAs discussed before.[53]

Working Party 29

The Working Party 29 was established as an advisory body to the European Commission under Article 29 of the Data Protection Directive. The Working Party 29 has advisory status only and acts independently.[54] Members are representatives of each of the DPAs, of the European Data Protection Supervisor and of the European Commission. The tasks of the Working Party 29 are to issue opinions to "contribute to the uniform application of the Data Protection Directive and [to] advise(...) on proposals for EU legislation having an impact of data protection."[55] The Working Party 29 further coordinates and facilitates cross-border enforcement actions by the DPAs, but has no enforcement powers itself. Though the opinions of the Working Party 29 are non-binding, they are followed in practice by the DPAs and *de facto* set the rules for application of the Data Protection Directive. See on the role of the Working Party 29 in more detail Paragraph 10.6.6, and on its tasks and procedural rules Paragraph 14.7.2 - 14.7.4.

7.1.6 Self- and co-regulation

The Data Protection Directive explicitly encourages the drawing up of codes of conduct as a useful instrument to contribute to the proper implementation of the national data protection provisions, taking into

51 Article 28(6), last sentence, Data Protection Directive.

52 Articles 22 and 23 Data Protection Directive.

53 Article 22 Data Protection Directive.

54 Article 29(1) Data Protection Directive. See para. 14.7.3 on the (lack of) independence of the Working Party 29.

55 See the Document "Tasks of the Working Party 29", as published at <www.ec.europa.eu>.

account the specific features of the various sectors.[56] As some of the material processing principles in the Data Protection Directive are of a general nature, the European legislator considers it desirable that such general principles are further detailed when applied to the data processing as part of the services of a specific sector. To ensure compliance of such codes of conduct with the Data Protection Directive, trade associations and other bodies representing groups of controllers may submit their codes to the opinion of their national DPA. The DPA may seek the views of the beneficiaries of these codes or their representatives.[57] European codes of conduct may be submitted to the Working Party 29 for opinion and also the Working Party 29 may seek the views of the beneficiaries or their representatives.[58] Though the use of codes of conduct is encouraged by European legislators and the Working Party 29, the number of codes actually adopted is at this time very limited and – with two exceptions[59] – are at Member State level only.[60]

7.2 Other comprehensive regimes

The EU transfer rules have prompted many non-EU countries to follow suit in adopting comprehensive data protection legislation[61] to ensure that their multinational companies retain access to the EU market.[62] Some of the

---

56 See Recital 61 and Article 27 Data Protection Directive.

57 Article 27(2) Data Protection Directive.

58 Article 27(3) Data Protection Directive.

59 The two organisations that achieved European validation of their codes of conduct so far are: the Federation of European and Interactive Marketing (FEDMA) and the International Air Transportation Association.

60 On the lack of uptake of self-regulatory codes, see Sjaak Nouwt, "Towards a Common Approach to Data Protection," in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 17, at para. 17.5.

61 Presently about 60 countries have comprehensive data protection legislation (including the majority of the OECD countries), see <www.privacyinternational.org> and <www.mofoprivacy.com>. Kuner (Chapter 6, n 18), at para. III, estimates that of the 192 Member States of the United Nations about 50-60 currently have a legal framework for data protection. For a comprehensive overview of about 60 countries that have data protection laws, see Miriam Wugmeister, Karin Retzer, Cynthia Rich, "Global solution for cross-border data transfers: making the case for corporate privacy rules," [2007] Georgetown Journal of International Law, Vol. 38, at 449 – 498. On the process of how the EU influenced other countries in adopting EU-based data protection laws, resulting in a shift toward the comprehensive system, see Newman (n 2), Chapters 4 – 5.

62 Büthe, T. and W. Mattli, *The New Global Rulers:The Privatization of Regulation in the World Economy*, Princeton University Press 2011, at 34 (and literature referred to in footnote 53): "In

countries that have introduced comprehensive data protection laws have chosen the EU regulatory system explicitly as a starting point.[63]

The states that have introduced a comprehensive system all struggle to regulate transnational data flows, which results in many of these states adopting a similar "long arm reach" as the Data Protection Directive. In addition, many of these countries have imposed similar restrictions on the outbound transfer of personal data from their countries to countries that do not provide an adequate level of data protection.[64]

7.3 Limited regimes

Other countries (including the US and many countries in Asia) have taken a limited approach to data protection.[65] The limited regimes[66] mostly focus on

---

the realm of data protection for e-commerce, regional standards developed in Europe at the EU level, largely won out over U.S. standards as the global standards after a period of (...) competition among public regulators, because firms that are engaged in transnational e-commerce were ultimately more concerned with adopting a single set of privacy standards for their increasingly global operations. United States databases with consumer information whose commercial use was illegal under EU standards thus lost most of their value."

63 This applies especially to countries in South America.

64 Countries with outbound transfer requirements include: Australia; Switzerland; Argentina; Mauritius; Russia; Singapore; South Korea; Hong Kong; Iceland; Israel; Taiwan; Thailand; Tunisia and the United Arab Emirates. Canada and Japan also *de facto* impose cross-border transfer rules as under their laws the party transferring personal data to a third party (wherever located) remains accountable for the processing of the data. As a consequence, the party transferring the data will normally have to impose contractual data protection obligations on the third party to guarantee that such third party will provide the required level of protection. For a comprehensive overview of countries with data transfer requirements, see Kuner (Chapter 6, n 8) Annex I at 55 and Wugmeister, Retzer and Rich (n 61), at II sub C at 457 -461.

65 During the 1970s and 1980s, the comprehensive systems and limited systems were in relative parity. Countries which initially took a limited approach but have now moved to comprehensive systems are: Australia; Canada; Japan; Czech Republic; Switzerland; Lithuania; New Zealand; and Slovakia. Countries considering legislative reform based on the Data Protection Directive include Hong Kong and several jurisdictions in Latin America, such as Chile and Ecuador. Limited systems are still in place in the US, Korea and Thailand. For a comprehensive description of systems with a comprehensive approach and systems with a limited approach, see Newman (n 2), Chapter 2. For a further comprehensive overview of the 60 countries that have data protection laws, see Wugmeister, Retzer, Rich (n 61), at para. II A.

66 Many (further) categorisations are possible. See for instance Cécile De Terwangne, "Is a Global Data Protection Regulatory Model Possible?", in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 10, at para. 10.3, using a further categorisation of the

the public sector (shaping the processing and transfer of personal data among governmental agencies) and a select number of sensitive industries (most notably healthcare and telecommunications). These limited systems generally permit the processing and transfer of personal data and rely on market mechanisms to check inappropriate processing activities. In these countries the protection of personal data is left to be driven by consumer demand and by industry self-regulation,[67] with patchy results at best. Under the EU transfer rules, these limited regimes are not considered as providing an adequate level of protection for the processing of personal data in those countries and a transfer of personal data from the EU to those countries constitutes a violation of the Data Protection Directive.

7.4 APEC Privacy Framework

In 2005, the APEC Member Economies (which include Australia, Canada, China, Japan and the US)[68] adopted the APEC Privacy Framework.[69] The APEC Privacy Framework provides for similar material processing principles[70] as the Data Protection Directive. However, for a number of reasons the APEC Privacy Framework is not expected to lead to an adequate

---

limited systems alongside the comprehensive model (the piecemeal model, the sector-oriented model and the risk-burden balance model).

67 Newman (n 2), at 24. For a comprehensive overview of the US on the "patchwork of privacy regulation and the lack of a dedicated privacy enforcement agency," see Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Books and on the Ground," in Stanford Law Review, Vol. 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385, available at SSRN: <http://ssrn.com/abstract=1568385, at 103–114>. Also in the US is a strong call for adopting 'omnibus privacy statutes' based on the model adopted throughout Europe, see Bamberger and Mulligan (above), at 104. For further reading on the US approach of relying on a combination of sectoral law, market forces and self-regulation, reporting that the Department of Commerce and the Federal Trade Commission expressly favour a self-regulatory approach, see Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* (March 1, 2010), NYU School of Law, Public Law Research Paper No. 10-16. Available at SSRN: <http://ssrn.com/abstract=1510275>, at 2.

68 APEC is the Asia-Pacific Economic Cooperation, which is an intergovernmental form in the Asia-Pacific region. At present 21 countries are Member Economies.

69 APEC Privacy Framework (Chapter 6, n 38).

70 The main APEC Privacy Principles are: (I) preventing harm; (II) notice, providing for the information rights of individuals; (III) collection limitation, similar to the data minimisation principle; (IV) uses of personal information, combining purpose limitation and lawfulness principles; (V) choice, expressing the principle of self-determination; (IV) integrity of personal information; (VII) security safeguards; (VIII) the right of access and correction; and (IX) accountability.

level of protection as required by the Data Protection Directive. First of all, the APEC Privacy Framework is voluntary[71] and it is unclear how many Member Economies will indeed implement it. The APEC Privacy Framework explicitly recognises that in view of differences in social, economic and legal backgrounds of Member Economies, the principles may be implemented in different ways. At present many APEC Member Economies already have their own data protection laws which are very diverse in nature. This divergence is likely to be continued.[72] The APEC Privacy Framework may be implemented through self-regulation[73] and the APEC principles are subject to derogation by mandatory rules of national law (for instance, the state control powers of such country).[74] It is therefore not to be expected that in the near future the APEC Privacy Framework will provide an adequate uniform level of data protection throughout the APEC region.[75]

The data transfer rules in the APEC Privacy Framework merit specific discussion. These are based on the "accountability principle". Principle 26 of the APEC Privacy Framework provides that if a controller transfers personal data to third parties, the controller remains accountable for taking reasonable steps to ensure that the relevant third party will protect the information consistently with the APEC principles. As a consequence, some form of central enforcement is introduced. Data subjects can address the original controller for breach of this obligation rather than the third-party recipient for a breach by such third party, which de facto results in centralising enforcement to a certain extent.[76] A more or less similar result is achieved under Japanese law[77] and the Canadian PIPED Act.[78] The data

---

71 See APEC Privacy Framework, preamble para 4, where it is noteworthy that the APEC Privacy Framework carefully avoids the word 'right',

72 Kuner (Chapter 6, n 8), at 21.

73 APEC Privacy Framework (Chapter 6, n 38), at 3 4.

74 APEC Privacy Framework (Chapter 6, n 38), at 8.

75 Chris Pounder, "Why the APEC Privacy Framework is unlikely to protect privacy," to be found at <www.out-law.com>; Lee Bygrave, "International Agreements to Protect Personal Data" in: James B. Rule and Graham Greenleaf, *Global Privacy Protection: The First Generation* (Edward Elgar Publishing 2009), at 44-45. Kuner (Chapter 6, n 8), at 22 -23; De Terwangne (n 66), at 181 and 183, gives a good overview of all critiques about the weaknesses of the APEC Privacy Framework.

76 Otherwise, enforcement under the APEC Privacy Framework (Chapter 6, n 38) is also based on the principle of cross-border cooperation between national data protection supervisors rather than central supervision, see Annex B sub II and III of the APEC Privacy Framework.

77 Kojin Joho Hogo Ho (act on the Protection of Personal information), law No. 57 of 2003, unofficial translation to be found at <www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.

protection laws in Japan and Canada do not distinguish between domestic and cross-border transfers to third parties. They apply the same rules, regardless of the location of the third party. These laws require that organisations remain accountable for information that is in their possession or custody, also after this information has been transferred to a third party.[79] At first sight, this seems to provide for a more extensive accountability of the original controller (i.e. for the outcome) than under the APEC Privacy Framework (where the original controller is only accountable for taking reasonable steps to ensure protection). However, case law indicates that also under the PIPED Act the original controller is only accountable for ensuring that adequate contractual or other means are in place (rather than for the outcome itself).[80] Also in Japan, organisations must establish contracts with

---

78 Canadian Personal Information Protection and Electronic Documents Act (**PIPED Act**), to be found at <http://laws.justice.gc.ca/eng/P-8.6/page-1.html>.

79 See PIPEDA (n 78) Section 5, 4.1.3 first sentence: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing."

80 See 5, 4.1.3, second sentence: "The organisation shall use contractual or other means to provide a comparable level of protection while the information is processed by a third party." See further the Decision of the Office of the Privacy Commissioner of Canada of 02 April 2007 on the complaint of Ms Philippa Lawson (available at <http://www.cippic.ca/documents/privacy/pipeda-complaints/OPCC_Letter_re_National.pdf>). This Decision illustrates that under Principle 4.1.3 of Schedule 1 of PIPEDA, the Canadian exporter of personal data is only responsible for the measures it takes to ensure "a comparable level" of data protection, rather than for the actual outcome. The complaint was filed against National Bank of Canada that transferred personal information to SWIFT established in the US for processing of monetary transfers which, in turn, disclosed some information pertaining to Canadian citizens to the US government for counter-terrorism purposes without seeking consent of those individuals or informing them. The Office of the Privacy Commissioner stated that "the banks did not disclose the information, SWIFT did. The contractual language between the banks and SWIFT clearly places responsibility for responding to such subpoenas in the hands of SWIFT; the banks notify their customers of the possibility of such disclosures by way of their respective privacy policies. Given that SWIFT was responsible for the disclosures, not the banks, the issues of the purpose for the disclosures and of the lack of consent are dealt with in the Commissioner-initiated complaint against SWIFT (…)." (at 13). Therefore, National Bank of Canada was not found responsible for the outcome of transfer of personal data. The Office of the Privacy Commissioner did, however, examine the measures the bank took to secure "a comparable level of protection" (at 3-13). In particular, the Office of Privacy Commissioner finds that "CIBC has in place a contract with its third-party service provider that provides guarantees of confidentiality and security of personal information. The contract allows for oversight, monitoring, and an audit of the service being provided." (at 13) The Office points out that "at the very least, a company in Canada that

service providers and other third parties that contain certain specific data security provisions.[81] A similar approach is chosen in the draft Australian Privacy Principles.[82]

outsources information processing to a company that operates in the US should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country, National Bank has clear language in its Confidentiality Policy, which informs customers [of such a possibility.]" (at 12). The Office concludes that what the Act demands is that when outsourcing data processing to service providers in other countries, "organizations be transparent about their personal information handling practices and protect customer personal information in the hands of third-party service providers to the extent possible by contractual means." (p. 13). In the case at hand, the National bank did meet those requirements.

81 Article 22 APPI.

82 See the Draft Australian Privacy Principles (Chapter 6, n 52). Also the Exposure Draft introduces a general accountability principle and makes clear that this also applies in case the data are transferred abroad. See Part B, section 19 of the Exposure Draft: "This Act extends to an act done, or practice engaged in, outside Australia by an agency. This Act and an approved privacy code extend to an act done, or practice engaged in, outside Australia by an organisation that has an Australian link."

8 Trends and developments in the legal landscape

8.1 Increasing tension between different regulatory systems

With the increased data exchange inherent to the digital era, the diverse national regulatory systems are increasingly in contact with one another and the differences in approach have become an increased source of economic and security disputes between nations.[1] The economic debate concentrates on the limited regimes claiming that the future of e-commerce depends on the free flow of data; the comprehensive regimes claiming that the future of e-commerce depends on individuals being prepared to participate in e-commerce activities only if their privacy has been guaranteed against business and government surveillance.[2] After 9/11 this economic debate has transformed into a security debate about the information requirements of the *war on terrorism*. Tension between the US and the EU came to a height when the US introduced the Patriot Act, expanding the state policing powers to counter terrorism. As a result of heightened security concerns, the US government has claimed access to increasing amounts of data processed about foreign citizens.[3] This increasingly presents multinationals with catch-22 situations where (especially) US government institutions require transfers of personal data of EU citizens while these transfers are outright violations of EU transfer rules.[4] A very public example is the SWIFT case. Following several press reports in June 2006,[5] it was revealed that the US Department of the Treasury had served administrative subpoenas on the Society for Worldwide Interbank Financial Telecommunication (**SWIFT**) in order to transfer personal data located on SWIFT's server in the US for

---

1 For the recent increase in surveillance across countries, see the study by Privacy International, "European Privacy and Human Rights 2010", to be found at http://www.privacyinternational.org/ephr.

2 Newman (Chapter 7, n 2), at 12 - 14.

3 This increase in surveillance is not limited to the US. This is also an issue in the EU. For an overview of the EU security data exchange policies and the data protection implications, see the Tenth Annual Report of the Article 29 Working Party on Data Protection, at 7-8 (to be found at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm>). In 2004, the EU and US finally entered into an agreement on the much debated transfers to the US Department of Homeland Security of 'passenger name records of air passengers' travelling from Europe. Until then these transfers lacked a legal basis under the Data Protection Directive.

4 On these data protection issues, see Lokke Moerel, Jeroen Koeter and Nani Jansen, "U.S. Subpoenas and European Data Protection Legislation," in US Privacy & Data Security Law Journal, July 2009, at 649-659.

5 U.S. Secretly Tracks Global Bank Data, Los Angeles Times, 23 June 2006, Bank Data Is Sifted by U.S. in Secret to Block Terror, New York Times, 23 June 23 2006.

counter-terrorism purposes. SWIFT is a cooperative society under Belgian law that is owned by European financial institutions. It operates a worldwide financial messaging system in relation to financial transfers between financial institutions. The information processed by SWIFT concerns messages on the financial transactions of EU citizens, amounting to more than 12 million messages on a daily basis. These messages contain without question personal data of EU citizens. The Working Party 29 issued an opinion on the transfers of personal data by SWIFT based on the subpoenas issued by the U.S. Treasury Department.[6] The Working Party concluded that SWIFT and the financial institutions that use SWIFT's services, had breached European data protection laws by transferring the personal data to the US without ensuring adequate protection of such data and by failing to inform the individuals concerned about how their personal data were being (subsequently) processed. In hindsight, it is clear that SWIFT found itself in a conflict of law position between applicable U.S. laws (granting U.S. authorities certain powers to seize data) and European data protection requirements. To avoid further violations of data protection, SWIFT transferred its data processing facilities from the US to Switzerland. In 2010, the violation was remedied in the Agreement between the EU and the US on the processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Program.[7]

As indicated, the catch-22 situation SWIFT found itself in is not unique. To date, many EU-based companies have encountered similar situations where US supervisory authorities such as the SEC, FTC, OFAC, the US Department of Justice or the US Department of the Treasury request information from their US group company, whether on a voluntary basis prior to such authority deciding whether to institute an official investigation, based on a criminal or administrative subpoena, or on the grounds of various specific statutes.[8] Often, the information requested may involve handing over e-mail correspondence between the US group company and its EU parent company, whose e-mail correspondence is often (centrally) stored on a server located at the parent company. EU data protection laws apply to such data. A company may also find itself facing similar dilemmas outside the realm of criminal or government investigations. This could be the case when a civil

6 Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Security for Worldwide Interbank Financial Telecommunication (SWIFT) adopted on November 22, 2006, 01935/06/EN WP128.

7 See Chapter 6, n 40.

8 A subpoena could be issued on the grounds of various statutes, including the Patriot Act, Foreign Intelligence Surveillance Act, the Stored Communications Act, or on the basis of National Security Letters.

suit is filed in the U.S. and data originating from the EU has to be presented for pre-trial discovery.[9] Incidents are not limited to the EU and the US. More in general, there are a growing number of incidents where foreign governments use their state control powers and demand access to foreign data. China, for example, requires service providers doing business in China to reveal data to Chinese law enforcement authorities and India has refused to allow BlackBerry handheld communication devices as the data are encrypted, demanding that entities offering communication services in India also maintain communications equipment in India facilitating real time access to corporate messages by the Indian government.[10]

8.2 Towards a global standard for data protection?

At present there is no treaty, convention or other instrument that is legally binding and which regulates data protection on a global basis.[11] The only

---

9 The Hague Evidence Convention provides a standard procedure through which the court of one country can request assistance from the designated central authority of another in obtaining relevant information in civil and commercial matters. Please note that not all EU member states are a party to The Hague Evidence Convention and some contracting Member States (like France, Spain, the Netherlands and Germany) have filed a reservation under Article 23 thereof, with the effect that pre-trial discovery of any information is not allowed in relation to foreign legislation. There are no multilateral treaties that regulate the cross-border exchange of information in regard to the type of subpoenas that fall within the scope of this paper. However, arrangements can be made per sector. For example, the Dutch Financial Supervision Act allows for the Dutch National Bank to provide information on possible violations of certain U.S. and other laws to its U.S. counterparts.

10 See the BBC article and the New York Times Google Inc. profile mentioned in Chapter 6, n 41.

11 The conventions that contain a binding right to data protection are on a regional rather than global basis, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, as further specified in Convention 108 for the Protection of Individuals with Regard to the Automatic processing of Personal Data of 28 January 1981 (both to be found at <www.conventions.coe.int>), which Convention 108 has been completed 10 years later by the Additional Protocol to Convention 108 (Chapter 6, n 48). Convention 108 has been ratified by 43 countries mainly in Europe and the Additional Protocol to Convention 108 by 30 countries. This is the state per January 2011, see the statistics of ratification of or accession to the Convention 108 at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=18/02/2011&CL=ENG> and to the to the Additional Protocol at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=3&DF=14/01/2011&CL=ENG>.
Also the Charter of Fundamental Rights of the European Union of 12 December 2000, [2000]

global data protection instruments issued to date take the form of non-binding guidance documents.[12] Although there is a persistent call for a binding international global standard for data protection[13] and there are some concrete initiatives in this respect[14], it is generally not expected that

---

OJ C364/01 (to be found at <www.europarl.europa.eu>), has become binding after TFEU came into force in December 2009.

12 OECD Guidelines on the Protection of Privacy and Transborder Flows of personal Data (1981) (n 38); the UN Guidelines concerning Computerized personal Data Files of 14 December 1990 (Chapter 6, n 48).

13 On the desirability of introducing a global legal framework for data protection and the initiatives in respect thereto and prospects thereof, see Kuner (Chapter 6, n8), at 307. The first initiative of relevance dates from 2005, when the 27th International Conference of Data Protection and Privacy Commissioners issued the 'Montreux declaration' which appealed to the United Nations to prepare a binding legal instrument detailing the right to data protection and privacy as enforceable human rights, to be found at <www.privacyconference2005.org>. This appeal was repeated at the 2008 conference, to be found at <www.privacyconference2008.org>. See further the Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, adopted by the OECD Council on 12 June 2007, at 4-5, which also stresses the need to reach a common protection of personal data throughout the world, to be found at <www.oecd.org>. Much attention was further received by the call for global privacy standards for online privacy worldwide by Peter Fleisscher (the Chief Privacy Officer of Google) in his blog of 14 September 2007. Many commentators doubted the true intentions of Google. See Nouwt (Chapter 7, n 60), at 286 and 291. See for an overview of the criticisms: De Terwangne (Chapter 7, n 66), at 175. See further for an overview of the various calls for international harmonisation and international standards wherever possible in respect of the broader context of the on-line environment, which also included calls for global standards in respect of the free flow of information while protecting the privacy thereof: Prins (Chapter 6, n 9) Chapter 6, at para. 6.2. The first call for global principles in EU context seems to have been at the EU Ministerial Conference 'Global Information networks: Realising the Potential', where Ministers of 29 EU member states agreed on Recommendation 46: 'Ministers agree to work together towards global principles on the free flow of information whilst protecting the privacy and personal and business data, building on the work undertaken by the EU, the Council of Europe, the OECD and the UN', to be found at
<http://europa.eu.int/ISPO/policy/isf/documents/declarations/Bonn-Ministerial-Declaration.htm>. See recently (4 May 2010) The Stockholm Program, An open and secure Europe serving and protecting citizens, OJ C115, 04/05/2010 at para. 2.5 at 11, where the European Council recommends that "the Union must be a driving force behind the development and promotion of international standards for personal data protection, based on relevant Union instruments on data protection and the 1981 Council of Europe Convention on the Protection of Personal Data, and in the conclusion of appropriate bi-lateral instruments."

14 See the Madrid Draft Proposal for International Standards (Chapter 7, n 21). At the same time, there are also discussions in relation to the future revision of Convention 108 of the Council of

such a global standard will be realised within the coming 10 years. The present regulatory landscape is considered still too diverse for such a standard to be acceptable for adoption on a global level.[15] It is clear that the many instances of "soft law" in the data protection area show a large number of common denominators[16] which is typically a stepping stone to hard law.[17] The international consensus, however, seems more to be focused on the objectives (i.e. the data protection to be achieved) than on the means to achieve such protection, on which the views differ widely.[18] The way forward

---

Europe and of the OECD Privacy Guidelines. See EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at 6.

15 Bygrave (n 75), at 48 -49. See also (citing Bygrave) Kuner (Chapter 6, n 18), para. IV; and Prins (Chapter 6, n 9), at 173. At 196 -199, Prins further identifies a number of criteria based on which it can be evaluated whether a certain area is suitable for regulation at an international level. Based on her analysis the question is justified whether data protection is inherently suitable for issuing global standards at all. The EDPS seems more optimistic as to a global standard, see EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at 6 and 25 recommending the European Commission to facilitate the achievement of such Madrid global standards and to ensure consistency with initiatives to revise Convention 108 and the OECD Privacy Guidelines (see n 12).

16 See De Terwangne (Chapter 7, n 66), at para 10.5 for an overview of the existing international and regional standards and at para. 10.5.2 for a listing of the 'admitted core data protection principles' that are part of universal data protection standards:

- Collection Limitation Principle
- Data Quality principle
- Purpose Specification and Limitation/Use Limitation Principle
- Non-discrimination (Sensitive Data)
- Security Principle
- Openness Principle
- Individual Participation Principle (Right of Access and of Correction)
- Responsibility / Accountability Principle
- Proper Level of Protection in case of Transborder Data Flows.

See also the Centre for Information Policy leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 4: "Beneath some different language, there is in fact a surprising amount of common ground across the issues raised in the Communication and reforms now under active discussion in the USA, notably in response to thinking within the Federal Trade Commission and the Department of Commerce and at Congressional level."

17 See n 67.

18 See, for example, the comment in the Welcome Speech of the Australian Federal Privacy Commissioner Malcolm Crompton at the 25th international Conference of Data Protection and Privacy Commissioners (10 – 12 September 2003 in Sydney: "If we look around the world we can see the different ways that countries are seeking to meet this dynamic challenge[i.e. effective

is therefore first and foremost "to work towards achieving 'policy operability' at the international level: 'That is, agreeing on goals a policy should achieve, while recognising that nations may adopt somewhat different policy means to implement the goals'.[19] The OECD takes this view in a guidance document on privacy in the on-line environment issued in 2003[20]:

> "There is a broad consensus on the important role of privacy protection in building trust in the on-line environment. Effectively protecting privacy on-line and ensuring the continued transborder flow of personal data are shared objectives. The means by which those objectives may be achieved are viewed differently in member countries. There is agreement however, that there is no uniform solution. A mix of regulatory and self-regulatory approaches blending legal, technical and educational solutions that suit the legal, cultural and societal context in which they operate holds the promise to provide effective solutions that, beyond the objective of building bridges, go to the actual integration of different elements into viable solutions."

In line with these OECD guidelines, the expectation is that private sector instruments (like BCR under the Data Protection Directive and CBPR under the APEC Privacy Framework) will assume increasing importance in the coming years.[21] In Paragraph 6.2 I discussed that the organisational-based data transfer tools BCR and CBPR are an important common factor of the Data Protection Directive and the APEC Privacy Framework and are

---

privacy protection], taking into account their particular culture and history" (...) and we must be prepared to explore a number of possible ways in which privacy can be respected"). See also the PIPEDA Guidelines for processing personal Data across Borders (January 2009), at 3: 'In contrast to this state-to-state approach, Canada has, through PIPEDA, chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However, under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement."

19 See Prins (Chapter 6, n 9), at 194, and especially footnote 156. See also the Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 3 and 8: "The Centre certainly agrees that higher priority should go on harmonising regulatory approaches in practice than on substantive laws."

20 *Privacy Online. OECD Guidance on Policy and Practice* (OECD Publishing 2003), at 4, to be found at <www.oecdbookshop.org>

21 See Kuner (Chapter 6, n 8) at 24; and Prins (Chapter 6, n 9), at 173: "A final remark is that the case of personal data protection is also a fine illustration of the role that soft law (codes of conduct, privacy policies, corporate rules, privacy seals and trust marks) and the actors involved therein can play in establishing a certain degree of international protection."

therefore expected to fulfil an important bridging function between these two systems in the near future.

While a global standard is not yet to be expected, a global standard should in any event not be taken as the holy grail for all international jurisdiction and enforcement issues as presently seen in the data protection field.[22] The limitations of law as a means of controlling international business are much more endemic than calls for global standards imply.[23] The chances of effective enforcement of global standards are limited if at the national level regulatory enforcement proves patchy, whether this is due to lack of effective institutional means, lack of resources, penalties that are treated as a business cost or a license to be paid rather than a deterrent[24] or damages that are difficult to quantify or are too small to be bothered with on an individual scale.[25] At the international level additional complicating factors play a role, such as cultural differences and the prioritisation by national governments of national commercial or other interests above regulatory enforcement of global standards.[26] The latter factor is, however, not

---

22 See Prins (Chapter 6, n 9), at para. 6.5, for a comprehensive discussion of the standard arguments used to justify the quest for international regulation in the on-line world (including data protection).

23 See Doreen McBarnet, "Corporate social responsibility beyond law, through law, for law: the new corporate accountability," in McBarnet, Voiculescu, Campbell (eds.), *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 44-45.
This is even the case in the EU, see the Rand Report (Chapter 6, n 27), at 35. See also Charles Raab and Bert-Jaap Koops, "Privacy Actors, Performances and the Future of privacy Protection," in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), at 216; Wugmeister, Retzer, Rich (Chapter 7, n 61), at 470.

24 In my experience, many companies see threats of potential data protection violations as a possible cost rather than a deterrent. It is therefore not surprising that the Working Party 29 recommends to include in the revised Data Protection Directive a uniform approach as to the sanctions the Member States are to implement to ensure that all DPAs will have the necessary powers, including the power to impose financial sanctions, see WP Contribution on The Future of Privacy (n 33), para. 90.

25 Colin David Scott, Enforcing Consumer Protection Laws (July 30, 2009), UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 15/2009, available at SSRN: http://ssrn.com/abstract=1441256, at 4, also published in: Howells, Geraint, Iain Ramsay and Thomas Wilhelmsson (eds). *Handbook of International Consumer Law and Policy*. Cheltenham: Edward Elgar 2010. This is also the main cause identified for the lack of enforcement of data protection, see in more detail para. 8.3, in particular the citations from the Rand Report in n 46.

26 McBarnet (n 23), at 45-46.

expected to play a major role in the data protection arena, in the sense that data processing industries would transfer to 'data havens' where enforcement would have no priority.[27] Even today, when there are many jurisdictions with lax or no privacy safeguards at all, there is little hard evidence of a widespread transfer of data processing industries to such data havens.[28] To the contrary, jurisdictions with lax data protection laws often also have excessive state control powers. Multinationals, when having to decide in which jurisdiction to locate their central data processing facilities, in practice tend to avoid these countries.[29]

Further, a well-known downside of international/global regulation as opposed to national regulation is that it excludes any competition between national regulations which curtails regulatory innovations, this while there is an increasing need to continuously adapt existing rules in view of rapidly changing circumstances and views.[30] For instance, if the EU data transfer

---

27 This is a fear expressed in the First Report on the Data Protection Directive (n 26), at 19: "An overly lax attitude in Some Member States (…) risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export."

28 Kuner (n 8), at 31; and Prins (n 9), at 181, both referring to Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* (MIT Press 2006), at 279.

29 This is based on my experience as a practitioner when advising multinationals on how to structure their worldwide data processing facilities. About 10 years ago, many EU based multinationals transferred their central data processing operations to the US, mainly for cost reasons (cheap electricity). Due to the enactment of the US Patriot Act, granting the US government authorities the right also to request transfer of data of foreign citizens, many EU based multinationals transferred critical data processing facilities back to the EU. The highest profile example is SWIFT, see (n 40). See also Burk (n 30), at 266 and footnote 20: "The certainty offered by a well-developed body of relevant law may in many instances offer greater business value than would relaxed regulation of information distribution." See on the phenonemon of a regulatory "race to the top" whereby more stringent national or regional regulatory standards become the de facto global standard (with a permament divergence by a small group of countries with weak domestic political and legal institutions and little concern for their international reputation), Büthe and Mattli (Chapter 7 n 62), at 24, in particular the research referred to in footnote 16.

30 Prins (n 9), at para 6.6; Dan L. Burk, "Comment on 'Should ICT Regulation Be Undertaken at an International Level?'", in Bert-Jaap Koops et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), para. 9.3, at 266 - 267: "(…) an international agreement forces international business to operate in a world where 'one size fits all'. Opportunities for jurisdictional experimentation and innovation are curtailed" and concluding that the international inefficiencies resulting from an international agreement "may be no less serious than the inefficiencies resulting from a lack of co-ordination." For a similar

rules had been universally adopted around the globe, the alternative solution of accountability for data transfers (as adopted under the APEC Privacy Framework) would not have come into existence. The latter system may well prove in practice to be the better solution (see on this Paragraph 13.6). Any global standard should therefore in any event be limited to setting general principles, leaving any detailed rules to secondary regulation which can be amended more quickly, if changing circumstances so require.[31] From this perspective, the present "common ground" on "core data protection principles"[32] may therefore already be sufficient for a global standard to materialise.[33] In light of the "data explosion" the world presently

---

observation in the context of company law, see The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe, Brussels, 4 November 2002, to be found at <http://ec.europa.eu/internal_market/company/modern/index_en.htm>, at para. 2, observing that the system in the EU of harmonising company law "may have led to a certain "petrification" of the law", while "simultaneously there is a growing need to continuously adapt existing rules in view of rapidly changing circumstances and views. The "shelf life" of law tends to become more limited as society changes more rapidly, and company law is no exception."

31 For a similar observation in the context of company law, see The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe (n 30), at para. 2: "Fixed rules in primary legislation may offer the benefits of certainty, democratic legitimacy and usually strong possibilities of enforcement. But this comes at a cost of little or no flexibility, and disability of keeping pace with changing circumstances."

32 See n 18.

33 I note that such a global standard itself need not necessary itself be binding at the global level. Global standards can also be developed by private institutions whereafter bindingness can subsequently be achieved by national or regional governments adopting such standards in their respective national laws. This indirect manner of achieving global harmonisation is a much observed phenomenon in the global arena. See on this shift from **national public** regulation to **global private** rule-making: Büthe and Mattli (Chapter 7, n 62), at Chapter 1 "The Rise of Private Regulation in the World Economy". See in particular at 5: where Büthe and Mattli observe as a trend: "the delegation of regulatory authority from governments to a single international private-sector body that, for its area of expertise, is viewed by both public and private actors as the obvious forum for global regulation. (…) This simultaneous privatization and internationalization of governance is driven, in part, by governments' lack of requisite technical expertise, financial resources, or flexibility to deal expeditiously with ever more complex and urgent regulatory tasks". Büthe and Mattli give as a striking example of both (i) norm-setting in general principles only and (ii) privatization internationalization of norm-setting the landmark decision of the SEC in August 2008, to switch the US accounting standards (at that time the US Generally Accepted Accounting Principles (GAAP)) to the International Financial Reporting Standards (IFRS), produced by the International Accounting Standards Board, a private-sector regulator based in London, see SEC "Roadmap to IFRS Adoption,

experiences,[34] data protection issues have become so vast and urgent that they can no longer be ignored by governments and multinationals alike.[35] In face of the huge challenge to regulate a global phenomenon that is already a reality and a moving target at that, my prediction is that agreement on the basic data protection principles in a global standard may prove less of a hurdle than past experiences with attempts to come to a global standard would suggest.[36]

8.3 Cross-border enforcement issues

Federal Register," 14 November 2008. At 2, Büthe and Mattli indicate that the implications of this switch are momenteous as "GAAP are highly detailed and address a vast range of specific situations (...) and the IFRS, by contrast, have traditionally been principle-based. They lay-out key objectives of sound reporting and offer general guidance instead of detailed rules" as a result of which "twenty-five thousand pages of complex U.S. accounting rules become obsolete, replaced by some twenty-five hundred pages of IFRS. Earlier the EU already made the use of IFRS mandatory for companies with publicly traded financial securities, by including a reference to IFRS in EU legislation," see Büthe and Mattli at 4 and at 99 (discussing the adoption for the EU of IFRS 8 (specifying what information a corporation must disclose in its consolidated finacial statements), by Commission Regulation 1358/2007 of 21 November 2007, OJ L 304/9.

34 See The Economist, "The Data Deluge: Businesses, governments and society are only starting to tap its vast potential" (Chapter 6, n 1).

35 And indeed are not ignored, as evidenced by the flurry of legislative action in the area of data protection and security around the world. See for an overview Kuner (Chapter 6, n 8) at addendum D.

36 This is already evidenced by recent rapprochement between the US – EU views on data protection: See for instance a publication "Google, Internet Companies Face Too Many Privacy Rules, U.S. Official Says", dated 25 March 2011, to be found at www.bloomberg.com, reporting that "Google and other U.S. Internet companies may be hampered by a multiplicity of data protection rules in Europe and beyond that are "potential barriers to the free flow of information," a U.S. official said. Daniel Weitzner, an Internet policy official in the U.S. Commerce Department, said regulators don't always recognize companies' efforts to set basic data protection standards that are adequate to stem abuses of privacy. (...) 'It's awfully difficult to adapt privacy practices for a hundred or more different' jurisdictions, Weitzner told reporters in Brussels the day after a meeting with Viviane Reding, the European Union's justice commissioner. "That is a substantial barrier today." (...) Cooperation between the EU and the U.S. may promote global standards for data privacy, Reding said in a speech today. Planned changes to data protection rules in both regions 'seem to be quite convergent,' she said. 'Our cooperation has a good chance to be the first step towards the development and promotion of international legal standards,' Reding said."

Applicability, jurisdiction and enforcement of data protection legislation are generally based on a jurisdictional approach.[37] These concepts are subject to limitations set by PIL.[38] This is due to the fact that a key concept of determining the limits of state regulation is 'sovereignty'. The concept of sovereignty is founded on the very existence of territory: "the principle where a state is deemed to exercise exclusive power over its territory can be considered [to be] the fundamental axiom of classical international law".[39] Cross border data flows inherently challenge such sovereignty. In order to seek regulation of these cross-border data flows, states gave their laws a long arm reach (both in terms of scope of applicability of their laws and adopting outbound data transfer rules).

Though data protection regulations may be of relatively recent times, the concepts of applicable law and jurisdiction are embedded in a long tradition of PIL, where laws that over-extend their jurisdictional reach are considered an unacceptable form of 'hyper-regulation' if they apply so indiscriminately that there is no hope of enforcement. Applicability regimes are therefore inherently delineated and cannot be instrumental in solving the present gaps in the protection of personal data and its enforcement.[40] This automatically also applies to data transfer regimes, as these are only triggered if the relevant data protection law is applicable in the first place.[41]

---

37 Also the APEC Privacy Framework 2005 (n 38) is based on the principle of cross-border cooperation between national data protection supervisors, see Annex B sub II and III of the APEC Privacy Framework. Some form of central enforcement is however realised by the accountability principle for data transfers. See para. 7.4 and in more detail para. 13.6.

38 See Kuner (Chapter 6, n 52), at 27 and Christopher Kuner, '*European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press 2007) at 125: "With regard to the ability of the EU Member States to enforce their own data protection law on foreign websites outside their borders, the answer is clear that this would be in violation of international law," referring to F.A. Mann, "The doctrine of jurisdiction in international law," (1964) 111 Recueil des Cours 9, 145-146: "[I]s it open to a State to have resort to its own legal system and, in particular, its own courts for the purpose of making the conduct of foreigners in foreign countries conform to its own commands? ... It would seem that the answers to the above questions must be in the negative. Any other result would be repugnant to one's commonsense and the dictates of justice, to that distribution of State jurisdiction and to that idea of international forbearance without which the present international order cannot continue."

39 Prins (Chapter 6, n 9), at 191, especially footnote 164.

40 See para 3.11, where I discussed the delineations of the present applicability and jurisdictional regime of the Data Protection Directive. See also Kuner (Chapter 6, n 61), at 183.

41 Kuner (Chapter 6, n 8), at 7, 15 and 31 indicates that regulation of transborder data flows in the EU was originally designed to prevent circumvention of data protection law. Kuner's position is, however, not substantiated by the legislative history of the Directive (see Chapter 6, n 2). Based on the legislative history the conclusion seems to be that the EU data transfer rules are designed

From a practical perspective, the jurisdictional approach to enforcement leads to many long arm reach data protection laws having no hope of enforcement if the relevant multinational is not established in the relevant jurisdiction or if the data processing operation is not physically located there.[42] This challenge is not specific to data protection. Similar issues are encountered in case of enforcement of any national right due to the fact that there is no global convention for the enforcement of a national right in other jurisdictions or for recognition and enforcement of court decisions in other jurisdictions.[43] Cross-border enforcement issues proliferate if (as with data protection) the laws are highly varied across the globe or even lacking (as is often the case in developing countries).[44] As a result questions arise as to the enforceability in an international context, for instance whether supervisory authorities of a country are entitled (or obliged) to provide assistance to another supervisory authority in respect of a breach of such authorities' national law while this would not constitute a breach in the country of the authority whose assistance is requested. Similar questions arise in respect of investigation powers, recognition of foreign judgements, enforcement of

---

to prevent that the protection afforded by the Directive is nullified if data are subsequently transferred abroad. As indicated in the text, data transfer rules are only triggered if the relevant data protection law is applicable in the first place. Any circumvention of protection can therefore only be addressed by the applicability regime in the Directive and not by the data transfer rules (as Kuner implicates) .

42 Article 29 Working Party 'Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on Standard Contractual Clauses for the Transfer of personal Data to Data Processors Established in Third Countries under Article 26(4) of Directive 95/46' (WP 47, 13 September 2001), at 3 says that "the physical location of the data in third countries makes the enforcement of the contract or the decisions taken by Supervisory Authorities considerably more difficult." See Kuner (n 52), at 271 and Chapter 3, at 37.

43 Illustrative of this is the fact that the The Hague Conference (a treaty drafting body with 62 member states) has (after more than a decade of work) ceased working on a new Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgements in Civil and Commercial Matters. For the relevant texts and status', see <www.hcch.net>. Kuner (Chapter 6, n 8), at 43 comments that it is unrealistic to expect such cross-border enforcement treaties to be forthcoming in the area of data protection as countries recently refused opportunities to enact global legal instruments protecting consumers in electronic commerce. See also Prins (n 9), at 15. Also in the data protection area no progress in this respect has been made whatsoever. See for the status in respect of data protection: Hague Conference on Private International Law, Cross-Border Data Flows and Protection of Privacy, Note submitted by the Permanent Bureau (13 March 2010), to be found at <http://www.hcch.net/upload/wop/genaff2010pd13e.pdf >., as discussed in detail in Chapter 4.

44 See in respect of consumer protection laws, Colin Scott, n 25, at 1. See on parallel between cross-border enforcement issues between data protection and consumer protection Paragraph 8.4.2.

foreign judgements, etc.[45] This may entail that supervisory authorities have to obtain information on alleged breaches via the internet rather than rely on investigation performed in the relevant other jurisdictions.

From the perspective of individuals whose data are processed, the present jurisdictional approach does not provide effective protection. This is not for a lack of rights and remedies of individuals. For instance, the Data Protection Directive provides for quite broad remedies and liabilities and in principle allows individuals ample opportunity to ensure that a breach is remedied and compensation is obtained. However, to effectuate these rights and remedies through traditional judicial means is not viable in practice for a number of reasons. Data protection breaches in most cases involve relatively small levels of economic damages for individuals where it would be more costly to pursue a case through traditional judicial means.[46] Due to

---

45 See Prins (n 9), at 173.

46 The Rand Report (Chapter 6, n 27), at 35: "Enforcing the Directive can be difficult because the damages suffered are often intangible (or sometimes not evident in the short term), it is difficult to assign a value to any damages, and determining responsibilities is complex". The Rand Report indicates that though remedies and liabilities in the Data Protection Directive are quite broad, and in principle allow ample opportunity for data subjects to obtain compensation for damages, this approach does not function in practice if damages are not immediate, are difficult to quantify or are too small to be bothered with on an individual scale. The Rand Report indicates that the approach chosen in the Directive "does not function in practice for a number of reasons, including:

- There may not be any immediate damages, such as when confidential data, e.g. credit card numbers, are leaked. As long as the data has not yet been abused, it may be difficult to obtain any compensation, even if negligence on the data controller's part has created a substantial security and privacy risk.
- The extent of damages may be difficult to quantify. To continue the example above: suppose a credit card is abused, but the bank rectifies the problem by refunding the injured party and by issuing a new card. The data subject must still obtain a new card, cancel any payments linked to the old number, notify service providers of changed payment info etc. Clearly, this loss of time and effort has a cost, but how can it be calculated fairly?
- Damages are typically too small to bother with on an individual scale. If 20,000 credit cards must be revoked because a data controller has been careless, 20,000 individuals will have to go through the aforementioned steps. The collective damage is clearly substantial, but it is quite unlikely that any of the individuals involved will undertake any action, since any compensation is likely to be dwarfed by the extra effort and expenditure required to obtain it. The risk of sanctions for the data controller responsible for such an incident therefore remains limited."

The Rand Report concludes with: "If errors are unlikely to have serious consequences, there is no incentive for data controllers to comply with data protection provisions. Enforcement is also perceived to be hampered by the fact that DPAs are poorly funded and overloaded with cases."

the networked economy, even relatively simple breaches of data protection present complicated cross-border jurisdictional and enforcement issues. The example below is for clarification.

> A US consumer purchases a product over the internet from a Dutch company. The Dutch company involves one of its group companies in India for customer service purposes (help desk for installation of the product). The Dutch company has a privacy policy informing the consumer that his data are shared with the Indian group company for helpdesk services and the consumer provides his consent for this. The data of the consumer are hacked and the consumer becomes subject of identity theft. Here, as in all other cases, the consumer has to determine: (i) who is at fault, (ii) what laws apply, (iii) what are his rights under the applicable law(s); (iv) what are his damages; and (iv) where to seek redress. Even in this relatively straightforward case answering of each of these questions proves problematic and leads to the consumer effectively having no recourse.
>
> **Re (i) Who is at fault?** In this case it will be difficult to establish which company is at fault (i.e. the Dutch or the Indian company) as in practice it is often impossible to determine at which point in a network a hacker found entry. As a consequence it will be impossible to prove for the consumer which of the two companies actually did not secure the data properly, in the absence of which each company can avoid liability.
>
> **Re (ii) What laws apply?** The Federal Trade Commission Act (**FTC Act**) does not apply to a Dutch company doing business from the Netherlands and the FTC

See Scott (n 25), at 4, presenting a similar observation in respect of consumer protection laws. Douwe Korff, New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (January 15, 2010). European Commission DG Justice, Freedom and Security Report, available at SSRN: http://ssrn.com/abstract=1638949, at 98 notes: "Indeed, and we may end this sub-section on this, it appears that litigation in the courts by ordinary citizens is extremely rare. In the UK, the case of Naomi Campbell, briefly set out in section 2.3(b) above, was the first case ever in which compensation was awarded for breaches of data protection law, but this remains a very rare instance. In other countries there may be more actions, but in most, the cost and effort of formal court proceedings deter most potential claimants. In our Final Report, we will examine if this can be changed and ought to change. We believe that, especially in the light of the weakness of enforcement by the data protection authorities (as noted in the next sub-sections), possibilities for empowering ordinary citizens should be further explored. We will examine why class actions are still extremely rare in Europe, also on data protection issues, and whether other, non-EU countries have more effective systems of this kind in place."

has no jurisdiction.[47] Dutch data protection law applies in respect to the data processing by the Dutch company. Supposing that the consumer can prove the security breach occurred in the systems of the Dutch company, the consumer can file a complaint with the Dutch DPA. Chances are slim that the Dutch DPA will take action based on an individual complaint of a US consumer in an isolated case. Instigating civil action in the Netherlands is too costly and not justified in light of the damages (if any) suffered by the US consumer. Language issues and time differences may also prove an impediment. If the consumer can prove that the security breach occurred in India, chances are that the Indian company did not breach any provision of Indian law, as a result of which no recourse is available at all.

Re (iii) What are his rights? / Re (iv) Proof of damages.
As long as the relevant identity theft has not led (yet) to any actual damages (like abuse of the credit card number of the US consumer), it will be difficult for the US consumer to prove actual damages and to establish whether these are recoverable under Dutch law.

From this example it may be clear that even if the questions can be answered, in practice still no effective resources may be available. The Working Party 29, the EDPS and the European Commission are well aware of the lack of access to justice of data subjects and have proposed to address this (to some extent) in the upcoming revision of the Data Protection Directive.[48] The Working Party 29 has proposed the introduction of the possibility of class actions and the introduction of an obligation of data controllers to provide for complaints procedures that are more accessible, effective and affordable. If these do not resolve the dispute, the data subject should (besides access to the courts) be able to turn to Alternative Dispute Resolution provided for by the industry.[49] The Commission has indicated it

47 See Section 5 of the FTC Act (15 USC 45). The Act generally does not apply to foreign trade with a limited number of exceptions, for instance in case of "practices involving foreign commerce that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States." (Section 5, subsection 4(A)).

48 See Chapter 6, n 26 and n 27 for an overview of the official EU documents showing the knowledge of the lack of enforcement of data protection laws in the EU. See for the lack of access to justice of data subjects EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 96:
"In cases with smaller impact, it is unlikely that the victims of a breach of data protection rules would bring individual actions against the controllers, given the costs, delays, uncertainties, risks and burdens they would be exposed to".

49 WP Contribution on The Future of Privacy (Chapter 6, n 33), at para. 62, at 16. See also the Rand Report (n Chapter 6, n 27), at 55: "Alternative Dispute Resolution (ADR) – ADR measures

intends to adopt the proposal to facilitate class actions, which should according to the Commission be extended "to DPAs and to civil society organisations as well as other associations representing data subjects' interests".[50] This is in conformance with the advice of the EDPS.[51] From the above it may be clear that the introduction of the possibility of class actions alone will not address the cross-border issues encountered by individuals.[52]

Again, at first glance the absence of effective enforcement of data protection may seem to be to the advantage of multinationals processing data, who can avoid potential liabilities. This is, however, not necessarily the case. As will be discussed in Paragraph 9.3 and 9.4, there are compelling reasons for multinationals to implement their own global privacy policies to be able to ensure (to a certain extent) uniform data processing rules throughout their group of companies and to ensure central supervision and enforcement by one lead DPA and the courts of one of the Member States. This would avoid the present patchwork of local and cross-border privacy rules in about as many as 60 different jurisdictions in the world.[53]

In areas of law where substantial harmonisation already has taken place, initiatives to ensure cross-border enforcement do exist and in isolated cases uniform procedures have been established.[54] This is, however, not yet the

---

are regarded as a useful means of permitting consumers / citizens to exercise their rights more easily. The principle is that they permit easier access to justice without having to go through the complex, time consuming and uncertain judicial system. They may be particularly useful in consumer contexts where relatively small levels of economic damage are being considered and where it would be more costly to pursue a case through traditional judicial means."

50 EC Communication on the revision of the Directive (Chapter 6, n 34), at 9.

51 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 96: "These difficulties could be overcome or substantially alleviated if a system of collective redress were in place, empowering the victims of breaches to bundle their individual claims in a single action. (…) The EDPS would also favour the empowerment of qualified entities, such as consumer associations or public bodies, to bring actions for damages on behalf of victims of data protection breaches. These actions should be without prejudice to the right of data subject to bring individual actions. The EDPS would also favour the empowerment of qualified entities, such as consumer associations or public bodies, to bring actions for damages on behalf of victims of data protection breaches."

52 See Scott (n 25), at 4 reporting that class actions are valuable in the category of cases where damage to consumers is extensive, but less so where damages are diffuse or small.

53 See n 61.

54 Mostly in the area of criminal law. Prins (Chapter 6, n 9), at 175 and 186. An example is the adoption of the Council of Europe's Cybercrime Treaty <to be found at <http://conventions.coe.int/treaty/en/treaties/html/185.htm>.

case in the area of data protection. At present, the main tool applied by DPAs to try to solve gaps in applicable data protection laws and enforcement is by seeking cooperation with other DPAs in the event of cross-border data protection violations (i.e. a network approach, each authority in its own territory).[55] In order to ensure that each authority may indeed play its role in such cooperation, there is a clear call for enforcing the positions and powers of DPAs around the world and further for aligning and coordinating enforcement policies.[56] In practice DPAs increasingly seek such cooperation.[57] However, until such time as all jurisdictions have adequate

---

55 Pursuant to Article 28(6) and (7) Data Protection Directive, the DPAs are required to cooperate with one another, exchange useful information and may be requested to exercise their powers by a DPA of another Member State (i.e. enforcement is based on a 'network approach'). See for the APEC Privacy Framework (Chapter 6, n 38). See further the Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, adopted by the OECD Council on 12 June 2007, at Point 2 of the Annex. This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities in order to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy, that also stresses the need to reach a common protection of personal data throughout the world', to be found at www.oecd.org. Since November 2006 the DPAs share best practices in the context of the 'London Initiative'. See Hustinx (Chapter 14, n 174), at para 7.5 and Prins (Chapter 6, n 9), at 190.

56 See n 55 and the WP Contribution on the Future of Privacy (Chapter 6, n 33), at para. 7, advising the Commission to strengthen and clarify the roles for DPAs and their cooperation within the EU and further at para. 36, advising the Commission "to encourage the cooperation between international data protection authorities, for example on a transatlantic level." The Commission announced in its Communication on the revision of the Directive (Chapter 6, n 34), at para 2.5 to examine how to "'strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities and ways to improve the cooperation and cooperation between DPAs." See also the EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 140, where the EDPS "also insists on the need to clarify in the new legal instrument the essential notion of independence of DPAs." The European Court of Justice has recently taken a decision on this issue in Case C-518/0754 Commission v. Germany, [2010] OJ C 113, at 3-4, where it emphasised that independence means the absence of any external influence. A DPA may seek nor take instructions from anybody. The EDPS suggests explicitly codifying these elements of independence in the law. See further the Declaration of Civil Society Organisations, adopted on 25 September in Montreal, stating that "stronger and more aggressive action by privacy commissioners is required," finding them uniquely positioned to defend our society's core values and rights of privacy, to be found at <http://www.privacyconference2007.gc.ca/Terra_Incognita_resolutions_ngo_E.html>.

57 Kuner (Chapter 6, n 8), at 32 and 42

data protection laws and supervision of these laws, this network approach cannot adequately solve all gaps in applicable laws and enforcement issues faced by data protection regulators. Further, as discussed in Paragraph 8.2 concerning global standards, even if international regulation of data protection including enforcement were forthcoming, experiences in other areas of law show that the actual enforcement activity often proves very different per jurisdiction.[58]

8.4 Thinking about alternative solutions for enforcement

8.4.1 Self-regulation backed up by governmental enforcement tools

When looking at other forms of international ICT regulation on cross-border enforcement, these show few ideas about a more integral approach to enforcement.[59] Initially, ICT regulators both at the national and the international level seemed to be united in their opinion that industry self-regulation and alternative dispute resolution (ADR) would prove a better alternative to solve enforcement issues in an international context than the traditional forms of jurisdiction-based government regulation, dispute resolution and enforcement mechanisms.[60] However, as ICT law developed over the years, by now a clear preference can be discerned for co-regulation above pure self-regulation.[61] The prevailing current thinking is that

---

[58] See para. 8.2 in particular n 23.

[59] Prins (Chapter 6, n 9), at 187.

[60] See Miriam Lips, "Inventory of General ICT Regulatory Starting Points," in Bert-Jaap Koops et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), Chapter 2, para. 2.6; WP Contribution on the Future of Privacy (Chapter 6, n 33), at 8.

[61] See for a comprehensive overview of the developments: Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 123 and Yves Poullet, "ICT and Co-Regulation: Towards a New Regulatory Approach?", in: Bert-Jaap Koops et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), at 247. For the preference for co-regulation as to data protection, see the Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 12: "We prefer the approach of "Co-regulation", where there is a clear and binding framework of principle which both requires and encourages companies to decide and demonstrate how they have achieved the desired outcomes in their own way. At domestic and international level, this is one of the main attractions of the Accountability principle – minimum imposed burden and maximum effectiveness in practice." See for the preference in broader context: EC White Paper on European Governance (Chapter 6, n 72), at 20-21. See further Fabrizio Cafaggi, Private Law-making and European Integration: Where Do They Meet, When Do They Conflict, in: *The Regulatory State,* ed. Dawn Oliver, Tony Prosser, and Richard

enforcement, in particular, cannot be left to industry alone; self-regulation should be backed up by governmental enforcement tools. This can only be achieved by means of co-regulation rather than by self-regulation and ADR.[62]. See in the same vein the OECD, which considers that the most effective online privacy protection will be delivered through a mix of regulatory and self-regulatory approaches,[63] whereby according to the OECD self-regulation will be more effective when it is backed up with appropriate legislation and effective government enforcement tools.[64]

Rawlings, December 2010 at 212, who notes that the Commission shows a clear preference for co-regulation, but that "the Parliament has displayed scepticism, if not opposition to the use of (…) alternatives to legislation on the basis primarily of legitimacy arguments." At 225, Cafaggi indicates that for TPR to work, "strong and effective public institutions are needed" as TPR complements rather than substitutes public law making. See further at 227: "I have distinguished the constitutional foundations of self-regulation from co-regulation emphasising the importance of public intervention to ensure legitimacy and binding effects". See also Cafaggi (Chapter 6, n 67) at 3.

62 EC White Paper on European Governance (Chapter 6, n 72), at 21. The Inter-Institutional Agreement on 'Better Lawmaking' (n 72) gives a somewhat different definition of co-regulation in Article 18: "the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)." This definition makes a clear divide whereby the legislators have to identify the essential public policy objectives and whereby the means, by which these public policy objectives have to be met, are established by the public and private sector together. This partitioning of responsibilities is also advocated by Article 49 of the 'WSIS Declaration of Principles,' as adopted at the World Summit on the Information Society (**WSIS**) which was organised by the International Telecommunication Union (ITU) and took place in Geneva on 10 -12 December 2003. The Declaration of Principles is to be found at the ITU website <www.itu.int> (ref. WSIS-03/GENEVA/DOC/0004).
EC White Paper on European Governance (Chapter 6, n 72), at 21: "Co-regulation implies that a framework of overall objectives, basic rights, enforcement and appeal mechanisms, and conditions for monitoring is set in the legislation".

63 See Privacy On-Line, OECD Guidance (n 20), at 28. See also Maurice Schellekens, Bert-Jaap Koops and Corien Prins, *Conclusion*, in: Bert-Jaap Koops et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), Chapter 8, at 233 and Poullet (n 61), at 248.

64 Privacy On-Line, OECD Guidance (n 20), at 28. It has to be noted however that until now, practice has not shown many examples of effective governmental enforcement in the international context. It is often the private sector or non-governmental organisations that take the lead in realising successful international co-operation on enforcement. See Prins (Chapter 6, n 9), at 187, giving as a lonely example of an effective international enforcement system, the

8.4.2 Parallel with enforcement of consumer protection laws

In the absence of more in-depth studies on cross-border enforcement of data protection, reference may be made to the general literature in respect of cross-border enforcement of consumer protection laws, which is shaped by ideas about what generally works in regulatory enforcement.[65] Many parallels can be identified between enforcement of data protection and consumer rights. And like data protection laws, consumer protection laws are highly varied across the globe and in some countries (especially in developing countries) even lacking. Styles of enforcement in countries differ widely, with the increased access of consumers to the internet, and where consumers are increasingly faced with cross-border enforcement against foreign suppliers, there is a similar problem of widely diffused small losses which makes private enforcement unrealistic. To counterbalance the lack of private enforcement, many countries have set up public agencies tasked with monitoring and enforcement of consumer laws (very similar to the role and powers of DPAs). Technical developments in e-commerce increasingly give satisfied and dissatisfied consumers a voice, which developments do not so much give consumers redress potential, but enable future customers to assess the risk of default by its counter party;[66] a parallel here with data protection are the "naming and shaming" sites publishing data security breaches, and websites ranking the worst privacy violators, etc.[67]

Summarising the developments in the policy thinking about enforcement of consumer protection laws, these show three stages in the regulatory response to the rise of the consumer society. Initially, enforcement was left to procedures in private law. The second stage in the 1960s and 1970s comprised a legislative response under which public agencies were empowered to take a more active approach to consumer protection. The third stage is labelled by some as the "post-interventionist phase", "in which the state is accorded a more modest role in stimulating market and community governance forms which are targeted at weaknesses in the state's capacity to deliver."[68] The general assumption of the third stage is that traditional forms of private enforcement complemented by agency

international approach of combating child pornography, for which an international network of hotlines is at work, see <www.inhope.org>.

65 This Paragraph draws on Scott (n25), at 1 -2.3

66 Scott (n25), at 6.

67 See further para. 9.3 and in particular n 28.

68 Scott (n 25), at 16 and 17, referring to Norbert Reich, Diverse Approaches to Consumer Protection Philosophy, Journal of Consumer Policy, [1992], 14:257 – 292.

enforcement are inadequate to force compliance, and that it is helpful to understand "the conditions under which businesses comply with their responsibilities",[69] that the "knowledge and capacity for effective controls lies with industry, NGOs, companies and consumers",[70] and "to adopt a wider conception of enforcement which embraces both formal and informal mechanisms through which agencies (and others) seek to promote compliance."[71] "Then the challenge for government is how to harness that capacity and steer it, for example through promoting the development and exchange of information, and changing incentives, such that it delivers on public objectives for consumer law regimes with both a degree of effectiveness matched by sufficiency of legitimacy".[72]

In cases where damage to individuals is extensive, the introduction of the possibility of class actions appears to be an adequate response.[73] In cases where damages are diffused and small, novel forms of enforcement are indicated, which can take many forms.[74] Examples given are as diverse as:

- introduction of new remedies for consumers which do not require formal enforcement. An example is the right of a cooling off period, provided in the EU Distance Selling Directive,[75] typically accompanied by an obligation of the company to notify customers of the right and how they may exercise it;[76]
- imposing strict liability on companies as a solution to overcome the difficulty of consumers to prove wilfulness on the part of the company.
- empowering consumer organisations to enforce consumer protection laws;[77]
- enforcement not against companies violating the consumer protection law, but via "gate keepers", for instance by imposing a

69 Scott (n 25), at 3.

70 Scott (n 25), at 17.

71 Scott (n 25), at 3.

72 Scott (n 25), at 17.

73 Scott (n 25), at 4.

74 The examples are based on examples discussed in Scott (n 25).

75 Article 6 and 4(1)(f) of the Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, [1997] OJ L144/ 19 (**Distance Selling Directive**).

76 Scott (n 25), at 5.

77 Scott (n 25), at 8 – 9.

charge back obligation on credit card issuers where companies do not meet their consumer contract obligations.[78]

- imposing disclosure and information obligations on companies on the basis of which consumers can make purchase decisions and NGOs can organise boycotts of products that they consider below standards or harmful, or "buycotts" of products that they consider as particularly worthy of support;[79]
- stimulating accreditation and monitoring schemes, so consumers can make informed purchase decisions.[80]

More radical approaches suggest that "there is a value in seeking to stimulate self-regulatory measures by businesses which can then be monitored and steered by public agencies".[81] An interesting parallel in this context is that (contrary to the expectations in the early days of internet), there are very few court cases dealing with cross-border consumer disputes.[82] One of the mechanisms that prevents these disputes is "the existence of self-regulatory and other systems".[83] Examples are the use of credit cards for online payments which bring their own dispute resolution system[84] and the emergence of large intermediaries like e-Bay, that was at

---

78 Scott (n 25), at 9. Another example in the internet context is imposing an obligation on banks to block payments to illegal online gambling sites provided by companies established in gambling paradises.

79 Scott (n 25), at 3.

80 Scott (n 25), at 17.

81 Scott (n 25), at 15 referring to Christine Parker and John Braithwaite, 2003. "Regulation" in *The Oxford Handbook of Legal Studies,* ed. Peter Cane and Mark Tushnet, Oxford.

82 Swire (Chapter 6, n 69), notes that despite the fact that "every encounter in cyberspace (…) raises the possibility that diverse laws will apply" and that the "rules for choosing among diverse laws (…) thus appear uniquely important for cyberspace. Surprisingly, however, the number of actual cases addressing choice of law on the Internet is far, far lower than the initial analysis would suggest. Although there is the possibility of diverse national laws in every Internet encounter, some mysterious mechanisms are reducing the actual conflicts to a handful of cases."

83 Swire (Chapter 6, n 69), at 1976.

84 Swire (Chapter 6, n 69), at 1990, gives this as the main reason for the fact that there are so few court cases involving online consumer purchases: "e-cash systems have failed to become widespread. Instead, credit card purchases (and systems such as PayPal that are based on credit and debit card accounts) have become the dominant means of payment over the Internet." As a result "[s]ellers and buyers are subject to the elaborate rules of the credit card payment system, and so there is relatively little recourse to national courts. Credit cards have two decisive consumer protections compared with e-cash systems. If there is unauthorized use of the credit or debit card, the individual's loss is limited by U.S. statute, usually to $50.47 In addition, the credit card brings with it an already-functioning dispute resolution system. If a merchant claims

first regulated by the ratings and review consumers could post, but later introduced full-fledged dispute resolution.[85] Regulating the "self-regulation" by such key players may be more effective than issuing further material rules.

It is outside the scope of this dissertation to evaluate the optimal mix of enforcement measures for data protection. There are, however, a number of reasons why this general literature is relevant for this dissertation. The main one is the realisation that the (by now) traditional forms of private enforcement complemented by agency enforcement are inadequate to force compliance, and that introduction of the possibility of class actions will not be sufficient to address the cross-border enforcement issues in the data protection arena. More creativity is required and the general literature in both the international ICT and the consumer protection areas point in the direction of self-regulation backed up with governmental enforcement. Further, self-regulation does not materialise just like that and some of the alternative enforcement measures in the consumer protection arena are intended to work as an incentive for just that purpose. For instance, the imposition of disclosure obligations on companies has proven a stronger incentive for companies to achieve compliance (often by introducing self-regulatory policies) than the introduction of material rules. I discuss this

---

that a customer has spent $200 on software, and the customer disagrees, then the customer is not charged for the $200 while the dispute is in process. With these ready-made ways to protect customers against unauthorized use and to resolve disputes, the credit card system inspires trust in consumers, creates effective dispute resolution mechanisms, and avoids the need for recourse to national courts."

85 Swire (Chapter 6, n 69), at 1991 – 1992: "The third early prediction about e-commerce was that search engines and the global reach of the Internet would eliminate the need for wholesalers and other intermediaries. Consumers can feel that it is very risky, however, to buy from a website they have never heard of, in a country far away. One major cure for this problem has been the phenomenal growth of auction sites, especially the Internet intermediary eBay (...). Although it was likely not a major goal of eBay's managers to avoid conflict-of-laws disputes, that has been one effect of the business model. Initially, trust in eBay was supposed to result from feedback ratings that customers gave to each other. Over time, however, eBay has created an entire legal system that accompanies each sale. The system contains at least a dozen consumer protections, including fraud protection for the buyer, an escrow service so that buyers can examine an item before payment goes to the seller, a verified identity program, and a system for fraud enforcement including referrals if necessary for criminal activity. (...) Although eBay initially became famous for small purchases, such as hobbyist collectibles, today's eBay includes numerous auctions for valuable items such as diamonds. Even these large consumer transactions appear to be conducted without recourse to national courts, avoiding judicial pronouncements".

element and its relevance for data protection in Paragraphs 13.2.1 - 13.3.3. Also, in the chapters where I discuss specific enforcement issues of data protection (for instance, in the context of supply-chain management in Paragraphs 11.5 - 11.6), I will draw on the empirical research and the general literature on enforcement of consumer protection laws. Thirdly, and more generally, what I found instructive myself in this literature is that at first glance, the possibility of self-regulation and this particularly in an international context has a flavour of "leniency", of a soft approach to compliance and that in an area where human rights are at stake. The first thought is "who is going to monitor and enforce compliance"? It is instructive to realise that empirical research shows that government regulation and enforcement will not do the trick in a cross-border environment unless such governmental regulation aims at regulating private regulation and some form of governmental enforcement of such private regulation. This concerns the concept of "meta-regulation", which has two elements. The first concerns how regulators can provide companies with incentives and tools to use their own inherent regulatory capacity. This I discuss in Chapter 8 in the wider context of introduction of the "principle of accountability". The second element concerns the optimal form of meta-regulation for governments to choose corporate self-regulation. I discuss the question "how best to regulate" in Chapter 9.

To set the background for this dissertation I discuss below three (partial) solutions which may contribute to the thinking on how to improve the position of individuals in case of cross-border data protection violations.[86] One of these solutions requires the introduction of self-regulation backed up by government enforcement. This is not meant to imply that this is thus the best of the three solutions. The solutions are totally different in nature, and in this dissertation I will show that these options can be combined and also have to be combined to achieve hopefully a better final result than we are

[86] Kuner (Chapter 3, n 64), looks at this issue from a jurisdictional perspective and concludes that the increasing jurisdictional conflicts on the internet involving data protection law cannot be solved merely by changes to jurisdictional rules, but that other measures should also be considered. See at 24-30, for Kuner's suggestions: (i) achieve greater harmonisation of the law; (ii) technical solutions (such as geolocation, whereby the internet can be 'zoned' geographically and thus making it easier to limit jurisdictional risk); (iii) development of a theory of comity or reasonableness (whereby jurisdiction is not to be asserted even when technically it could be); and (iv) greater interaction between the jurisdiction and data protection worlds (by improving interaction between scholars, international organisations, regulators, and others working on international jurisdiction, and those working on data protection). Though all good suggestions, my assessment is that more creative solutions are indicated to achieve some form of meaningful redress for individuals.

presented with today. The underlying goal of all three solutions is to try to achieve some form of **integral** enforcement of cross-border data protection. By integral, I do not mean the network approach where each supervisory authority enforces in its own territory and the relevant supervisory authorities work together.[87] By an integral approach, I mean that enforcement is somehow centralised, one supervisory authority being able to enforce on a cross-border basis. This would solve some of the problems discussed above, most notably the potential requirement to address different courts under application of different laws. The starting point of each of these solutions is that, given the sovereignty of states, any such form of central enforcement will involve the relinquishing by a state of enforcement powers of such states in cross-border situations, in return for central enforcement powers in other cases. As long as the instances where central enforcement powers are obtained are of more relevance to a regulator than the instances in which enforcement powers are relinquished, this would seem a viable option. Taking this as a starting point, the three alternative mechanisms that can be identified to achieve some form of central enforcement are:

(i) the country-of-origin approach;
(ii) the accountability approach; and
(iii) choice of law and forum in TPR.

8.4.3 Country-of-origin approach

Central supervision may (at least for the EU) be achieved by introducing the country-of-origin principle.[88] European legislators already have introduced the country-of-origin principle for certain areas of law, most notably for cross-border television broadcasting services[89] and e-commerce

---

87 In the EU such cooperation in respect of enforcement of consumer protection laws is made mandatory by Regulation 2006/2004/EC of the European Parliament and the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws.

88 See also Lips (n 60), at 49; and Prins (Chapter 6, n 9), at 195.

89 Directive 89/552/EEC of the European Parliament and of the Council of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, [1989] OJ L 298/ 23 (**Television without Frontiers Directive**) as recently amended by Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 (renaming the Television without Frontiers Directive into) (**Audiovisual Media Services Directive**). The deadline for implementing the Audiovisual Media Services Directive was 19 December 2009.

services.[90]/[91] According to the country-of-origin principle each member state applies its own law to the services provided by service providers established in their territory (i.e. these services are governed by the law of their "country of origin"). The other countries must allow these services to be provided within their jurisdiction and may not apply additional regulations.[92] This prevents the cumulative application of the different national laws to cross-border services within the relevant region. Application of the country-of-origin principle is considered justified in a European context if a certain area of law has been extensively harmonised within the EU. Given the purpose of the Data Protection Directive (full harmonisation of data protection law within the EU)[93], introduction of the country-of-origin principle also for data protection law would have been the obvious choice, but this was at the time apparently not yet feasible.[94] Recently, the Working Party 29 and the EDPS have recommended adoption of the country-of-origin principle also for data protection in the revised Directive.[95] According to the country-of-origin

---

90 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] OJ L 178/1 (**E-commerce Directive**) . See E.M.L. Moerel, "The country of origin principle in the E-commerce Directive: the expected 'one stop shop'?", [2001] CTLR , at 184.

91 Another example is the "passporting" of the approval of a prospectus required by a company for an offer of securities to the public, or the admission to the trading on a regulated market for securities, by the regulator of the "home Member State" of the company for the whole of the EU. See Article 17 and Recitals 14 and 45 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC (**Prospectus Directive**). See in particular Recital 14: "The grant to the issuer of a single passport, valid throughout the Community, and the application of the country of origin principle require the identification of the home Member State as the one best placed to regulate the issuer for the purposes of this Directive."

92 See Articles 2 and 2a and Recitals 10 – 14 Television without Frontiers Directive and Article 3 and Recital 5 E-commerce Directive.

93 See Recital 8 Data Protection Directive, indicating that the purpose of the Directive was full harmonisation with the exception of specific discretionary powers in a limited number of areas. See also Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para. 95-96.

94 See paras. 2.10.5 and 2.11, where I propose to introduce the country-of-origin principle in the Data Protection Directive.

95 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law. Adopted on 16 December 2010, 0836/10/EN WP (**WP Opinion on applicable law**) at 31 and the EDPS Opinion on revision of the Directive (n 35), at 125: "If some significant margin of manoeuvre is kept in the new instrument, the EDPS would support the suggestion from the Working Party for

principle, the Member States would each apply their own law to data processing by controllers who are "established" in their territory (i.e. such data processing is governed by the law of their "country-of-origin"). What is relevant here is that application of the country-of-origin principle results in no more than one place of establishment of the controller in respect of the data processing involved. For instance, the E-Commerce Directive provides that if the service provider of e-commerce services has more than one place of business in the EU (i.e. more than one establishment), such provider is considered "established" for purposes of application of the country-of-origin principle, in the Member State where the service provider has "its centre of activities" for that particular service. [96] The same applies to broadcasting services. The Television without Frontiers Directive provides a set of factors to determine which of multiple establishments involved in a certain broadcasting service should be considered to have 'effective control' over the relevant service (i.e. should be considered the 'primary establishment' for purposes of application of the country-of-origin principle). In the data protection context this would mean that if a parent company processes the employee data of all of its group companies in a central HR system located in a Member State, the "centre of activities" regarding this central processing and the "effective control" over such central processing is with the parent company in that Member State. Under the E-commerce Directive and the Television without Frontiers Directive, the country-of-origin principle applies **to a specific service**. If a multinational, for instance, provides different e-commerce services, then for each of these services the "centre of activities" has to be determined and these may therefore differ. As a consequence the different e-commerce services of a multinational in the EU may still be subject to the laws of different Member States. As for data protection, I propose not to link the country-of-origin principle to specific data processing operations, as these will in practice be very difficult to

---

a shift from a distributive application of different national laws to a centralised application of a single legislation in all Member States where a controller has establishments."

96 See Recital 13 of the E-commerce Directive, which makes it clear that if a provider of e-commerce services has more than one place of business in the EU (i.e. more than one establishment), such provider is considered 'established' for purposes of application of the country of origin principle in the Member State where the service provider has its centre of activities for that particular service. The same applies to broadcasting services. Article 2(3) of the Television without Frontiers Directive provides a set of factors to determine which of multiple establishments involved in a certain broadcasting service should be considered to have 'effective control' over the relevant service (i.e. should be considered the 'primary establishment' for purposes of application of the country of origin principle). See for an overview of the case law: Oliver Castendyk, Egbert Dommering, Alexander Scheuer, European Media Law (Kluwer International 2008), at 847–866.

discern. The reason for this is that by now the data processing operations of a multinational are in most cases so intertwined (and in any event connected) that it becomes very difficult to identify the separate processing operations and decide what is the centre of activities. And as the systems in most cases feed into each other, keeping track of applicable law per data feed is a practical impossibility. Instead the proposal is to apply one law to all data processing activities of a multinational which are covered by the Data Protection Directive (the multinational qualifying as a controller in this respect).[97] This would preferably be the law of the EU headquarters of the multinational (the company having control in the EU of all data processing operations of such multinational).

As a consequence the DPA of the EU headquarters will have central supervision powers and the other DPAs must assist the DPA and courts of the country-of-origin.[98] This is a form of integral enforcement which will require that the DPA of the country-of-origin has supervisory powers to the detriment of other DPAs (i.e. such other DPAs will have to relinquish their supervisory powers as to the secondary establishments in their respective territories). In return such other DPAs obtain central enforcement in respect of the processing activities of multinationals that have their primary establishment in such DPAs' respective territories. Given the level of harmonisation of data protection in the EU (which is likely to be even more extensive after revision of the Directive)[99] it is justified that the country-of-origin principle is also introduced for data protection.[100]

Taking it one step further, I cannot see any justified objection against extending the country-of-origin principle also to those countries that have obtained an adequacy finding.[101] If it is considered safe to transfer data from the EU to those countries, this implies that we can rely on the enforcement

---

97 The EDPS proposes to apply "a single legislation in all Member States where a controller has establishments". This seems mistaken. However, it may well be possible that the single law has to apply also to data processing operations in Member States other than the Member States where the multinational has an establishment (or non-EU countries for that matter). For application of the Data Protection Directive the connecting factor is not the Member States where the multinational has an establishment, but rather "whether the processing takes place **in the context** of the activities of an establishment of the controller in a Member State". The data processing operation itself may take place in another Member State or even outside the EU. See para 2.3.6.

98 See also Article 19 E-Commerce Directive.

99 See EC Communication on the revision of the Directive (Chapter 6, n 34), para 2.2.1.

100 See also para. 2.11.

101 See para. 7.1.3 and especially n 24.

systems of those countries to protect this EU originated data. Also in those cases the "trade off" in enforcement powers referred to above seems to work out in a positive manner. The benefits of obtaining central enforcement in respect of an EU-based multinational that has the centre of its processing activities in the EU seems to outweigh any national enforcement powers of Member States in respect of an EU group company that is co-controller to part of a central data base only operated by the parent company outside the EU.

However, even if introduction of the country-of-origin principle were forthcoming at the EU level (and could possibly be extended to adequate countries), it is not expected that this will be feasible on a truly international scale. Introduction of the country-of-origin principle will therefore be only a partial solution of cross-border enforcement issues. However, this being said, introduction of the country-of-origin principle would be a clear improvement to the present enforcement system in the EU, which can be extended to countries that have obtained an adequacy ruling.
In Chapters 2-4 on the applicability and jurisdiction regime of the Data Protection Directive, I have recommended the introduction of the country-of-origin principle to prevent the accumulation of applicable laws of the Member States and to achieve central enforcement.[102] I repeat this recommendation here, with the addition that I recommend extending the country-of-origin principle also to countries that have obtained an adequacy ruling.

Recommendation 1
Introduce the country-of-origin principle and extend this principle also to countries having obtained an adequacy ruling under Article 25(6) Data Protection Directive.

[102] As discussed in para. 2.11, the country-of-origin principle will become superfluous if the Directive were to be replaced by an EU regulation, with the exception of the issue of jurisdiction remaining with the DPAs. Also, if the Directive is replaced by an EU regulation, multinationals with more establishments in the EU have an interest in central supervision and enforcement by the DPA of their Member State of origin.

8.4.4 Accountability approach

Though enforcement of the APEC Privacy Framework is also based on cooperation between Member Economies[103], some form of central enforcement is achieved by Principle 26 of the APEC Privacy Framework (see Paragraph 7.4). This principle provides that if a controller transfers personal data to third parties, the controller remains accountable for taking reasonable steps to ensure that the relevant third party will protect the information consistent with the APEC Principles. As a consequence, individuals can address the original controller for breach of this obligation in addition to the third-party recipient for a breach by such third party. This results de facto in partially centralising enforcement. Even if multiple onward transfers have taken place, enforcement may still take place against the original controller. What is relevant here is that application of the accountability rule leads to more parties that can be addressed for a specific breach, but not to one party being responsible for the whole processing. There are often more parties responsible for various parts of one processing (each being controller of a part of the processing only). These joint controllers may not necessarily be established in the same country. All these controllers will remain accountable for their respective parts of the processing also after transfer if the data processing is subsequently transferred to a third party. In case of a breach, the DPAs and the data subjects can now enforce also against the original joint controllers rather than just against the data importer. Assuming that in many cases the original controller will be established in the country of the data subject, this may be considered an improvement, but will it also lead to more effective enforcement? If the DPAs and data subjects in all countries concerned have to take enforcement action to achieve full enforcement in respect of a data processing activity, enforcement is still not efficient. This would only be achieved if the accountability principle could lead to central accountability for the processing activity as a whole. This result, however, will only be achieved by implementing the country-of-origin principle rather than an accountability principle for data transfers. The following example is provided as clarification.

A multinational has set up a separate group company as a shared service centre for the data processing of all its group companies. The individual group companies transfer their data to the shared service centre which processes the data on behalf of such group companies (i.e. acts as a data

[103] Otherwise, also the **APEC Privacy Framework** (Chapter 6, n 38) is based on the principle of cross-border cooperation between national data protection supervisors rather than central supervision, see Annex B sub II and III of the APEC Privacy Framework.

processor on behalf of its group companies). The shared service centre transfers all data to a third party outside the EU. The accountability principle would make each individual group company accountable for all subsequent transfers of the data of that group company (i.e. these group companies each being the original controller of their data). However, efficient enforcement would be best served with accountability of the parent having the effective control over the central processing including all data transfers.

In addition to introduction of the country-of-origin principle the Working Party 29 seems to be in favour of introduction of an accountability rule for data transfers in the revised Directive (though this seems to be in addition to the present data transfer rules rather than as a replacement of these). [104] I discuss the merits of this proposal in Paragraph 13.6.

8.4.5 Private choice of law and forum in TPR

Central supervision and enforcement might also be achieved if companies were able to regulate their data protection in TPR and make a choice of forum for central supervision and enforcement by one "lead" DPA and the courts of the country of such lead DPA.[105] This would preferably be the authority of the place of establishment of the EU headquarters of such multinational. If a cross-border breach occurs, such lead DPA (and its courts) would be able to enforce on a cross-border basis. If this form of central enforcement is at the same time accompanied by an obligation of the multinational to facilitate cross-border enforcement within their group of companies, the beneficiaries of the TPR would also be better off. If a breach occurs, the individual will be able to file a complaint with the group company with which he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The complaint may be filed by the individual in his own language. The group company that received the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and will ensure the required translations. If the complaints procedure does not lead to a satisfying result for the individual, the group

[104] WP Contribution on The Future of Privacy (n 33), para. 39.

[105] This option is also mentioned by Prins (Chapter 6, n 9), at 178, noting however: (i) that restrictions may apply under the international private law of the home country of the relevant company adopting the TPR; and (ii) that the applicability of the rules of international private law do not provide legal certainty when applied to on-line situations. See also Wugmeister, Retzer, Rich (Chapter 7, n 61), at 477 and Cafaggi (n 61), at 227.

company will facilitate the filing of the complaint with the lead DPA or the courts of the lead DPA.

This procedure would lead to enforceable rights even in jurisdictions where no (adequate) data protection laws are in place or where insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimises cost.

Looking at the three alternatives discussed above, the conclusion from an enforcement perspective is that introduction of the country-of-origin principle is in any event to be recommended as this would lead to central enforcement throughout the EU, possibly extended to the countries that obtained an adequacy ruling. However, looking at a global scale, a choice of law and forum through TPR would seem to be a promising alternative.

To what extent data protection may be regulated by TPR and whether any choice of law and forum is allowed under PIL so that central supervision and enforcement are indeed possible, are two main topics of this dissertation and are evaluated in Chapter 13 and Chapter 12, respectively.

9 Developments and trends in multinational corporate practice

9.1 Increase in international data transfers within and between multinationals

As indicated in the introduction, the digital era shows an unprecedented continuous worldwide flow of data both within multinational companies as well as with their external service providers. These transfers are facilitated by the maturing of internet technology, but three specific factors in particular play a pivotal role:

- **Centralisation of ICT**. Multinationals recently have begun to use enhanced technology to streamline their ICT on a worldwide basis, facilitating central storage of personal data of their employees and customers (including consumers) and having these data accessible on a worldwide basis. Internet technology also increasingly facilitates central e-commerce and e-procurement solutions, involving central processing of consumer and vendor data. Multinational companies consider the efficient worldwide intercompany flow of employee and customer information and the enhanced management information generated by these central systems, to be critical for the management and competitive functioning of their operations.[1]
- **Outsourcing and off shoring**. Another trend is that multinationals outsource their ICT (helpdesk services, server management and application services) to third parties, mostly for cost reasons. As part of these services such third-party service provider processes the personal data of employees and customers of the multinational.[2] To save costs, most outsourcing suppliers subsequently offshore these helpdesk and server management services to countries outside the EU.[3] Often a "follow the sun principle" is followed to ensure 24-7 helpdesk services against the lowest costs (i.e. by making use of the regular working hours of the different time zones). Such offshoring involves the transfer of the

---

1 This research does not concern itself with the desirability of this policy of companies, but takes it as a given. In my experience, multinationals rarely take data protection considerations into account when implementing new technologies. The task for their legal departments is to address the data protection implications after the decisions to implement new (cost-saving) technologies have been made.

2 For instance with server management, the outsourcing supplier hosts the servers of the customer on which all such customer's IT applications operate (varying from HR to CRM applications).

3 Favourites are the 'BRIC' countries (Brazil, Russia, India and China).

employee and customer data to all service centres of these outsourcing suppliers in the countries involved.

- **Dynamic routing and cloud computing**. A third trend is that for the transfers of data both by multinationals and their service providers increasing use is made of technology, that leaves uncertain how the data will ultimately be routed (use is made of "dynamic routing"). Further, for storage purposes, increasing use is made of "cloud computing"[4], where it is not always[5] foreseeable where the data will ultimately be stored as use is made of unused storage capacity of other companies as it presents itself at a given moment in time.

9.2 Multiple jurisdictions

As a consequence of these trends, the central data processing and storage by multinational companies with establishments around the world and related offshoring to third countries attracts a multitude of applicable national data protection laws.[6] Some federal countries also have data protection laws that vary per state and in many cases data protection is not regulated in one comprehensive data protection law, but is found in many sectoral laws.[7] Multinational companies (whether with headquarters within or outside the EU) find compliance with all applicable national laws a "challenge" for a host of reasons:

---

4 See for the data protection implications of cloud computing, Lieneke Viergever, "Privacy in the Clouds," [2010] Tijdschrift voor Internetrecht, at 78 - 86.

5 I note that by now some cloud service providers do localise their services to a certain jurisdiction or regional zone, see Bradshaw, Simon, Millard, Christopher and Walden, Ian, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010. Available at SSRN: http://ssrn.com/abstract=1662374, at 5 and at para. 4.10.

6 If in a central system data are processed of EU subsidiaries, such central processing will in any event have to comply with all EU data protection laws. Also, the transfer of such data to the off-shoring countries will be subject to the EU data transfer rules. Other national data protection laws have a similar extensive scope.

7 Examples are the federal states of Germany and the provinces of Canada. Often data protection rules are not comprehensively enacted in a single data protection act, but rather enacted in different sectoral laws. This is even to a certain extent the case for the EU, where data protection regulations for the private sector can also be found in the e-Privacy Directive (Chapter 7, n 5).

- As many provisions of the various national data protection laws diverge or conflict outright[8] 100% worldwide compliance by a multinational is a practical impossibility. This is especially a problem if a multinational has implemented a central system for the processing of its employee or customer data. For instance, many laws impose an obligation to ensure that personal data is protected from loss and corruption. Some countries have even issued specific technical requirements. In the event of a central system, however, it may only be possible to implement **one set of security standards**; local variations may not be possible.[9] If requirements are set in technical standards, only one can be followed leading to automatic non-compliance in all other cases.
- As many national data protection laws are based on a long arm reach (to avoid gaps in the protection of personal data or to prevent circumvention of their data protection laws), it has become difficult for multinationals to track and comply with all applicable laws. This especially poses an obstacle in the event of unforeseen situations, such as a data security breach. Due to central storage and cloud computing, a single security incident may involve data of a host of individuals residing in countries around the world, which may trigger as many national notification requirements. It is difficult for multinationals to predict where a security incident will occur and whether, and if so, which types of personal data will be involved and where the individuals reside whose data are compromised. As a consequence it may be difficult to comply with security breach legislation in the event such breach actually occurs. For instance, in the US more than 45 states have imposed notification obligations on organisations that discover (or are notified about) a data security

---

8 An example is Germany, where it is required for employers to register the religious faith of employees. The processing of religious data is, however, prohibited in other Member States (see Chapter 6, n 19).

9 Even in the EU, the security requirements are not sufficiently harmonised. The Data Protection Directive just requires Member States to implement 'adequate safety measures'. Each EU country has subsequently decided for itself what it considers to be 'adequate safety measures. In Italy and Spain, the security requirements are even set in technical specifications which are difficult to combine. See Annex B ('Disciplinare Tecnico') to the Italian Data Protection Act, English translation to be found at <http://www.mofoprivacy.com>. See further the recent IT security measures introduced in Spain by Royal Decree 1720/2007 of 21 December 2007, unofficial translation to be found on the website of the Spanish DPA <www.agpd.es>. In addition there are many other laws that regulate data security, especially in relation to sensitive data such as health data, like the US HIPPAA and HITECH, see n 12.

breach.[10] While there are some similarities, these state laws have different scopes (some apply to computerised data only, others apply also to other media), different definitions of personal information, different harm thresholds, different timing requirements for notification to individuals, different requirements for notifying state agencies and credit agencies, different requirements for substitute notification, etc. Some laws even contain conflicting requirements.[11] In addition, the US has several federal laws regulating security breaches involving medical and health data.[12] At federal level specific data breach notification requirements also apply to financial institutions.[13] Besides the US, there are 13 other countries regulating data security breaches of which 8 have mandatory breach notification obligations.[14] In the EU a data security breach notification requirement has recently been imposed on the providers of electronic communication services.[15] The expectation is that this notification obligation will be extended to all data controllers in the revised Directive.[16] Further, Mexico has introduced and South Africa is presently in the process of introducing, notification requirements in the event of a data security

---

10 These state security breach notification laws are understood to be modelled on the California Security Breach Notification Act, which came into force in July 2007 (Cal. Civ. Code § 1798.82 (LEXIS through 2007, ch. 12, June 7, 2007)).

11 An example is the law of the State of Massachusetts. This law does not allow description of the incident, while several other US states require such description.

12 Health Insurance Portability and Accountability Act (**HIPAA**) of 1996 (Pub.L.104-191) and the Health Information Technology for Economic and Clinical Health Act (**HITECH**), enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5).

13 Under the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 (Pub.L. 106-102).

14 See for a summery overview Karin Retzer and Joanna Łopatowska, Dealing with Data Breaches in Europe and Beyond, PLC Cross-border Data Protection Handbook 2011/12.

15 See Article 2(4)(c) of the e-Privacy Directive (Chapter 7, n 5). The deadline for transposing the e-Privacy Directive into national laws was 25 May 2011.

16 WP Contribution on the Future of Privacy (Chapter 6, n 33):at 16; EC Communication on the revision of the Directive (Chapter 6, n 34), at 6-7; EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 75. Member States that did not await EU legislation and already introduced a general data security breach notification requirement are Germany and Austria (notification to individuals) and Ireland (notification to the DPA, which in its turn decides on notification to individuals). Member States that have voluntary guidelines prescribing notification are the UK (notification to the DPA) and Denmark (notification to individuals).

breach.[17] As a consequence of this myriad of rules, companies can only issue instructions on **how to proceed** in the event of a security incident rather than instructions on **how to comply** with all the laws in the event of an incident.[18]

- The transfer of data between EU companies and non-EU companies of the same group triggers the application of the EU transfer rules (see Paragraph 7.1.3 above). In practice the only option[19] for most multinationals to comply with these transfer rules is to introduce adequate safeguards for the protection of personal data by entering into EC Standard Model Clauses between (each of their) EU data exporting companies and (each of their) data importing companies. This is not a workable solution for multinationals that exchange numerous data between all group companies around the world as part of their daily routine. This would lead to hundreds (and sometimes thousands) of agreements to be concluded between group companies. As the data processing operations of a multinational are subject to continuous change, these contracts would require frequent updating as well.[20] The same applies if such

---

17 Mexico: Federal Law on the Protection of Personal Data Held by Private Parties (*Ley federal de protección de datos personales en posesión de los particulares*) published on 5 July, 2010, took effect on 6 July 6 2010. available at http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010 (in Spanish). South Africa – Art. 21 of the Protection of Personal Information Bill (still in legislative process) available at <http://www.pmg.org.za/files/bills/090825b9-09.pdf>

18 Thus a security breach in a central data storage facility of a multinational may trigger a host of different obligations: for instance notification obligations to Californian nationals (if data of nationals from California are involved), an obligation to offer a public apology (if data of Japanese nationals are involved) or (within the near future) an obligation to notify the breach to the EU data protection authorities (if the EU data protection laws are applicable to the processing).

19 As multinationals transfer data on a truly worldwide basis, the other derogations of the Data Protection Directive are not of practical use. The countries that obtained an adequacy ruling are only very limited in number (and will therefore not facilitate a worldwide solution). The option to obtain consent of the individuals for the transfers is in practice not possible if the data concerned are employee data. Employee consent may not be considered 'freely given' as employees are in a relationship of authority. See for a discussion of the options (and their pros and cons) available to multinationals to facilitate cross-border intra-company transfers of data: Wugmeister, Retzer, Rich (n 61), Chapter III.

20 The Rand Report (Chapter 6, n27) identifies 6 main weaknesses of the EU Data Protection Directive, of which 2 concern the EU data transfer rules (outmoded) and the EU data transfer tools (cumbersome). See also ICC Report on binding corporate rules for international transfer of 28 October 2004 (**ICC Report on BCR**), at 11, to be found at <www.iccwbo.org> Doc.373-

multinational outsources its IT to a third-party service provider with establishments in non-adequate countries. In most cases the countries involved in offshoring are **not** considered by the European Commission to provide for an adequate level of data protection (i.e. do not qualify for an adequacy finding). As a result, the transfer of personal data to these countries requires each of the EU subsidiaries of the multinational to enter into EU Standard Contractual Clauses with each of the subsidiaries of the service provider involved in providing the services.

- A complicating factor is that certain countries following suit with European legislators have also imposed restrictions on the transfer of personal data from their respective countries to countries that are (by such countries) not considered to provide an adequate level of data protection (see Paragraph 7.2 above). These data flow regulations exist not only at the national level, but also at the state level in some federal countries,[21] and may take the form of practical requirements like notification to the DPAs who may subsequently block transfers or impose conditions on them.[22] It is a serious obstacle for multinational companies to have to not only comply with the material data protection rules of each jurisdiction, but also to track and comply with all requirements relating to data transfers **between specific countries**.

9.3 Corporate mitigation of data protection risks

22/115, where as a benefit of BCR is listed as by introducing BCR, "the company does not need to conclude (and keep track of) thousands of contracts between its corporate members." See also Wugmeister, Retzer, Rich (Chapter 7, n 61), Chapter IV and V, at 475: "Managing the contracts among affiliated entities or obtaining workers' consents imposes an enormous administrative burden on companies. Any given organisation may need to manage hundreds or thousands of contracts depending on how many affiliates the organisation has at the time. In addition, anytime there is an organisational change among the parties to the contract (…), new contracts will need to be negotiated.", and at 749: "From a business perspective, Corporate Privacy Rules are attractive because they would enable organisations to implement uniform privacy policies and practices on a regional or global basis without the administrative, legal, and organisational complexities of contracts."

21 This is, for instance, the case in the German federal states and in some Canadian provinces. See Kuner (Chapter 6, n 8), at Annex B.

22 See Kuner (Chapter 6, n 8), at 22.

In order to mitigate worldwide data protection risks[23] throughout their group of companies, many multinationals have introduced some form of global corporate privacy policy. These companies have chosen a top-down approach (central instructions to their group companies) rather than trying to achieve data protection compliance on a country-by-country basis. For the reasons set out in Paragraph 9.2, these multinationals, when setting up their corporate privacy policies, more or less disregard the applicable individual national data protection laws and have set their own worldwide rules for what they consider to be an adequate protection for their employees and customers based on general principles of data protection expressed by the OECD Guidelines and as **underlying** the Data Protection Directive. Furthermore, given the administrative burdens, most multinationals ignore the EU data transfer rules and transfer their data to all group companies worldwide.[24] The same applies to the EU data transfer rules in the event of offshoring. The EU data transfer requirements are considered to create an obstacle to off shoring of services and in practice are ignored by many outsourcing service providers and multinationals alike. Although many EU DPAs have an arsenal of enforcement tools (both administrative and criminal) and cooperate amongst themselves in relation to enforcement,[25] most companies consider reputation risk to be their single greatest concern which motivates their privacy compliance in practice.[26] A strong driver here

---

23 "Risks" is used in a broad sense and from the perspective of the multinational. Risks include the risk of non-compliance with applicable national laws, risks of security breaches which may trigger applicable national data security breach notification requirements as well as the risk to the reputation of the company.

24 See Chapter 6, n 26 and 27.

25 Sanctions for non-compliance with local EU privacy laws vary from country to country, but often involve criminal liability in the event of transfer of data to countries outside the EEA, criminal or administrative fines in the event of a failure to comply with registration obligations of the relevant data processing with the national DPAs, and in some cases also criminal liability for directors is in place. Most EU DPAs can apply administrative enforcement, in which case the controller will be given a set period to comply with the local data protection laws. If the controller does not comply, the authority may remedy the violation itself. This especially poses a threat for databases that are accessible worldwide as it will be difficult to bring these into compliance with all applicable privacy laws on very short notice (the option remaining for a multinational to close down the central database, which is obviously not viable). For an overview of possible sanctions and the enforcement policies of the EU DPAs, see the report 'Privacy Protected 2008' at <www.linklaters.com>.

26 This is my experience in practice advising many multinationals on their worldwide compliance. See further McBarnet (Chapter 8, n 23) at 17, referring to research by assurance company AON, which showed that the top 2000 private and public sector organisations regard damage to their reputation as their biggest risk, under Aon Insurance Group, 2000, reported in SustainAbility,

has been the introduction of the many (especially US) data security breach notification laws (see Paragraph 9.2 above), which forces companies to notify data subjects in cases where their data are exposed due to a security breach.[27] This may lead to headlines in newspapers about such security breaches. Privacy rights' advocacy organisations collect data on major security breach notifications and ensure instant worldwide publicity by publishing the collective results on their websites and providing a forum for instant criticism and debate.[28] In that sense, it is frequently commented that there is no "hiding place" for multinationals.[29] As "brand value" is an increasing component of the market value of a company, so too is reputation.[30] Outsourcing does not diminish this reputational exposure[31] as

---

The changing landscape of liability (London, Sustainability, 2004), at 17. See also the Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 4: "There has been a transformation since the Directive was adopted in 1995, with the majority of commercial organisations now driven by reputational, financial and other reasons for ***wanting*** to process personal data properly."

27 Bamberger (Chapter 7, n 67), at 106, report their results of empirical research in the US which shows that introduction of the US data breach notification laws has been a main driver for what he calls substantial 'privacy on the ground' compliance by US companies: "While individual U.S. sectoral statutes and the EU Data Protection Directive were credited in some instances for firms' initial commitment of resources and personnel, and for the establishment of a regulatory floor, the path these professionals would take was influenced by two other regulatory developments, notably: the rise of the Federal Trade Commission's role as an 'activist privacy regulator' advancing an evolving consumer-oriented understanding of privacy; and the passage of state Security Breach Notification (SBN) laws as a means for binding corporate performance on privacy to reputation capital."

28 For an overview of worldwide data security breaches, see <www.privacyrights.org> and www.attrition.org (reporting 850 major data breaches since 2001). Many more may be found by simply searching for 'data breach security.'

29 See on the phenomenon that due to new technology there is no hiding place for multinationals as to corporate responsibility, McBarnet (Chapter 8, n 23), at 15.

30 McBarnet (Chapter 8, n 23), at 16, referring to the analysis of FTSE 100 companies in 2005, which found that 60% of the companies' market value had to be categorised as 'intangible' and 53% under US Fortune 500 in 2006. An interesting perspective on the value of reputation of a company is provided by Sacconi (Chapter 6, n 82), at 317, who explains the crucial role the reputation mechanism plays in economic theories, in particular the "trust game": "Reputation is one of the most valuable, albeit intangible, of the firm's assets. It is reputation that induces the stakeholders to trust the firm and consequently to cooperate with it, so that transactions come about at low costs of control or bargaining." See Sacconi (Chapter 6, n 82), at 18 for an explanation of how the trust game functions as to CSR which includes privacy. See further para. 15.2.10.

in practice any mistakes made by sub-contractors are attributed in the press to well-known brand holders, as they are easy targets for criticism (a phenomenon which has been labelled the "brand boomerang").[32] The classic case here is Nike. Nike, like many other multinationals, has its products manufactured in cheap labour countries by independent suppliers. Nike in fact at the time was only its designs and the brand. In 1998 the Guardian[33] reported that manufacturers of Nike products seriously violated human rights (using child labour and working hours above, and wages below, what even local laws allowed). Nike's code and local law were broken, but not by Nike (as the CEO of Nike was the first to point out). However, Nike was held to account by civil society campaigners, demonstrations, "shoe-ins" (publicly throwing away of Nike trainers), public rejection of sponsorships, a flood of publications and cartoons in newspapers, and a substantial fall in profits.[34] Ultimately, Nike also lost a court case in the US based on unfair competition and false advertising.[35] The Nike case illustrates what can happen if companies stick to a legal notion of corporate responsibility only. An example of this in the data protection field is the resignation in August 2010 by the CEO of a Hong Kong cashless payment operator due to intense criticism of the handling of data protection issues at the company, which admitted to selling personal data of nearly two million customers to business partners. The company did not violate any applicable laws or regulations, but the CEO decided to step down "as the company works to regain public trust and confidence".[36] Research shows that even in case of data leaks in

---

31 I note that in the case of outsourcing data processing operations, data security offered by the outsourcing supplier is often better than when the company itself processed the data (in my experience as a practitioner, this is often one of the reasons to outsource). In that sense, outsourcing does not create additional exposure for the company.

32 A recent example is the public attack on H&M and C&A in the Dutch newspapers (Volkskrant dated 3 September 2010) for breaching human rights when it was revealed that a manufacturer they both use in India violates the rights of (all female) textile workers by not offering an employment contract and prohibiting contact with labour unions. The women are *de facto* locked up in housing on the walled manufacturing property, 25% of their wages is withheld for their dowry to be paid only after three years of service and payment of a wedding, which will only induce workers to work extremely long hours. Additionally, the manufacturer only pays overtime after 3 years of employment. For some other examples see McBarnet (Chapter 8, n 23), at 16.

33 13 June 1998.

34 McBarnet (Chapter 8, n 23), at 16.

35 See Supreme Court of California, re Marc Kasky v. Nike, et al, 2 Cal. Daily Op. Serv. 3790, 2002 Daily Journal D.A.R. 4757.

36 See Wall Street Journal, 4 August 2010, <www.wsj.com>. It is clear is in any event that, notwithstanding consumers' lack of understanding about how companies collect and use

respect of which the multinational is not to blame whatsoever (for instance if criminal hackers have stolen data), data breach notifications in respect of confidential data (like credit card data) are shown to have a serious impact on the stock prices of listed companies.[37] This reputational exposure of multinationals for data protection and security breaches has had a strong impact on the compliance efforts of companies in an effort to try to prevent data protection and security breaches rather than address these after the fact. Given the global nature of these companies and their suppliers these efforts have necessarily extended also to countries that do not have data protection and security laws.

9.4 Other drivers for corporate privacy policies

Other factors appear to play a role in inducing multinationals to introduce corporate privacy policies. The factors discussed below are based on my experience in assisting EU-based multinationals in deciding on the introduction of BCR. Part of my research under the HiiL Program will be to perform empirical research to verify whether these factors do indeed play a role and/or whether other factors are also relevant. It is possible that this empirical research will show that the factors I encounter in practice are "EU centric" and that the factors may vary from region to region (i.e. 'national or regional narratives'). This empirical research into the "driving forces" behind BCR (also labelled "practical determinants") is part of the HiiL Program in order to be able to evaluate why a particular type of regulation has been resorted to (in particular private or co-regulation). Existing

consumer data, consumers care about their privacy. See on this topic extensively Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change, A proposed Framework for Business and Policymakers, December 2010, at 28. The FTC provides some illustrative facts and figures, such as that 35% of Facebook's 350 million users customised their privacy settings when Facebook released new privacy controls in December 2009; and the fact that 77 million Mozilla Firefox users downloaded NoScript, a privacy and security-enhancing tool that blocks Javascript commands.

37 Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security 11 (2003), at 443 – 445, which reports that they "find a highly significant negative reaction [on stock prices] for those breaches that relate to violations of confidentiality"; and L. Murphy Smith and Jacob L. Smith,
"Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?", at 12, to be found at site van de Texas A&M University http://www.tamu.edu/ : "Results suggest that costs of cyber crime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company's stock price, at least in the short run." See further Annex 6 for a table with effect on stock prices in 10 cases.

research into practical determinants influencing the emergence of new TPR in other areas of law shows remarkable overlap with the practical determinants I have encountered for BCR. For readability purposes I have included the practical determinants, as identified in this existing research regarding TPR in other areas, in the footnotes.[38] Based on my experience in

[38] See for an overview of practical determinants that play a role in emergence of TPR in other areas of law, Cafaggi (Chapter 6, n 67) at 4-8, who lists as the main factors:

(i) **Need for International Harmonisation.** The main driver is the need to overcome normative fragmentation of market regulation, often associated with divergent state legislation.

(ii) **Weakness of States as Global Rule-Makers.** It has proven difficult for States to regulate markets that operate across boundaries. The main driver for TPR is the need for harmonisation at the global level of regulatory standards or at least for strong coordination by way of mutual recognition. Failure to reach political consensus over treaty based solutions triggers TPR.

(iii) **Weaknesses of State Regulation in Monitoring Compliance with International Standards.** Often domestic monitoring brings about conflicting results which are contrary to the rationale of the international standard.

(iv) **Weakness of Public International Law.** The accountability of international organisations is still mainly ensured by states. This intermediate role hampers the rule making by non-state actors and international public entities which triggers TPR.

(v) **Technology.** New technologies and in particular the internet have redistributed rule-making power from national to transnational and public to private.

(vi) **Distributional effects**. TPR enables a shift in cost of compliance from states to private actors but also from developed economies to developing economies (where the TPR is implemented and monitored). Cost may then be partly transferred to suppliers upstream and ultimately consumers. TPR may increase the power and market share of big suppliers and impose a threshold for market entry which may be a trigger for adopting TPR).

For an overview of practical determinants specifically for CSR codes (labelled by McBarnet "contextual drivers"), see McBarnet (Chapter 8, n 23), at 13-22, which also show a remarkable overlap. Some **additional** 'contextual drivers' are identified which may be caused by the fact that CRS codes have a longer presence in the market. Examples are:

- What McBarnet calls 'concerned consumption,' whereby consumers avoid products and services of companies that they consider as having questionable ethics (e.g. the public is prepared to pay more for fair trade goods). As far as I am aware there has been no empirical research performed into whether data protection compliance has an influence on spending patterns of consumers. In practice I have encountered the situation where a multinational hesitated to implement privacy notices and consent for data processing in the connection with the sale of software based on the assumption that sales would go down. After the implementation, the multinational reported that against all

expectations, sales had gone up notably after implementation of the data protection requirements. Practice has shown similar experiences with implementation of online opt-in requirements for direct e-mail where prior opt-out requirements applied. If the opt-in opportunity was given with a possibility for consumers to select their areas of interest from among a number of options, response was larger than expected (and resulted in many consumers opting in who would have otherwise opted out). This is obviously an area of interest for further empirical research.

- What McBarnet calls a 'socially responsible investment', where investment funds and investment companies and banks screen companies based on their ethical values and compliance. For that purpose for instance the FTSE (Financial Times Stock Exchange Index) introduced in 2001 the FTSE4Good index using criteria based on CSR and the Dow Jones has the Sustainability Index. If privacy compliance is also included in CSR codes and reporting on privacy in annual accounts will be required in a prescribed format, it is not unthinkable that privacy will be included in the criteria for these indices. In certain business areas that are sensitive to privacy issues, a privacy ranking is published by the veteran international privacy watchdog Privacy International. For a ranking of the major Internet service providers, see the report 'A race to the Bottom – Privacy Ranks of Internet Service Providers", to be found at www.privacy.international.org.
- McBarnet finally reports on the self-enhancing or self-serving function of what he calls the CSR industry (CSR consultants, lawyers, accountants specialised in advising on CSR policies, offering training and writing codes of conduct; CSR standard-setting organisations; CSR reporting certification firms; CSR magazines; CSR conference organisers etc.). All these businesses have invested in CSR, with the result that CSR has become a business and a market factor itself. This is fuelled by the fact that many working in this area are CSR 'enthusiasts' and have a personal interest in keeping up CSR momentum. A clear parallel with the data protection area can be seen here. The recent past shows many new privacy right advocacy organisations, privacy seal organisations, and specialist privacy consultancy firms, and within my experience equal enthusiasm is apparent as in the CSR sector.

The empirical research to be performed in respect of contextual drivers for BCR as part of the HiiL Program will show whether the additional contextual drivers as identified by McBarnet indeed also play a role for BCR. However, as Neil Gunningham notes in respect of corporate environmental responsibility, the general conclusion will probably be that many contextual drivers play a role varying from law and social and economic pressures. See Neil Gunningham, "Corporate environmental responsibility: the law and the limits of voluntarism" in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 500. See on the rise of private regulation in the world economy: Büthe and Mattli (Chapter 7 n 62), at Chapter 1 "The Rise of Private Regulation

practice, I believe that the following practical determinants have played a role in the decision-making of multinationals to introduce corporate privacy policies:

- Given the diverging (and in many instances conflicting) national data protection rules, 100% worldwide compliance is practically impossible.[39] In respect of central systems and applications, therefore many **policy decisions** have to be taken in respect of data security and data processing rules on the basis of what such company considers as offering **adequate protection** rather than full compliance with all relevant national laws. These strategic decisions have obviously to be taken on a central level and then imposed on the various group companies. This is generally effectuated by means of implementing a corporate privacy code.
- As data from central ICT systems may also be processed by employees in countries where no (adequate) data protection law applies, such employees have to be instructed on how to process the relevant data stored in the central systems, which is also done by means of a corporate privacy policy.
- But even if a country does provide for an adequate level of protection, a privacy policy is generally required. For instance, the EU data protection rules concern general processing principles, which have to be "translated" into practical guidelines for employees involved in the processing of the data. One of the processing principles is that data may be processed "for specified and legitimate purposes only". This requires a specification tailored to the operations of the multinational of which categories of data may be processed, for which purposes, by which categories of employees, and for how long such data may be subsequently stored. The use of open norms is one of the reasons that the Data Protection Directive

in te World Economy", in particular at 5: "This simultaneous privatization and internationalisation of governance is driven, in part, by governments' lack of requisite technical expertise, financial resources, or flexibility to deal expeditiously with ever more complex and urgent regulatory tasks, Firms and other private actors also often push for private governance, which they see as leading to more cost-effective rules more efficiently than government regulation". See further at 25, where Büthe and Mattli note as a main driver for TPR the "excruciatingly slow pace of standards production" of public regulators.

39 Implementation of all national laws would de facto imply that the strictest national law applies to a multinational on a worldwide basis. For most companies this is understandably not an acceptable starting point. The EU DPAs have in practice recognised this by accepting BCR that provide for an adequate level of protection rather than only authorising BCR which comply with all applicable national requirements.

explicitly encourages the introduction of privacy codes for sectors of industry, as it is understood that the general norms may require specification for specific industry sectors.[40]

- Multinationals apply a risk-based approach to regulatory compliance, including data protection compliance.[41] Priorities are identified in the roll-out of compliance measures, whereby priority is given to high-risk data processing systems (such as sensitive or financial data) and to systems that have the largest security risks (such as cross-border systems). This is in line with the approach to data protection compliance taken from the start by the Working Party 29.[42] These strategic decisions based on a risk assessment can

---

[40] Recital 61 Data Protection Directive.

[41] This is based on my experience assisting multinationals with their data protection compliance. Risk assessments of data processing systems are generally performed by the multinational by means of "Privacy Impact Assessments" (**PIAs**). In most cases, firstly a quick scan will be made to assess the risk category of each system. After this, the high risk, cross-border systems will be subject to the most extensive PIA and certain local-for-local paper-based filing systems with low risk will not be subjected to further review. On the risk-based approach of multinationals in relation to their supply chain management, see paragraph 13.3, in particular of Doreen McBarnet and Marina Kurkchiyan, "Corporate social responsibility through contractual control? Global supply chains and other regulation," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 63: "The supply chain is becoming increasingly recognised as an area of reputational – and indeed insurance – risk, with a number of companies beginning to develop a "risk-based approach to supplier engagement" and "systems to identify higher risk suppliers" (referring to Vodafone's Corporate Social Responsibility Report for 2004 – 2005, at 24 and other examples listed).

[42] The Working Party 29 applied from the start a risk-based approach to data protection compliance, indicating as the first (of three) objectives of the Data Protection Directive "to deliver a good level of compliance", acknowledging that a 100% compliance is not achievable in practice. See WP 12 (Chapter 7, n 22), at 7: "The objectives of a data protection system are essentially threefold: 1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them." The Working Party 29 further applied from the start a risk based approach as to the content of data protection obligations (i.e. requiring more strict security measures in case of a transfer of sensitive data, etc), as well as to identifying priorities in enforcement for the DPAs. See WP 12 (Chapter 7, n 22), at 28. Such a risk-based approach is further in line with the First recommendation for amendment of the Data Protection Directive made in the Rand Report (Chapter 6, n 27) at 42: "Encourage the use of a risk based approach to the application of the rules, focussing on acts of data processing where harm can reasonably be expected." See further at 50, where the Rand

only be taken at a central level (mostly by the parent) and then imposed on the group companies. This risk-based approach to data protection is compatible with the broader trend of introducing the "principle of accountability" for data protection, which is also risk-based and fits in with the trend where legislators focus on achieving desired outcomes through regulating corporate governance processes. This signifies a decisive move in the direction of abandoning traditional "command and control" state regulatory schemes in favour of "responsive regulation", which is supposed to facilitate self-regulation programs.[43] Introduction of the accountability principle in the Data Protection Directive is in conformance with the proposal of the Working Party 29 to the Commission for the revised Directive and the Rand Report[44], which proposals the Commission intends to adopt.[45] Introduction of the accountability principle will mean that multinationals will have to implement a data protection compliance program, which in any event will require a corporate privacy policy setting the data

---

Report recommends the introduction of the accountability principle (see on the accountability principle para. 13 below), and recommends that all compliance tools (like privacy policies, PIAs, training programs) will be drafted on a risk- based approach, reflecting the scale of the data processing (amount of data, cross-border environment) privacy-sensitive nature (health data), and the field of activity of the data controller (financial sector, healthcare). The Rand Report, at 57, recommends introduction of a risk-based sanction system. The EDPS proposes a risk-based notification system, by proposing to limit the obligation to notify to specific kinds of processing that entail specific risks, stating that "these notifications could trigger further steps such as prior checking of the processing." This is without prejudice to the prior-checking requirement also imposed on the basis of specific risks, such as large scale information systems (EDPS Opinion on the revision of the Directive, (Chapter 6, n 35), at paras. 62, 63 at 15).

43 For instance in respect of achieving desired CSR outcomes, see Christine Parker, 'Meta-regulation: legal accountability for corporate social responsibility', in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 228: "To the extent that scholars and policy makers focus on achieving CSR through corporate governance processes (i.e., meta-regulation), it signifies a decisive move in the direction of abandoning traditional "command and control" state regulatory schemes in favour of "responsive regulation", which is supposed to facilitate – yet not enforce and dictate – self-regulation programs and "compliance-oriented" regulation, which is carried out through corporate consent and voluntary organizational processes of reflexive learning." For more detail on risk-based regulation, see para. 13.3.

44 See WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 37 - 39 and for a more detailed opinion on the accountability principle itself, see WP Opinion on the principle of accountability (Chapter 1, n 15),, at 10.

45 See EC Communication on the revision of the Directive (Chapter 6, n 34), at para. 2.2.4.

protection standard (see for the implications of the introduction of the accountability principle in the revised Data Protection Directive Chapter 13 below).

- Enforcement action by DPAs customarily starts with a regulatory investigation (privacy audit). In order to be able to show (initial) privacy compliance, the multinational subject of an investigatory audit will have to have readily at hand (i) the internal data processing instructions (the corporate privacy policy) and (ii) the results of its internal privacy audits (auditing compliance against the corporate privacy policy). Experience shows that DPAs realise that 100% privacy compliance is not achievable, but accept this as long as a company takes a structured approach to its privacy compliance.
- Last, but not least, the introduction of corporate privacy policies fits within the broader trend of CSR where multinationals adopt CSR codes to express their commitment to human and civil rights, the environment, opposition to bribery and corruption and fairness to their customers and suppliers. The range of issues is constantly expanding[46] and many CSR codes[47] also contain a commitment to protect the privacy of employees and customers.[48] At first, for some multinationals adoption of privacy commitments was part of a strategy to achieve competitive advantage in an industry sector.[49] Practice has shown that for instance licence revenues increase if proper privacy policies are implemented.[50] By now, however,

---

46 See on SRC for instance Sacconi (Chapter 6, n 82), at 289 – 344. See further the research listed in "The added value of private regulation in an international world? Towards a model of the legitimacy, effectiveness, enforcement and quality of private regulation," HiiL 2007 – 2008, at 8-10, to be found at <www.hiil.org>.

47 Often called: 'Company Ethics Code,' 'Company Business Values' or 'Company Business Principles'.

48 See for instance the CSR codes of Philips, Shell and Sara Lee.

49 This certainly applies to adoption of CSR codes (see McBarnet (Chapter 8, n 23), at 21), but in my experience also (to a lesser extent) applies to adoption of privacy commitments. For instance the Dutch ISP XS4All made it a distinguishing factor in its advertising campaign for paid ISP services, where it depicted under the heading 'Everything has a cost,' the privacy provisions in the general terms and conditions of its main competitors providing free ISP services, allowing such competitor to sell the personal data of its subscribers to third parties for advertising purposes.

50 This is based on my own experience where multinationals that were initially reluctant to comply with privacy requirements (based on the expectation that sales or response to opt-in requests would be less than without the privacy measures) reported later that (to their surprise) sales and

adoption of privacy commitments no longer seems to be an advantage but non-adoption a disadvantage.[51] See Paragraph 15 for an evaluation of BCR in the context of CSR.

It is on account of these drivers that some multinationals introduced corporate privacy policies and, having introduced these policies, asked the DPAs to recognise these policies as an alternative means to comply with the EU data transfer rules. The underlying thought is that as their policies introduce an adequate level of protection within their group of companies, this company group constitutes a "safe haven" for the processing of personal data, as a result of which data may flow freely between the companies within the group. In the next chapter I discuss the EU authorisation procedure and the conditions under which a global privacy policy of a multinational may be recognised as Binding Corporate Rules, constituting an alternative method of complying with the EU data transfer rules.

opt-in responses had increased remarkably after the privacy protecting measures were implemented. It would obviously be interesting to verify this by conducting empirical research.

[51] This is a common feature with general experiences with CSR. See Conley and Williams (Chapter 6, n 67), at 21.

10 Implementation of self-regulation: Binding Corporate Rules

10.1 Introduction

The complications with the EU transfer rules have led multinationals to put pressure on the DPAs to recognise their corporate privacy policies as equivalent to the EU Standard Contractual Clauses for the purpose of facilitating their intercompany transfers of personal data.[1] As their corporate privacy policies are based on the general processing principles of the OECD Privacy Guidelines and of the Data Protection Directive (see Paragraph 7.1.1), it can be argued that they establish an "adequate level" of protection of personal data within their group of companies (a "safe haven"). Insofar as such processing involves data transfers to group companies in a non-adequate country, the policy provides for the "adequate safeguards" as required pursuant to Article 26(2) Data Protection Directive.[2]

The Working Party 29 and the DPAs are well aware of the fact that multinational companies exchange personal data on a worldwide basis (through their central systems) and outsource their ICT to non-adequate countries and realise that the traditional jurisdiction-based enforcement

---

[1] See Lokke Moerel, "Privacy without Borders," Dutch Financial Times 3 April 2003. In reaction to this publication, the Data Protection Commissioner of the Dutch DPA (Peter Hustinx) invited the 10 major Dutch-based multinationals to discuss the possibility of BCR as a tool for data transfers, which resulted (after long discussions) in a template form BCR which had the informal approval of the Dutch DPA. The work performed by the Dutch DPA and this working group was subsequently used by the Working Party 29 in its discussions and drafting of the WP Opinions.

[2] As required for the transfer of data to non-adequate countries pursuant to Article 26(2) Data Protection Directive. This exercise is different from the approval of codes of conduct provided for in Article 27 Data Protection Directive, which codes are aimed at the practical application of the relevant applicable national data protection law in a specific sector. These codes of conduct therefore have to be fully compliant with the relevant national law. For BCR it is sufficient that they provide for an adequate level of protection which may be in some respects different from or stricter than applicable data protection laws of the Member States. Note that the BCR do not set aside any applicable national requirements; the company will remain bound by law. These national requirements, however, do not need to be included in the BCR. See WP 74 Transfer of personal data to third countries: applying article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003, at 7 (**WP 74**). A common denominator of BCR and codes of conduct under Article 27 Data Protection Directive is that both are supposed to overcome the level of abstraction of the data protection processing principles. See WP 74 (n 2), at 14.

tools are not adequate to force compliance.[3] The Working Party 29 has recognised the added value of transnational corporate self-regulation in the data protection area in light of the deficiencies of the present enforcement regime of the Data Protection Directive and has recognised corporate self-regulation as an alternative method of complying with the data transfer rules of the Data Protection Directive.[4] Thus the Working Party 29 in fact has approved a voluntary system of a combination of self-regulation with public validation and enforcement. For the paragraphs hereafter, it is relevant that the Working Party 29 has advisory status only.[5] Though the opinions of the Working Party 29 are followed in practice by the individuals DPAs, they are not obliged to do so and (in relation to Binding Corporate Rules) some follow their own course.[6]

10.2 BCR requirements

To date, the Working Party 29 has issued seven Opinions[7] (**WP Opinions**) setting out criteria that a corporate privacy policy should meet before it can be approved as "Binding Corporate Rules" (**BCR**).
The WP Opinions make clear that recognition by DPAs of BCR as a valid tool for data transfers is voluntary.[8] As BCR are not recognised in the Data Protection Directive, it is up to the DPAs in the national approval procedures whether to recognise BCR as a valid tool for data transfers or not.[9] The Working Party 29 has issued a checklist with the elements that the Working

---

3 See Chapter 6, n 26.

4 See WP 74 (n 2), at 6. See for a comprehensive overview of benefits of BCR for individuals and businesses: Wugmeister, Retzer, Rich (Chapter 7, n 61), Chapter V.

5 See Chapter 6 n 29.

6 See Chapter 6 n 29.

7 WP 74, (n2); WP 107, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting from 'Binding Corporate Rules,' adopted on 14 April 2005 (**WP 107**); WP 108, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules adopted on 14 April 2005 (**WP 108**); WP 153, Working Document Setting Up a Table with the Elements and Principles to be found in Binding Corporate Rules adopted on 24 June 2008 (**WP 153**); WP 154, Working Document Setting Up a Framework for the Structure of Binding Corporate Rules adopted on 24 June 2008 (**WP 154**); WP 155 Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adopted on 24 June 2008 (**WP 155**); and WP 133, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data adopted on 10 January 2007 (**WP 133**). For a general discussion of the BCR requirements see Kuner (Chapter 2, n 29), at paras 4.120-153.

8 WP 108 (n 7) at 2.

9 BCR are subsequently not recognised by all DPAs, see further below at n 40.

Party recommends being incorporated in the BCR and considered by the national DPAs in their assessment of adequacy.[10] The Working Party 29 has announced that the requirements are not carved in stone and may be revisited.[11] Indeed, the Working Party 29 has held a consultation[12] and a Public Hearing[13] on the first of the WP Opinions, the input from which was taken into consideration when developing its subsequent WP Opinions. Some DPAs (e.g. of the UK and Austria) have published further national guidance clarifying issues a company must address in its BCR.[14] The main requirements set by the Working Party 29 for BCR are the following:

(i) If the headquarters of the multinational are not established within the EU, the multinational should appoint an EU group company to have delegated data protection responsibilities (**Delegated EU Headquarters**).[15]

(ii) The BCR should be submitted for approval to the DPA of the Member State where the relevant multinational has its headquarters (**EU Headquarters**). If the multinational does not have its headquarters in the EU (or it is not clear where the ultimate parent company is established), the application must be submitted to the "most appropriate" DPA, which will in most cases be the DPA of the Delegated EU Headquarters (the "**Lead DPA**").[16]

---

10 See for the latest checklist WP 153 (n 7).

11 This was announced in WP 74 (n2) and in practice the later WP documents issued by the Working Party do indeed deviate in certain respects from the requirements initially listed in WP 74.

12 For which a number of multinationals and industry groups were invited to submit their input. See for their contributions <www.ec.europa.eu>.

13 See the Official Summary of the Public Hearing on internal codes of conduct for multinationals drafted by the Dutch Data Protection Authority, to be found at <www.ec.europa.eu>. The Public Hearing was attended by 30 representatives of the business community and one consumer organisation.

14 For the UK: "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers: Putting the concept into practice in the United Kingdom," Information Commissioner, 11 February 2004, to be found at <www.ico.gov.uk>. For Austria: "Required Contents of Submission for Approval of 'Binding Corporate Rules' to the information Commissioner," Information Commissioner, SR/HR/BCR Checklist 11/2/2004, at 1, to be found at <www.dsk.gv.at>.

15 See for this requirement WP 74 (n 2), at 18.

16 See WP 107 (n 7) for relevant criteria to decide which DPA is the most appropriate.

(iii) The geographical and material scope of the BCR should make clear whether the BCR apply worldwide or to EU originated data only[17]/[18], which data are covered, the categories of individuals covered, the countries covered, etc.

(iv) The BCR should describe the **nature** of the data processed (i.e. categories of sensitivity), the **purposes** for which they are processed and the extent of the international **data transfers** within the group.

(v) The BCR should incorporate the material data processing principles (transparency, fairness, purpose limitation, data quality, rights of individuals and security (see also Paragraph 7.1.1 above) and the

---

[17] The Working Party 29 accepts that the scope of the BCR is limited to EU-originated data only. In practice most companies opt for applicability of their BCR to all data processed by the company. Various factors play a role in this decision. Most important factor is that companies find it hard to explain to their employees and customers why protection is afforded to some and not to others, which is often experienced as an unjustifiable discrimination between individuals. This is especially the case with multinationals headquartered in the EU, where adherence to data protection rules is by now part of their regular compliance and has been integrated in their corporate culture, as a consequence of which the limitation of these rights to EU-originated data based only on the argument that other countries do not require that protection, seems against the ethical sensibilities of the managers. For a similar effect of other forms of TPR, see Conley and Williams (Chapter 6, n 67), at 15, and literature therein referred to. More practical determinants are: (i) the fact that it is difficult to 'tag' EU-originated data in such a manner that compliance with the BCR can be ensured also if these data are further transferred to other databases within the company (this is a common occurrence as often local databases are "fed" with data stored in the central HR or CRM database; and (ii) the fact that the employees who process data often process both data of EU origin data and non-EU-originated data, and would have to receive different sets of instructions for the different types of data even while these often coincide in the same databases. Compliance with the BCR for EU-originated data can then only be ensured by imposing the stricter BCR processing regime.

[18] Examples of BCR that have introduced some form of limitation as to scope are the BCR of DaimlerChrysler (which applies only to personal data that are subject to data transfer restrictions) and those of GE (these BCR apply to all data processing worldwide, but do not provide for an 'adequate' level of data protection according to EU standards. For EU-originated data, GE has added an addendum to its BCR that provides for additional requirements for the processing of EU-originated data, which ensures the required adequate level to obtain the required permit for data transfers. Other options to limit the scope of BCR to a certain extent are for instance: (i) to apply the material processing principles of the BCR on a worldwide basis regardless of the origin of the personal data and the location of the processing, but restrict the BCR for transfers to third parties (outside the group of companies) to EU-originated data only; and (ii) to exclude from the transfer rules any local-for-local transfers.

restrictions on onward transfers to third parties outside the group (see also Paragraph 7.1.3).[19]

(vi) The BCR should be **internally** binding within the organisation (on all group companies and on employees) and **externally** binding for the benefit of individuals (i.e. must create third-party beneficiary rights for individuals).

(vii) The BCR should provide for a network of privacy officers for handling complaints and ensuring compliance with the rules.

(viii) There should be an internal complaint handling process.

(ix) Compliance with the BCR should be enforceable by the individuals via the DPA and the courts in the Member State of (i) the EU group company at the origin of the transfer ***or*** (ii) the EU Headquarters or the Delegated EU Headquarters.

(x) The (Delegated) EU Headquarters should accept liability for paying compensation and remedying breaches of the BCR.[20]

(xi) The burden of proof with respect to an alleged breach of the BCR should rest with the (Delegated) EU Headquarters and not with the individual.[21]

(xii) The group companies should have a duty to cooperate with the DPAs, to abide by their advice regarding the BCR and to submit to their audits.[22]

(xiii) The BCR should provide for an auditing programme covering all aspects of the BCR, including methods of ensuring that corrective actions have taken place. The audits have to take place on a regular basis (by either internal or external accredited auditors) or on specific request from the corporate privacy function. The BCR must

---

[19] See WP 154 (n 7) on how these general processing principles can be 'translated' into practical requirements in BCR.

[20] The WP Opinions do not specify according to what law this liability should be considered.

[21] This requirement has been criticised by companies applying for BCR. The main criticism is that the full reversal of the burden of proof entices frivolous and unfounded complaints by data subjects, which are difficult to disprove by the company (it being impossible to prove a 'negative'). In practice the Lead DPAs accept the following provision: "Where data subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCR, it will be for the EU headquarters to prove that the member of the corporate group outside of Europe was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place."

[22] This requirement has also been criticised by companies applying for BCR. Not all DPAs have audit rights under their national law and would now acquire such rights just because a company opts for BCR. In practice, Lead DPAs accept that the right to have access to the audit results and the audit right is granted to the Lead DPA only. Other DPAs keep their own access rights and audit rights to the extent they have these under their own laws.

provide that the results of the audit will be communicated to the privacy function and the ultimate parent's board. The DPAs must have the right of access to the results of such audits.

(xiv) The individuals concerned should have easy access to the BCR, and in particular easy access to the information about their rights.

(xv) There must be a suitable training of the employees who process the data.

(xvi) There should be a process for updating the BCR and a mechanism for reporting changes in the BCR to the Lead DPA.

(xvii) The group companies should be obliged to be "transparent" if applicable national law prevents the group from complying with the BCR, to take an informed decision about what action to take, and to consult with the Lead DPA in case of doubt.

10.3 Different types of BCR

10.3.1 BCR for Controllers

The BCR regime as developed by the Working Party 29 addresses the data processing obligations of **data controllers**.[23] This is logical as the requirements of the Data Protection Directive are directed at controllers of personal data only. The Data Protection Directive does not (directly) impose obligations on data processors.[24] Instead, the Directive imposes an obligation on controllers, when they involve a data processor to process data on their behalf, to impose certain mandatory requirements on that processor. In Paragraph 6.1 I discussed how multinationals in the course of their business activities process different types of data, the main categories being (i) employee data, (ii) personal data of customers, suppliers and other business partners, and (iii) specific categories of data. An example mentioned of the last category is the processing by the pharmaceutical industry of large quantities of patient data as part of their scientific research. Here a patient is neither employee nor customer or business partner. In respect of all these categories, the multinational processes these data in its capacity of data controller. However, it is possible that group companies in certain cases also act in a capacity of data processor on behalf of other group companies. This is, for instance, the case if a multinational has centralised certain data processing operations in a shared service center. In that case one of the group companies providing the shared services processes data on behalf of other group companies (i.e. in a capacity of data processor). Such data processing will still be covered by the BCR for data controllers as in that

[23] See for definition Chapter 13, n 145 below.

[24] See para. 7.1.1.

case other group companies of the multinational qualify as controller (as a result of which the processing activities are still covered by the BCR). This is no longer the case if a group company starts processing data on behalf of a third party outside the multinational group of companies. These activities would not be covered by a BCR for controllers. See however Paragraph 10.3.3 for the possibility of BCR for Processors.

10.3.2 BCR for Employee Data vs BCR for Customer Data

Though in theory one comprehensive corporate privacy policy would be feasible setting out the data controller obligations for the processing by a multinational of all different categories of data, in practice multinationals regulate these different types of data by separate BCR. The reason is first and foremost the clarity of the relevant policies and the resulting processing instructions for the employees who process the different types of data. By adopting different policies for the separate categories of data, the instructions can be more tailored to the processing at hand. This is desirable because the applicable data protection rules vary according to the data processed. For instance, direct marketing rules are of relevance only for customer data, and not for employee data. Also, the consent rules vary on whether consent is requested of a customer or of an employee. Yet different rules apply if specific categories of data are processed, like the patient data for research purposes as mentioned before. From a practical perspective, these different types of data are mostly also processed by different departments within a multinational; customer data are mostly processed by the marketing department, employee data mostly by the HR department and patient data by the R&D department. Also for this reason separate sets of instructions are indicated. To illustrate the differences and how these work out in concrete examples of BCR, I attach as **Annex II** an example of a BCR for Employee Data and as **Annex III** a BCR for Customer Data. These template forms incorporate the relevant requirements and have been approved by a number of DPAs.[25]

[25] In April 2011, the Working Party 29 started publishing the BCR that have been approved, to be found at http://ec.europa.eu/justice/policies/privacy/binding_rules/bcr_cooperation_en.htm. The website (which since its launch has not been updated) indicates that the BCR of 15 multinationals have been approved by 5 Lead DPAs (UK, France, Luxembourg, the Netherlands and Germany). Some of these BCR are for employee data, others for customer data and others for both. In January 2011, the Dutch DPA informally communicated that 46 BCR applications were in the pipeline throughout the EU.

10.3.3 BCR for Processors

If a multinational processes personal data on behalf of its customers, these activities fall outside the BCR for controllers. This is the case if, for instance, the business activities of a multinational consist of the provision of data processing services to other companies (e.g. payroll processing on behalf of a customer). Such customer data are then processed by the relevant multinational in a capacity as data processor. Until now the BCR regime has been applied to data processing obligations of controllers only.

However, there are no convincing reasons why a BCR for Processors would not also be conceivable. As already discussed in Paragraph 9.1, if a multinational with establishments in the EU outsources data processing services to a third-party service provider with establishments in non-adequate countries, this also triggers the application of the EU transfer rules. As a result, the transfer of personal data to these countries requires each of the EU subsidiaries of the multinational to enter into EU Standard Contractual Clauses with each of the group companies of the service provider involved in providing the outsourcing services. A solution for the requirement of these numerous EU Standard Contractual Clauses may be that the outsourcing provider also adopts BCR to regulate its data processor obligation. The BCR would then consist of a privacy policy which applies to all group companies of the service provider introducing company-wide processor obligations (especially as to the company wide security requirements),[26] together with general commitments in respect of training, auditing, etc. If the multinationals being the controller of the data have BCR for Controllers in place and the outsourcing service provider being the data processor have BCR for Processors in place, a free exchange of data would also be facilitated between these two multinationals. The concept of an organisational tool to govern the involvement of a data processor is already embodied in the EU Standard Contractual Clauses for controller-to-processor relations and further exists under the Safe Harbor Framework, where companies can either adhere to the controller regime or the processor regime.[27] A first draft BCR for processors has been submitted to the Working Party 29 for opinion. Since introduction of a potential regime for BCR for

[26] The possibility of BCR for processors was first suggested by myself at the Conference on international transfers of personal data, co-organised by the European Commission, the Working Party of Article 29 and the U.S. Department of Commerce, Brussels (23-24 October 2006), and further by Eduardo Usteran at several other data protection conferences. See Binding Safe Processor Rules, at www.youtube.com.

[27] http://www.export.gov/safeharbor.

Processors is outside the scope of this dissertation, I will refrain from elaborating on it here.

10.4 EU BCR approval procedure

In principle a multinational requires the approval of its BCRs in all Member States[28] where it has an establishment and from where personal data are transferred outside the EU. To facilitate the approval procedures, the Working Party 29 initially introduced the "EU Cooperation Procedure" (**CP**).[29] The multinational had to introduce the CP by approaching the most appropriate DPA[30], which was then appointed as "lead" DPA (**Lead DPA**). The Lead DPA subsequently coordinated the comments of the other DPAs whose approval was required, which led to a final draft that was subsequently circulated again by the Lead DPA for final approval.

After the first experiences with the CP had been positive, the DPAs of (by now) 19 Member States joined the "Mutual Recognition Procedure" (**MRP**), which entails that these DPAs will mutually recognise each other's adequacy findings in respect of BCR without further review of the draft BCR involved.[31] Like the CP, the MRP requires that one of the DPAs is appointed Lead DPA. This Lead DPA will be assisted by one or two other of the relevant DPAs to co-review the BCR (**Co-Leads**). The Co-Leads should be the DPAs of a Member State where the relevant multinational has "a strong presence". The steps to be taken are as follows: the multinational submits its BCR application to the DPA it considers suited to act as Lead DPA and lists the Member States in which the multinational has a presence. This DPA will subsequently contact the other DPAs involved to solicit their consent that it indeed may act as Lead DPA. After it has been established that the relevant DPA can indeed act as Lead DPA, the Co-Leads will be selected and contacted by the Lead DPA. Then the consultation phase starts where the

---

28 This except for the UK where submission is voluntary. See: "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers: Putting the concept into practice in the United Kingdom," Information Commissioner, 11 February 2004, to be found at <www.ico.gov.uk>.

29 See for a description of the co-ordinated procedure WP 107 (n 7).

30 See WP 107 (n 7), at 2 for the relevant criteria to decide which DPA is the most appropriate to act as Lead DPA.

31 See for a first press release Working Party 29 on 2 October 2008. At present, the following countries have joined the Mutual Recognition Procedure: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovak Republic, Spain and the United Kingdom. Some DPAs (like the Danish DPA) have not officially adhered to the MRP, but in practice automatically approve applications for BCR that have been approved in the MRP.

BCR are reviewed by the Lead DPA and discussed with the multinational, which may lead to amendments to the BCR (see Paragraph 5.3 for the sequence of steps of this consultation phase). After the consultation phase has ended the BCR will be informally approved by the Lead DPA. The lead DPA will then solicit the input of the Co-Leads. Apparently there are informal agreements between the DPAs that are part of the MRP to respond to the request of the Lead DPA for input within one month.[32] The comments of the Co-Leads may lead to further consultations with the multinational and possible changes to the BCR. The so-finalised BCR will then have to be formally adopted by the ultimate parent of the multinational. After having been formally adopted by the multinational, the BCR will be submitted for formal approval by the Lead DPA. Upon formal approval by the Lead DPA, the BCR will automatically be recognised by the other DPAs that are part of the MRP. For those Member States that are not part of the MRP and in respect of which the multinational requires an approval, the Lead DPA will initiate the CP to obtain the approval of the BCR by the DPAs of such countries.

10.4.1 How to align the MRP with EU works council requirements?

Multinationals introducing BCR and starting up the MRP have to make sure that these procedures are in accordance with EU works council consultation and approval requirements. A multinational with subsidiaries in two or more Member States can be obliged to set up a European works council (**EWC**).[33] The rights of the EWC are generally limited to information and consultation with regard to matters with a EU dimension which are of common interest to the entire group, or to at least two group companies in different Member States. As a rule of thumb, adoption of the BCR is a matter that falls within the scope of the rights of the EWC. The EWC - if established - must therefore be informed of and consulted on this matter.

Multinationals with establishments in the EU will further have to comply with specific works council requirements in the Member States in which they have establishments.[34] In some Member States they will be obliged to set up a national works council (**WC**) and (if more group companies are established in a Member State) also a central works council (**CWC**). Matters which are of common interest to the majority of the group companies in a Member State will be dealt with by the CWC (in most Member States to the detriment of the rights of the WCs). The specific rights to which a national

[32] This is according to informal information provided by the Dutch DPA. At present, the experience in practice is that these timelines are not observed by the Co-Leads.

[33] Pursuant to Directive 1994/45/EC of 22 September 1994.

[34] As a result of Directive 2002/14/EC of 11 March 2002.

WC/CWC is entitled must, however, be determined on the basis of national legislation. As a rule of thumb, the intended decision to introduce BCR requires in most Member States at least the prior information and consultation of the WC/CWC and in some Member States, their prior consent.[35] Further, the actual decision to adopt the BCR can also require the consent of the WC/CWC. The rights of the WC/CWC apply next to those of the EWC (unless explicitly agreed otherwise).

Multinationals have to ensure that they comply with the works council requirements as part of the MRP. This will mostly entail that as soon as a company decides to embark on a BCR project (i.e. before a DPA is contacted to act as Lead DPA), the local WC/CWC in each Member State and the EWC should be informally consulted. For that purpose, the company has to inform the EWC/WC/CWC:

(i) that draft BCR are being drawn up;
(ii) that the draft BCR will be drawn up in consultation with the Lead DPA;
(iii) that the local WC/CWC will be consulted when the draft BCR has the **informal** approval of the Lead DPA;
(iv) of the timeframe in which all the above will take place.

Once the Lead DPA has given its **informal** approval, the formal consent procedure or advisory proceedings (depending on the applicable national rules) with the WC/CWC are instituted. As the EWC has already been consulted, it is sufficient to inform the EWC of the final result.

To enable a multinational submitting BCR to the MRP to meet these works council requirements, the most logical sequence of steps in the consultation phase is as follows[36]:

(i) the multinational submits its draft BCR for review and informal approval by the Lead DPA;
(ii) after the informal approval from the Lead DPA is obtained, the company institutes the formal works council consent or advisory proceedings (this depending on the applicable national rules);
(iii) when the consent of the works council is obtained (or the works council consultation procedure is completed), the company formally adopts the BCR (which in most cases

35 See for instance Article 27 para. 1 under k Dutch Works Councils Act.

36 These are the steps agreed with the Dutch DPA if it acts as Lead DPA in a BCR approval process.

takes adoption of the BCR by the board of management of the parent company of the multinational);

(iv) the company submits the adopted BCR for formal approval by the Lead DPA.

The sequence above is the most opportune for various reasons. Formal approval by the Lead DPA will only be given by the Lead DPA for BCR that have been formally adopted by company (to avoid the risk that the MRP has to be reopened in case of changes).

The company in its turn will only formally adopt the BCR after it has obtained the comfort of the Lead DPA that what it adopts will be acceptable to the Lead DPA (i.e. after informal approval is obtained).[37]

Further, the company can only formally approve the BCR after it has obtained the approval by the works council (or after the consultation process has been completed). In any event the company will want to avoid that the works council is consulted about BCR that may not be acceptable to the Lead DPA. The reason for this is that multinationals in most cases have establishments in a large number of Member States. The (coordination of) the formal works council consent and consultation procedures involves as many countries and may take many months. Any changes to the BCR will yet have to be resubmitted to the works council procedures, which would lead to unnecessary delays. Another reason is that the works council in its turn in practice heavily relies on the informal confirmation by the Lead DPA, that the BCR in question indeed provide for an adequate level of protection (and thus meet the criteria of Article 26(2) Data Protection Directive).

10.5 Shortcomings of the EU BCR approval procedure

Though the present system of the MRP (possibly supplemented by the CP) is obviously a substantial improvement as compared to just the CP, the situation is still unnecessarily cumbersome and requires further streamlining. It is unworkable in practice that, despite the position of the Working Party 29 on BCR, some DPAs still refuse to authorise BCR or apply other limitations.[38] This is possible because the WP Opinions of the Working

---

[37] Another practical issue is that the board of management of the parent company of a large multinational may have a very strict policy as to which topics may be discussed at board level, and in which frequency. If a policy is submitted for approval and is approved, such policy may not be resubmitted for approval until the next round of the relevant topic is scheduled. These boards have so many topics to discuss and policies to adopt that repeated submission is not an option.

[38] At the moment, Estonia, Greece and Romania still refuse to recognise BCR at all. Portugal refuses to become part of the MRP as "it is unable to rely on a decision determining data

Party are not binding[39] and BCR are not recognised as an alternative tool for data transfers in the Data Protection Directive or any other form of binding EU regulation or decision. As a consequence the Member States have discretion whether to accept BCR as an adequate tool or not. Apparently the Working Party 29 has not been able to convince all DPAs of the usefulness of BCR as an alternative tool for data transfers (some DPAs still refuse to recognise BCR)[40] or of the advantages of joining the MRP (at present 19 out of 26 Member States have joined). Other unnecessary obstacles in the BCR approval procedure are the many additional national requirements imposed by the various Member States (i.e. which apply on top of the requirements set by the Working Party 29). These additional national requirements are very diverse (and sometimes even highly unusual) in nature.[41] No

---

protection adequacy by another EU DPA" and has further stated that "unilateral declarations are not valid for international data transfers". A contract, in the form of an intra-group agreement, would still be necessary between group companies to facilitate any international data transfers to third countries which do not meet European data protection adequacy standards. Such agreements must be notified to the Portuguese DPA (see Privacy Laws & Business Newsletter 2 December 2010, at 1 and 3). In Spain, only BCR for employee data is possible (and not for customer data). Another limitation is that certain Member States consider BCR to authorise specific existing transfers, but not future transfers.

39 See Chapter 6 n 29.

40 The Working Party 29 itself is also of the opinion that this approval procedure requires streamlining. See WP Opinion on the principle of accountability (Chapter 1, n 15), at para. 5, where in the context of BCR it is explicitly mentioned that "it is also relevant to discuss the mechanisms to streamline the current system based on authorisations of data transfers by national authorities." Also the Rand Report (Chapter 6, n 27) identifies one of the main weaknesses of the Data Protection Directive (see at 26 and 35) as being that "the length of time and effort to get [...] Binding Corporate Rules approved is excessive. Uneven practices of approval and authorisation; too little coordination between the Member States." It recommends (see Recommendation 2, at 43) that the use of alternatives to the adequacy rule (such as BCR), should be facilitated as a priority in any Member State. See also the ICC Report on BCR (Chapter 9, n 20), at 12; Wugmeister, Retzer, Rich (Chapter 7, n 61), at 481; and EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 8.4.

41 National requirements vary: France, Poland, Spain have local translation requirements; Austria, Lithuania and Spain require that on top of the MRC/CO procedure, an individual application with the relevant DPA is also required by the national legal entity, accompanied by all other legal entities in that country (if any) and powers of attorney to file applications also on their behalf; Hungary requires consent to be obtained from all data subjects; Belgium requires incorporation of the BCR in a Royal Decree signed by the King(!); Germany requires review of the BCR both by the Berlin DPA and the federal state where the main processing takes place, and other federal states (most notably Hamburg) require that, in addition to the BCR, EU Standard Contractual Clauses must be entered into for data transfers from that state (while the

comprehensive overview of such requirements is available for multinationals,[42] which in practice leads to much unnecessary delay in identifying and completing all national formalities. Though in practice the Working Party 29 has made efforts to put pressure on individual DPAs to eliminate such additional requirements, the Working Party 29 is not able to enforce this in any way.

10.6 How to address shortcomings in EU BCR approval procedure?

10.6.1 Recognise BCR and impose the Mutual Recognition Procedure

European legislators would be well advised to address the shortcomings of the BCR approval procedure in the upcoming revision of the Data Protection Directive by (i) recognising BCR in the revised Directive as an appropriate tool to provide adequate safeguards, including defining the main substantive requirements and (ii) defining and imposing the MRP on all Member States. This would fit in with Article 27 Data Protection Directive that encourages self- and co-regulatory approaches to data protection through codes of conduct. This is also the recommendation in the First Implementation Report of the Commission,[43] in line with the recommendations in the Rand Report,[44] the advice of the Working Party 29 itself in its WP Contribution on

---

wish to avoid entering into such model contracts was the reason why multinationals adopted BCR in the first place!). See further examples given in n 38. In April 2011, the Working Party 29 published a table with information on the national requirements of each DPA for the granting of authorisation of transfers on the basis of BCR, to be found at http://ec.europa.eu/justice/policies/privacy/docs/binding-rules/table_national_administrative_requirements_14_04_11_en.pdf.

42 The website of the Working Party 29 provides an overview of the national filing requirements for authorisation of transfers on the basis of BCR: http://ec.europa.eu/justice/policies/privacy/docs/binding-rules/table_national_administrative_requirements_14_04_11_en.pdf, but this overview is not complete and in many instances incorrect.

43 See First Report on the Data Protection Directive (n 26), at 18.

44 See Rand Report (Chapter 6, n 27), at 42, where it is recommended to "ensure that BCR can be more easily used to ensure the legitimacy of personal data transfers to third countries." This could be achieved by formalising the measures currently being developed by certain supervisory bodies, with associated guidance as to their common understanding, and should be designed so as to maximise common acceptability across Member States. Care should be taken to maintain incentives for the private sector. The current attempts to introduce a system of mutual recognition between Member States are partly successful but run into problems, notably because some of the national transpositions have not included a sufficient legal basis for

the Future of Privacy[45] and the EPCD in its Opinion on revision of the Directive,[46] which revision was launched by the European Commission on 1 July 2009. The Commission in its recent communication on the revised Directive of November 2010, announced that it will indeed "improve and streamline the current procedures for international data transfers, including (…) Binding Corporate Rules".[47]

When revising the MRP, EU legislators are well advised to take into account the fact that at present, the Lead DPAs lack the resources to process the current number of BCR applications. Though in absolute terms the number of BCR applications is very small, the BCR applications are concentrated within a very limited number of Lead DPAs,[48] and despite these limited numbers, there is currently a backlog of BCR applications.[49] If the uptake of BCR increases, staffing of BCR applications for such DPAs will become even

---

adopting such a system. Member States should be persuaded to amend their national personal data protection law accordingly to allow such systems to operate in practice."

45 See WP Contribution on The Future of Privacy (Chapter 6, n 33), at para. 38, where it recommends including a provision on BCR in the new legal framework to serve the following purposes:

- "Recognising BCR as [an] appropriate tool to provide adequate safeguards;
- Defining the main substantive and procedural elements of BCR, following the WP29 Opinions on the subject."

Noteworthy here is that the Working Party (apparently) is not even sure that BCR can indeed be a tool for the transfer of data to non-adequate countries under Article 26(2) Data Protection Directive. See WP Opinion on the principle of accountability (Chapter 1, n 15), para. 56.

46 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 127:

"The EDPS recommends addressing conditions for BCR in an explicit way in the new legal instrument, by:

- recognizing explicitly BCR as tools that provide adequate safeguards;
- providing for the main elements / conditions for the adoption of BCR;
- setting forth cooperation procedures for the adoption of BCR, including criteria for the selection of a leading supervisory authority (one stop shop)."

47 EC Communication on the revision of the Directive (Chapter 6, n 34), at 16.; Viviane Reding (Chapter 6, n 35), at 3-5.

48 The DPAs of the UK, Germany, France and the Netherlands.

49 This is based on my experience as a practitioner. The BCR applications are concentrated up until this point with 5 Lead DPAs (see n 25), where there is already a backlog of BCR applications has accrued. Those authorities are limited in expanding their resources. See also the Centre for Information Policy Leadership "A New Approach to International Transfers in Response to the European Commission's Communication on "A comprehensive approach to personal data protection," January 2011, to be found at <www.huntonfiles.com> (**Centre for Information Policy Leadership New Approach to International Transfers**), at 4.

more problematic, if not impossible.[50] A simple streamlining of the MRP will therefore not be sufficient. One solution is that DPAs could appoint third-party certifying agencies to certify BCR on their behalf.[51] A more radical solution recently suggested by the Centre for Information Policy Leadership is to have multinationals self-certify their BCR.[52] This recommendation is in line with the general empirical and theoretical public policy literature, which suggests that the long-term attention that "regulating self-regulating" requires is too costly and difficult to maintain if regulators do not "prompt organisations' rigorous self-evaluation and investment in the search for appropriate solutions to regulatory problems. "[53]

---

50 Centre for Information Policy Leadership New Approach to International Transfers (n 49) at 4: "A 2003 Yale study conservatively estimates that there are some 63.000 multinational corporations, with 821,000 subsidiaries. They directly employ 90 million people and produce 25 per cent of the world's gross product. It can be asserted with confidence that every single multinational corporation now transfers personal data internationally. Beyond that, there are countless SMEs and other organisations which are not multinationals, but which are nevertheless involved daily in international transfers of personal data, often of highly sensitive nature. In short, it is inconceivable that the BCR approach – without improvement – could meet the potential underlying demand."

51 This in line with the intention of the Commission to explore the creation of EU certification schemes for privacy compliant products and services. See EC Communication on revision of the Directive (Chapter 6, n 34), para. 2.2.5 at 12. The EDPS supports this and suggests including a provision in the revised Directive "providing for their creation and possible effect across the EU." See EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 7.4. See on the possibility of introducing certification schemes also WP Contribution on the Future of Privacy (Chapter 6, n 33), at para. 58 at 15; The Stockholm Program (Chapter 8, n 13), at para 3.5 at 11; and the Rand Report (Chapter 6, n 27), at 53, also lists certification as one of the possible tools to implement data protection principles: "Standards provide additional support for accountability, by permitting a regular review of whether those that have agreed to abide by certain rules do so. This is only possible, however, if organisations become compliant (i.e. get certified) against a standard, rather than merely implementing the best practice."

52 The Centre for Information Policy Leadership New Approach to International Transfers on (n 49), at 7: "Organisations would self-certify their own Code without the need for prior DPA approval, which is simply not practicable with the scale of the challenge" and "if self-certification is considered too radical, there are other options for the initial adoption or approval of a Binding Global Code to ensure that minimum requirements are in fact met. These include certification by an independent Third Party (Accountability Agent) appointed by a DPA at the expense of the business or certification by a Third Party approved by the DPA". The suggestion of self-certification or, if this is not acceptable, certification by a DPA, has also been suggested by Wugmeister, Retzer, Rich (Chapter 7, n 61), at 485.

53 Sharon Gilad, It runs in the family: meta-regulation and its siblings, Regulation & Governance (2010) 4, at 502.

10.6.2 Adequate level of protection

When setting the main substantive requirements for BCR, European legislators should also provide that the BCR should ensure an adequate level of protection (only) rather than a level equivalent to that of the Data Protection Directive. The Rand Report[54] rightly observes that the present: "pass-porting of the BCR is regarded as counter productive, since the regulators review them more stringently than SCCs [Standard Contractual Clauses] because, if approved, they will be valid in several countries." This has also been the experience of multinationals in the BCR approval procedures. Also, more generally, the experience is that whenever self-regulation is attempted and submitted for review to DPAs, this leads to an "enhancement rather than a substitute means of making data protection legislative requirements more effective and legitimate".[55] The criteria for review of BCR became yet even stricter the moment the DPAs agreed on the MRP, when instead of review by the Lead DPA the two Co-Leads were added to the review process.[56] By insisting on an equivalent level of protection and sometimes even superseding protection,[57] rather than an adequate level, the baby is thrown out with the bathwater. Multinationals, when applying for BCR, experience this as being punished rather than being encouraged to embark on a BCR implementation and authorisation project, which may be an explanation for the current low uptake of BCR.[58] This seems a disadvantage to all concerned, including the EU citizens the Working Party 29 and DPAs try so hard to protect. In this borderless world only global solutions will truly result in an increase in compliance and privacy

54 Rand Report (Chapter 6, n 27), at para. 3.3.4.

55 See in respect of privacy policies in the area of electronic communications, where the conclusion was that the low uptake was possibly due to a perception that they are an "enhancement rather than a substitute means of making data protection legislative requirements more effective and legitimate." See reference in the Rand Report (Chapter 6, n 27), at 10 to the Report of WIK-Consult and Rand Europe: Comparison of Privacy and Trust policies in the Area of Electronic Communications – Final Report, European Commission 2007, at 10, to be found at <www.ec.europa.eu>.

56 This is based on my experience assisting multinationals in their BCR applications.

57 In footnotes 21 and 22 some examples are given of where the DPAs have been trying to obtain rights and remedies or additional protection for data subjects via BCR that DPAs and data subjects do not have under their national laws. This may seem a good result in the short term, but is counterproductive in the long.

58 See n 55.

protection for everyone concerned.[59] If European legislators wish to increase the current low uptake of BCR, it is therefore advised to set the requirement for BCR at an adequate level, rather than accumulating all national requirements.[60] It seems that the European Commission is aware of the fact that at present it is insufficiently clear what the required level for protection is when data are transferred outside of the EU. In its EC Communication on the revision of the Directive, it announced that it will examine how to improve the current data transfer regime by examining how "to clarify the Commission's adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organisation" as well as "to define core EU data protection elements, which could be used for all types of international agreements".[61]

10.6.3 Harmonise the powers of DPAs

It is in any event advisable to harmonise the enforcement powers of the DPAs at the right level. At present certain DPAs lack certain enforcement rights which they try to obtain via the BCR regime.[62] If the enforcement regime were properly harmonised at the right level, this would no longer be necessary. As equal enforcement powers do not also guarantee a harmonised enforcement strategy, I further recommend developing a common enforcement strategy for the Lead DPAs to ensure a common approach. These recommendations in respect of enforcement are in line with the recommendations of the Rand Report, the Working Party 29, the EDPS and the Commission itself.[63]

---

59 Wugmeister, Retzer, Rich (Chapter 7, n 61), at 497: "Once a practical global solution is developed, compliance will increase, thus increasing privacy protection for everyone concerned, and greater economic benefits will flow to the countries that permit businesses to utilize a global solution for their cross-border data transfers."

60 The Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 3 states: "Harmonisation must be based on common principles and objectives, avoiding both highest and lowest common denominators. Harmonising regulatory approaches, including robust education programmes, is as important as the substance of the law itself."

61 EC Communication on the revision of the Directive (Chapter 6, n 34), at 16.

62 See examples in footnotes 21 and 22.

63 See the Rand Report (Chapter 6, n 27), at x and xiv and 57 - 58. See in particular at 44: **"Recommendation 4: Develop common enforcement strategies**. The London Initiative of DPAs should develop a common enforcement strategy for independent supervisory authorities, crystallised in an instrument such as a non-binding Memorandum of Understanding. This should be published and endorsed by the EDPS so that the standards used to judge the regulated are clear. This strategy should take into account legal and cultural

10.6.4 Define BCR requirements in general principles

The recommendation that the revised Directive should "define the main substantive requirements" for BCR, does not imply that these should be defined in detail. In order for the revised Directive to remain "future proof", the norm-setting in the revised Directive should be in general terms only: e.g. the BCR should provide for an adequate level of protection, should provide for internal complaints procedures etc. Detailed norm-setting can and should be delegated to the European Commission in accordance with recently introduced Article 290 TFEU[64], in order to ensure that the relevant norms remain more adaptable to changing circumstances and insights.[65]

---

traditions and contexts across the Member States and use these differences to its advantage." See also the WP Contribution on the Future of Privacy (Chapter 6, n 33), at para. 7 at 22, where the Working Party 29 advises the Commission to strengthen and clarify the roles of DPAs and their cooperation within the EU. The Commission announced in its Communication on the revision of the Directive (Chapter 6, n 34), at para 2.5 to examine how to "strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities and ways to improve the cooperation and coordination between DPAs." This is also the opinion of the EDPS, EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at paras. 59 and 140. See further the Declaration of Civil Society Organisations, adopted on 25 September in Montreal, stating that "stronger and more aggressive action by privacy commissioners is required," finding them uniquely positioned to defend our society's core values and rights of privacy, to be found at <http://www.privacyconference2007.gc.ca/Terra_Incognita_resolutions_ngo_E.html>

64 Article 290 TFEU introduces the following delegation mechanism:
"1. A legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act. The objectives, content, scope and duration of the delegation of the power shall be explicitly defined in the legislative act. The essential elements of an area shall be reserved for the legislative act and accordingly shall not be the subject of a delegation power.
2. Legislative act shall explicitly lay down the conditions to which the delegation is subject; these conditions may be as follows:
(a) the European Parliament or the Council may decide to revoke the delegation;
(b) the delegated act may enter into force only if no objection has been expressed by the European Parliament or the Council within a period set by the legislative act.
For the purposes of (a) and (b), the European Parliament shall act by a majority of its component members, and the Council by a qualified majority.
3. The adjective 'delegated' shall be inserted in the title of delegated acts."

65 The EDPS in its Opinion on the revision of the Directive (Chapter 6, n 35), at paras. 106 and 114, recommends to delegate specific tasks to the European Commission in order to supplement the basic criteria on for instance accountability, privacy by design etc.

This is not a new insight, but has also been the trend in other areas of law, like company and financial markets law.[66] In the words of the High Level Group of Company Law Experts in its 2002 Report on a Modern Regulatory Framework for Company Law in Europe[67]:

> "We noted that the system of harmonising company law through Directives – that have to be implemented by Member states – may have led to a certain "petrifaction". Once Member States have agreed to an approach in an area of company law and have implemented a Directive accordingly, it becomes very hard to change the Directive and the underlying approach. Simultaneously however, there is a growing need to continuously adapt existing rules in view of rapidly changing circumstances and views. The "shelf life" of law tends to become more limited as society changes more rapidly, and company law is no exception. Fixed rules in primary legislation may offer the benefits of certainty, democratic legitimacy and usually strong possibilities of enforcement. But this comes at a cost of little or no flexibility, and disability of keeping pace with changing circumstances. EU Directives are in practice even more inflexible than primary legislation. We can see a movement in Member States to use alternatives for primary legislation by government and parliament, which allow for greater flexibility. Such alternatives include:
>
> - Secondary regulation by the government, based on primary legislation in which broad objectives and principles are laid down; the secondary regulation can be amended more quickly when circumstances require change. (This process also often enables more effective consultation and reflection of an expert consensus)."

10.6.5 Replace Directive by an EU regulation

Given the fact that many of the obstacles in the MRP and CP are caused by differences between the various national implementation laws in the Member States[68] and differences in enforcement powers of the DPAs, I recommend that, rather than trying to ensure a proper implementation of the Data Protection Directive and further harmonise certain requirements,

---

66 A striking example of the trend to move from detailed rules to principle-based standards is the switch by the SEC from the highly detailed US accounting standards (GAAP) to the principle-based IFRS, see in more detail Chapter 221, n 33.

67 The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe, Brussels, 4 November 2002 (Chapter 8, n 30), at para. 2.

68 It is generally acknowledged that the main shortcoming of the Data Protection Directive is that the level of harmonisation under the current framework is unsatisfactory, see further n 65.

European legislators choose the form of an EU regulation[69] as a legislative instrument rather than an EU directive to regulate data protection. This is also the recommendation of the EDPS.[70] As EU regulations are directly applicable in all Member States, and do not require further implementation in national legislation (which always leads to variations in the implementation provisions), uniformity between the laws of the Member States will be ensured to a much greater extent.[71] Also if the form of an EU regulation is chosen, I recommend that detailed norm-setting can and should be delegated to the European Commission in accordance with recently introduced Article 290 TFEU.[72] Alternatively, if the form of a regulation is not achievable, EU legislators are advised to confer the implementing powers in respect of the revised Directive on the European Commission, as it is authorised to do so pursuant to the new Article 291(2) TFEU since in this case "uniform conditions for implementing legally

---

69 Article 288 TFEU defines a regulation as follows: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States." Whereas "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."

70 EDPS Opinion on the revision of the Directive (Chapter 6, n 35) at para. 5.5: "A Regulation would reduce room for contradictory interpretations and for unjustified differences in the implementation and the application of the law. It would also reduce the importance of determining the law applicable to processing operations within the EU, which is one of the most controversial aspects of the present system." See further at para. 125.

71 The European legislator is free to choose the relevant legislative instrument when implementing the right to data protection under Article 16 TFEU. The TFEU prescribes in a number of cases whether the European legislator should act by means of a regulation or directive. However, in numerous other cases, including in respect of the implementation of Article 16 TFEU, the relevant article does not specify a particular kind of secondary law to be used, but uses a neutral wording such as "rules," "measures" etc. In those cases the European legislator is free to choose the appropriate Community instrument (i.e. directive, regulation or decision), provided the principle of proportionality is observed. See Article 296 TFEU: "Where the Treaties do not specify the type of act to be adopted, the institutions shall select it on a case-by-case basis, in compliance with the applicable procedures and with the principle of proportionality." See also: Bruno de Witte, "Legal Instruments and Law-Making in the Lisbon Treaty," in Stefan Griller, Jacques Ziller eds., *The Lisbon Treaty: EU Constitutionalism without a Constitutional Treaty?* (Springer 2008), at 96 and 97; Jacques Ziller, "Constitutional Boundaries of Self-Regulation," in Fabrizio Cafaggi (ed.), *Reframing Self-Regulation in European Private Law* (Kluwer Law International 2006), at 157. Kuner (n 60), at 44, points out that "so far no data protection instruments of direct relevance to business have been implemented by way of regulation, but this may change in the future."

72 See n 64.

binding EU acts are needed".[73] This conferring of implementing powers to the European Commission is in addition to the delegation in the revised Directive of detailed norm-setting to the European Commission as recommended in Paragraph 10.6.4.

10.6.6 Role of the Working Party 29

As European legislators (with possible delegation to the Commission) will not be able to specify all BCR requirements in full detail, the Working Party 29 will continue to play an important role in **providing guidelines** in respect of these requirements. The (informal or de facto) delegation of norm-setting in respect of BCR to the Working Party 29 (as has been the case to date) seems contrary to the new rules on delegation, which are limited to delegation to the European Commission only.[74] The Working Party 29 seems to realise this where it, rather than suggesting that its opinions become binding, suggests that the European Commission insists "on a strong commitment by the members of the Working Party 29 to implement the views of the Working Party 29 into national practice".[75] Also, the EDPS proposes to "make the opinions more authoritative" by including an obligation for the DPAs and the Commission "to take utmost account of opinions".[76] The EDPS puts a caveat against introducing stronger measures,

---

73 Pursuant to 291(1) TFEU, the Member States have to "adopt all measures of national law necessary to implement legally binding Union acts." Article 291(2) provides that the legally binding Union acts may "confer implementing powers on the Commission" (and in specific cases on the Council), "where uniform conditions for implementing legally binding Union acts are needed", provided the provisions of 29193) are observed. See Wim J.M. Voermans, "Is the European Legislator after Lisbon a Real Legislature?" (December 15, 2009), Legislacao Cadernos de Ciencia de Legislacao, No. 50, pp. 391-413, December 2009, available at SSRN: http://ssrn.com/abstract=1347959, at 11, observes that based on Article 291 TFEU, "the Commission or the Council will be able to draft implementing regulations (…) as well, even though this requires the express conferral of a competence for this purpose in the basic instrument (the legislative act). (…) Conferring an implementing power of a general nature constitutes a delegation within the meaning of Article 290 of the TFEU as well." See further n 73 on the delegation under Article 291(1) TFEU.

74 For a further delegation mechanism in respect of implementation powers of a Directive, n 73.

75 WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 99. See also Wugmeister, Retzer and Rich (Chapter 7, n 61), at 492.

76 EDPS opinion on the revision of the Directive (Chapter 6, n 35), at 146: "The EDPS recommends solutions which would make opinions of the Working Party more authoritative without modifying substantially its way of functioning. The EDPS suggests including an obligation for the DPAs and the Commission to take utmost account of opinions and common positions adopted by the Working Party, based on the model adopted for the positions of the Body of

such as giving binding force to Working Party 29 positions, as this "would have consequences as for instance transparency and redress requirements".[77] Given the fact that (as is now also already the case) the intention of both the Working Party 29 and the EDPS is that the opinions will be more than just guidelines, but policy rules *de facto* setting norms for DPAs and controllers, the question is whether "legitimacy" requirements like transparency and redress should not already also apply to such *de facto* norm-setting. This issue is discussed in Chapter 14, in particular Paragraph 14.7.3.

As to the enforcement function of the Working Party 29, the Working Party 29 at present coordinates and facilitates cross-border enforcement actions, but has no enforcement powers itself. It may be clear that increasingly more cases require coordination of enforcement on a cross-border basis. Illustrative examples are the fact that at present the Working Party 29 already fills a coordinating role in respect of enforcement of the national data protection laws of the Member States against a number of (inherently cross-border) ad network providers, browser providers, search engine operators, and social networking site providers.[78] The EDPS signals the fact that such coordination on an EU-wide basis will be indicated more and more, but does not propose to solve this by granting the Working Party 29 decision-making and enforcement powers in such cross-border cases[79] (as

---

European Regulators for Electronic Communications (BEREC). Furthermore, the new legal instrument could give the Working Party the explicit task to adopt "interpretative recommendations". These alternative solutions would give the positions of the Working Party a stronger role, also before the Courts. For the position of the BEREC: Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L337, 9 18.12.200, p. 1.

77 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 151: "The EDPS would put a caveat against introducing stronger measures, such as giving binding force to WP 29 positions. This would undermine the independent status of individual DPAs, which has to be guaranteed by the Member States under national law. Would the Working Party decisions have a direct impact on third parties such as data controllers, new procedures should be foreseen including safeguards such as transparency and redress, including possibly appeal before the European Court of Justice."

78 All dating from 2010 and to be found at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm.

79 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 148 -149: "Some cases have a strategic dimension which should be addressed in a centralised way. The Article 29 Working Party facilitates coordination and enforcement actions between DPAs in major data protection issues with such international implications. This was the case with social networks

the EDPS itself has in respect of data protection compliance of the EU institutions[80]). Given the fact that as to data protection cross-border violations will increasingly be the rule rather than the exception, coordination of enforcement will become indispensable. From this perspective, it is worth considering whether in case of data protection violations with EU-wide implications, central enforcement should be considered by creating a pan-European DPA that will take over some of the powers and responsibilities of the national DPAs, similar to that which is presently agreed in respect of the supervision of the European financial markets.[81] It is clear that based on existing case law[82] and literature[83] many

---

and search engines, as well as with regard to coordinated inspections conducted in different Member States on telecommunication and health insurance issues. There are however limits to the enforcement actions that the Working Party can undertake under the present framework. Common positions can be taken by the Working Party, but there is no instrument to ensure that these positions are effectively implemented in practice."

80 The EDPS itself, alongside its advisory functions, possesses extensive enforcement powers. According to the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, the EDPS is given powers to "monitor and ensure" respect of data protection principles by the European bodies and institutions (Article 46(c)); keep a register of processing operations (Article 46 (i)); execute prior checks of the notified processing (Article 46(i)); order the institutions' compliance with the requests to exercise data subjects' rights (Article 47(1)(c)); warn or admonish the controller (Article 47(1)(d)); ban processing (Article 47(1)(f)); refer the matter to the ECJ (Article 47(1)(h)) and intervene in the ongoing ECJ proceedings (Article 47(1)(j)). Article 47(2) gives the EDPS the right to access all information necessary to fulfil its duties and, with reasonable grounds, access to a premises.

81 On 22 September 2010, the European Parliament voted for a new supervisory framework for financial regulations that came into force in January 2011. Part of this new framework will be the replacement of the existing financial committees with advisory powers only, by three pan-European Supervisory Authorities to which certain national powers are transferred. For an overview of the reforms, see <www.ec.europa.eu> under 'financial supervision.'

82 This case law still dates from the 1950s when the ECJ first considered the question of legality of delegation to an agency in the *Meroni* cases: Case 9/56, *Meroni & Co. Industrie Metallurgiche SpA v High Authority* [1958] ECR 133 and Case 10/56 *Meroni & Co., Industrie Metallurgiche, S.A.S., v High Authority of the European Coal and Steel Community* [1958] ECR. The cases are based on similar facts, decisions were rendered on the same day and the conclusions and reasoning of the ECJ largely coincide. On the facts of the cases, Meroni filed for annulment of a decision of the High Authority of the European Community of Coal and Steel (ECSC) ordering Meroni to pay a sum of money to the Imported Ferrous Scrap Equalization Fund. The Fund was a voluntary body of large steel companies that received authorisation of the High Authority of ECSC to exercise powers on the common ferrous scrap market. The ECJ found the decision of

questions can be posed as to the legal basis for such delegation of powers to an EU supervisory authority. Indeed, the position of EU and national independent regulatory authorities has been subject to academic and

---

the High Authority regarding Meroni null and void. To achieve this conclusion the ECJ, among others, had to examine if the authorisation of the High Authority constituted delegation of powers and if such delegation was lawful. The ECJ found that delegation took place, and that such a delegation constituted a violation of the EC Treaty. However, the Court did not rule out delegation completely. The Meroni test (Case 9/56 at 151-52) is the following:

- In general, an EU institution cannot delegate more or broader powers than it has itself under the Treaty;
- Within the scope of the institution's own powers, only clearly defined executive powers may be delegated to another body, whereas, discretionary powers implying a wide margin of discretion which may make possible the execution of actual economic policy, cannot be delegated;
- The delegated powers are subject to the same conditions to which the EU institutions would have been subject if they had exercised them directly, such as the obligation to state reasons, publish annual reports, and judicial control;
- The powers delegated remain subject to conditions determined by the delegating EU institution and subject to its continuing supervision; and
- The institutional balance between the EC institutions must not be distorted.

83 On the issues relating to the legal basis for the delegation of supervisory and enforcement powers to European Supervisory Authorities, see Luc Verhey and Tom Zwart, (2003) "Agencies in European and Comparative Perspective," (Intersentia: Antwerp-Oxford-New York); Ronald van Ooik, (2005) "The Growing Importance of Agencies in the EU: Shifting Governance and the Institutional Balance" in *Good governance and the European Union: Reflections on Concepts, Institutions and Substance,* (Intersentia: Antwerp – Oxford – New York), at 151-52). Verhey and Zwart at 130 and Ooik at 151-152, offer an alternative reading of the *Meroni* doctrine, which justifies the creation of the EU agencies with powers broader than pure managerial or technical tasks, provided that the institutional balance is respected. Van Ooik at 152, continues that as the balance "emerged from the E(E)C Treaty itself, [t]reaty legislator itself [...] may change the institutional balance [...] by giving an explicit and clear Treaty basis to a certain body". Alternatively, creation of effective system of supervision and control "may mitigate objections against a far-reaching delegation of powers to independent agencies". See further H. van Meerten and A. Ottow, "The proposals for the European Supervisory Authorities: the right (legal) way forward?", Tijdschrift voor Financieel Recht, Vol. 1, 2010. Available at SSRN: http://ssrn.com/abstract=1517371. Van Meerten and Ottow observe at 37, that acting under Article 291 TFEU, Member States may, by adopting a legislative act, delegate implementation to a European agency. On this, they say that "delegating decision making power from one competent national authority to another is already recognized and embedded in EU law. If this is possible, Member States can via primary and secondary EU law certainly delegate these powers to an agency. And to be perfectly clear: ultimately only the Court can determine a breach of EU law."

political debate in the Member States ever since their existence.[84] This being said, in its 2001 White Paper on European Governance, the European Commission noted that there were already 12 EU agencies and communicated its intent to create more pan-European regulatory agencies and listed the conditions on which it considers this possible.[85] These conditions are clearly inspired by the requirements for delegation set by the ECJ in the *Meroni* cases.[86] The European Commission subsequently issued an operating framework for such EU agencies[87] and in 2010 communicated its substantiation of the legal basis for setting up the new EU financial supervisory authorities and the powers of the latter to take legally binding decisions.[88] Whether the views of the European Commission are indeed in

---

84 Annetje Ottow and Saskia Lavrijssen, 'The legality of independent regulatory authorities', in: L. Besselink, F. Pennings & A. Prechal (eds), The Eclipse of Legality, Kluwer Law International, 2010, Chapter 5, at 73, and especially the literature listed in footnote 1.

85 White Paper on European Governance (Chapter 6, n 72), at 24: "The creation of further autonomous EU regulatory agencies in clearly defined areas will improve the way rules are applied and enforced across the Union. Such agencies should be granted the power to take individual decisions in application of regulatory measures. They should operate with a degree of independence and within a clear framework established by the legislature. The regulation creating each agency should set out the limits of their activities and powers, their responsibilities and requirements for openness." The Commission further set the following conditions for the creation of regulatory agencies at EU level: " The Treaties allow some responsibilities to be granted directly to agencies. This should be done in a way that respects the balance of powers between the Institutions and does not impinge on their respective roles and powers. This implies the following conditions:

- Agencies can be granted the power to take individual decisions in specific areas but cannot adopt general regulatory measures. In particular, they can be granted decision making power in areas where a single public interest predominates and the tasks to be carried out require particular technical expertise (e.g. air safety).
- Agencies cannot be given responsibilities for which the Treaty has conferred a direct power of decision on the Commission (for example, in the area of competition policy).
- Agencies cannot be granted decision-making power in areas in which they would have to arbitrate between conflicting public interests, exercise political discretion or carry out complex economic assessments.
- Agencies must be subject to an effective system of supervision and control".

86 See n 82.

87 Commission Communication, "The operating framework for the European Regulatory Agencies", COM (2002) 718.

88 On 11 November 2009, the Second chamber of the Dutch Parliament sent a request to the European Commission as to the proposals of the European Commission for Regulations concerning the reinforcement of the Financial Supervision in the EU - COM(2009)499, COM(2009)501, COM(2009)502, and COM(2009)503, requiring the Commission to further

conformity with the requirements of the TFEU is ultimately the decision of the ECJ. However, based on the position of the European Commission, it seems possible to also establish an EU supervisory authority for data protection to which certain decision and enforcement powers are delegated. I note that granting such central enforcement powers to the Working Party 29 would have as a consequence that the Working Party 29 would have to combine its advisory tasks with enforcement, which is generally considered to be a difficult combination (the first task interfering with the required freedom to execute the second) and further contrary to concepts of "separation of powers", as it involves a mixing of norm-setting and adjudicative tasks.[89] In any event this requires further research which is

---

substantiate the relation between the legal basis for setting up the new European Supervisory Authorities (ESAs) and the powers of the latter to take legally binding decisions. The European Commission in its reply dated 5 February 2010, to be found at http://www.ipex.eu/ipex/webdav/site/myjahiasite/users/stafEU/public/financieel%20toezicht%20europese%20commissie.pdf, gives the following justification: "Regarding the first issue, the Court of Justice has acknowledged [See CJCE, C-217/04, pt. 44] that Article 95 of the Treaty relating to the adoption of measures for the approximation of legislation for the establishment and functioning of the internal market provides an appropriate legal basis for setting up a "Community body responsible for contributing to the implementation of a process of harmonisation", when the tasks conferred on such a body are closely related to the subject matter of the acts approximating the national legislations. The purpose and tasks of the ESAs - assisting competent national supervisory authorities in the consistent interpretation and application of Community rules and contributing to financial stability necessary for financial integration - are closely linked to the objectives of the Community acquis concerning the internal market for financial services. It was therefore decided to establish the ESAs on the basis of Article 95 of the Treaty. Concerning the powers of the proposed ESAs, it should be stressed that while Article 95 of the Treaty is clear about the objective of such Community bodies, it does not specify their precise powers. However, case law has recognised the possibility for Community institutions to delegate binding powers to these bodies, in so far as the delegation relates only to clearly defined executive competences, meaning that the delegated powers cannot consist of "a discretionary power implying a wide margin of discretion which may, according to the use which is made of it, make possible the execution of actual economic policy". Moreover, the delegating authority cannot grant to the ESAs more powers than those that it holds from the Treaty. This entails that it is possible for a legislative measure to grant to an agency an independent power to adopt binding decisions, provided that such a power is contained within a precise legal framework and is limited in its scope. Moreover, the power entrusted to such Community bodies should be limited to executive tasks, and must therefore be confined to the adoption of individual decisions."

89 This cristisism is also voiced in respect of the present combination of tasks of some DPAs. See for instance the study into the competences of the Dutch DPA conducted by the Comission Brouwer-Korf (2009) Gewoon Doen. Beschermen van veiligheid en persoonlijke levenssfeer,

outside the scope of this dissertation. It will suffice here by my recommending to European legislators that they investigate whether (and to what extent) it is indicated to establish a pan-European DPA to which certain decision-making and enforcement powers are delegated in case of data protection violations with an EU dimension.

In summary, the above leads to the following recommendations to the European legislator:

Recommendation 2
Recognise the BCR as an appropriate tool to provide adequate safeguards for the transfer of data and define the main substantive requirements for BCRs:
- to be defined in general principles
- to be set at an adequate level.
and to delegate the further norm-setting to the European Commission pursuant to Article 290(1) TFEU.

Recommendation 3
Define the MRP and impose the MRP on all Member States.

Recommendation 4
Investigate whether it is indicated to establish a pan-European Data Protection Supervisory Authority, to which certain decision-making and enforcement powers are delegated in case of data protection violations with an EU dimension.

Rapport aan de ministers van justitie en Binnenlandse zaken, Den Haag, at para. 3.7, at 63-64, to be found at http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/01/22/rapport-gewoon-doen-beschermen-van-veiligheid-en-persoonlijke-levenssfeer.html. The Commission concluded that the mixture of the various roles of the Dutch DPA and in particular the combination of on the one hand advising organisations on data protection compliance and approving self-regulatory codes and on the other hand enforcement thereof is inappropriate, as the first role limits the freedom of the DPA in its enforcement role. Further the Commission notes that it is strange that organsiations have to address the same authority for advice while this authority can subsequently use such information to enforce. See further J.E.J. Prins, *Burgers en Hun Privacy: Over Verhouding En Houding Tot Een Ongemakkelijk Bezit*, (NJCM 2010), at 11. ; and the Report *i-Overheid* of the Wetenschappelijk Raad vooor het Regeringsbeleid, at para. 7.1.2, at 174-175, to be found at http://www.binnenlandsbestuur.nl/Uploads/Files/Document/Ioverheid.pdf.

Recommendation 5
Provide for equal enforcement powers for DPAs and develop a common enforcement strategy for the DPAs to ensure equal enforcement.

Recommendation 6
Replace the Data Protection Directive by an EU regulation when revising the Directive, or, as the next best alternative, to confer implementing powers in respect of the revised Directive on the Commission pursuant to Article 291(1) TFEU.

10.7 Recognition of BCR in other countries

A substantial number of non-EU countries have data transfer restrictions (see Paragraph 7.2). For multinationals to also comply with the data transfer rules from those countries, it is crucial that these countries recognise BCR as a tool to facilitate data transfers from their countries. At the moment, the EEA countries and Switzerland acknowledge BCR as a tool for data transfers (Norway is even already part of the MRP).[90] Further, the Additional Protocol to Convention 108[91] provides for data transfer rules similar to the Data Protection Directive and should also be able to facilitate BCR. The Additional Protocol to Convention 108 has been ratified or acceded to by 30 countries of which a number are non-EEA countries,[92] and which countries therefore (should be able to) recognise BCR. The APEC Privacy Framework intends to facilitate a similar organisational tool, where it provides that member economies shall endeavour to facilitate that organisations adopt "Cross Border Privacy Rules" (**CBPR**) as a manner to facilitate their cross-border data transfers.[93] In countries that have introduced the accountability

[90] In Switzerland BCR are recognised as an appropriate tool pursuant to para. 6(2) of the Swiss Data Protection Act. BCR have to be notified to the federal DPA and are then valid without any further review.

[91] See Chapter 6, n 48.

[92] Albania, Andorra, Bosnia and Herzegovina, Croatia, the former Yugoslav Republic of Macedonia, Monaco, Montenegro, Serbia, Switzerland and Ukraine. This is the state as per January 2011, to see the statistics of ratification of or accession to the Additional Protocol visit http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=3&DF=14/01/2011&CL=ENG.

[93] The APEC member economies have explicitly agreed:

- "To endeavour to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data

approach (also for) data transfers, e.g. Canada and Japan, organisational measures like introducing CBPR are already a requirement (see Paragraphs 7.4 above and 13.6 below). For these countries, recognition of BCR may be more or less assumed. This will also apply if the proposed Australian Privacy Principles become law.[94] In the US there are also proposals to introduce a co-regulatory approach for regulating privacy in the US, which is very similar to the BCR regime, where companies create a privacy safe harbor and enjoy considerable scope in shaping self-regulatory guidelines, while government retains general oversight authority to approve and enforce these guidelines.[95] All in all, given the fact that the EU has a high level of data protection, the expectation is justified that if BCR are recognised by the EU as providing an adequate level of protection for data transfers, BCR will also be recognised by other countries. A pre-condition for this is that countries do recognise self-regulatory tools rather than public regulation or contractual tools as an instrument to regulate transborder transfers. Again, the expectation is that in most countries this will not pose problems or if this does pose problems, countries are willing to address these. Already in 1985, the OECD published the Declaration on Transborder Data Flows,[96] in which the OECD expressed the intention to "develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonised solutions". Also the Madrid draft proposal for an International Standard provides that data transfers may be carried out if

---

protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

- To give effect to such cross-border privacy rules, Member Economies will endeavour to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.
- To endeavour to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers."

See APEC Privacy Framework (Chapter 6, n 36), Part B, Section III, Cooperative Development of Cross-border Privacy Rules, Principles 46 - 48. See also the Centre for Information Policy Leadership New Proposal to International Transfers, n 49, at 8: "The BGC approach has the potential to align with equivalent provisions in the APEC Privacy Framework to achieve a genuinely global solution, but perhaps with the robust substance which would flow from European leadership."

94 See on the Australian Privacy Principles (Chapter 6, n 52).

95 Rubinstein (Chapter 7, n 67), at 47.

96 11 April 1985. Available at <www.oecd.org>

tools like BCR are implemented.[97] From the above is clear, however ,that in respect of recognition of BCR as a tool for outbound data transfers from non-EU countries, a lot of "work" still has to be done. It is recommended that this work be undertaken by the European Commission, rather than it being left to individual companies to obtain recognition of their individual BCRs in such countries. The optimal solution would obviously be that these countries not only recognise BCR as a tool for data transfers also from their country, but that the European Commission also comes to an agreement for mutual recognition of BCR and central enforcement.[98] By central enforcement I mean that all supervisory authorities involved in supervision of a certain multinational group of companies accept that in respect of the BCR of such company one Lead DPA (and the courts of such Lead DPA) have central supervision and enforcement powers. The Lead DPA should preferably be the DPA of the country of establishment of the headquarters of the multinational, to ensure such company can indeed effectuate compliance throughout its group of companies. In any event, EU legislators should improve the cross-border cooperation both between the DPAs and with DPAs outside the EU, in the enforcement of data protection laws.[99]

Recommendation 7
Engage with non-EU countries in mutual recognition and enforcement of BCR as a tool for cross-border data transfers.

10.8 Conclusion

In this chapter I evaluated the BCR regime, including the MRP, and my conclusion is that already based on an evaluation of the regime itself, without evaluation from other disciplines, a number of improvements are

97 Madrid draft proposal for an International Standard (Chapter 8, n 14), at para. 15(2).

98 See for more or less similar recommendations: Wugmeister, Retzer, Rich (Chapter 7, n 61), at 494; the Rand Report (Chapter 6, n 27), at 57; and the Centre for Information Policy Leadership New Proposal to International Transfers, n 49, at 7.

99 A good basis therefore seems to be the OECD 2007 Recommendation on Cross Border Co-operation in the Enforcement of Laws Protecting Privacy, to be found at <www.oecd.org>. See para. 8.3, especially n 55. See further The Stockholm Program (Chapter 8, n 13), p. 1-38, at para. 2.5 at 10: "The Union must secure a comprehensive strategy to protect data within the Union and in its relations with other countries." See also the EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 166 and 185; and the Communication on the revision of the Directive (n 34), at para 2.4.2 at 17.

possible to address the shortcomings of the regime. In the following chapters I will evaluate the BCR regime from different disciplines, starting with general principles of contract law, to evaluate whether this should lead to further recommendations.

11 BCR and contract law

11.1 Introduction

In the introduction to this dissertation, I indicated that the emergence of BCR is part of a wider trend where legislators who wish to regulate global corporate conduct opt for "regulating" transnational private regulation (**TPR**) rather than introducing public regulation with its inherent jurisdictional limitations. There is by now a vast body of research concerning the concept of TPR.[1] As also indicated in the introduction to this dissertation, the main questions raised in this research in respect of TPR,[2] and which are of equal relevance to BCR, are the following:

- TPR raises questions of private international law (**PIL**) as to the validity of a choice of law and forum in BCR;
- the suitability of TPR for regulating human rights;
- how to best regulate TPR, i.e which of the different forms of regulation would be most suitable to regulate TPR;
- the legitimacy of TPR as compared to public regulation;
- the alignment of TPR with conventional principles of contract law (TPR raises questions of enforceability by the third-party beneficiaries of such TPR);
- the enforceability of contractual "supply chain management" as a mechanism to effectuate TPR, which solution is also part of the BCR regime.

I will discuss the questions above in the following chapters. In this chapter I will start with the contractual issues (the questions of enforceability by third-party beneficiaries and supply chain management issues) as these are of prime relevance to the BCR regime. The first requirement set by the Working Party 29 in respect of BCR is that the BCR should be "internally binding" within the organisation (on all group companies and on employees) and "externally binding" for the benefit of individuals (i.e. must create third-party beneficiary rights for the individuals).

The questions under PIL are subsequently discussed in Chapter 12. An evaluation of BCR as a form of TPR is given in Chapter 13.

---

[1] For an inventory of prior research, see the 'Survey of Research Programmes', Annex 2 to "The added value of private regulation in an international world? Towards a model of the legitimacy, effectiveness, enforcement and quality of private regulation" HiiL 2007 – 2008, at 1 – 21, to be found at <www.hiil.org>.

[2] These research questions will also be addressed in the HiiL Program, see Chapter 1, n **13**.

11.2 Internally binding

In practice BCR are made internally binding on group companies and on employees.

11.2.1 Binding on group companies

The BCR will bind the party that adopts the BCR, i.e. the (Delegated) EU Headquarters. The group companies would not be bound unless they are signatories to the BCR or if the (Delegated) EU Headquarters has adopted the BCR also on their behalf (and was duly authorised). However, as one of the requirements of the Working Party 29 is that the (Delegated) EU Headquarters has to accept liability for paying compensation and remedying breaches of the BCR by all group companies, this is irrelevant. The (Delegated) EU Headquarters will subsequently have to seek redress for any breaches of the BCR by a group company from such group company. For those purposes most multinationals have intra-company arrangements in place. If a multinational wishes to make the BCR legally binding on all individual group companies, various possibilities exist. The most obvious is to back up the BCR with intra-group agreements, either in a multi-party agreement in which all group companies participate, or each group company has a separate identical contract with the parent.[3]

11.2.2 Binding on employees

The requirement in the WP Opinions that the BCR should be internally binding on employees is in practice complied with by means of a clause in the individual employment contracts, that all company codes (as amended from time to time) should be complied with.[4]

11.3 Externally binding

[3] See ICC Report on BCR (Chapter 9, n 20), at 18 -22 on possible structures to achieve that BCR are binding on all group companies.

[4] See ICC Report on BCR (Chapter 9, n 20), at 23, reporting that in all countries researched (Belgium, Denmark, Germany, the Netherlands, the UK, Spain, Hong Kong, Japan, Switzerland and the US), inclusion of a contractual clause in employment agreements is valid. Another possibility reported is linking observance of the BCR with disciplinary procedures. This would obviously improve adherence to the BCR, but would not make BCR legally binding on employees.

11.3.1 Enforceability of unilateral undertakings

BCR are in principle a unilateral undertaking by the multinational and not a contract.[5] Most, but not all Member States seem to take the view that rights may be granted to third parties by means of unilateral undertakings.[6] For instance, under Dutch law unilateral undertakings are considered valid and binding on the party giving the undertaking[7] and all provisions of Dutch contract law will apply *mutatis mutandis* to such unilateral undertaking.[8] The Dutch Civil Code further contains an express provision to ensure that any such undertakings may be enforced before Dutch courts.[9]

11.3.2 Other grounds of enforcement

Even if certain jurisdictions do not consider unilateral undertakings to have binding effect, such legal orders will to varying extents recognise the protection of reliance on promises.[10] Where in a business context one party makes a promise which induces reliance by another party, such other party must be protected by law. The key element is whether there is "self-binding behaviour that gives the impression of being serious".[11] In BCR this self-binding behaviour is a given, as otherwise the BCR will not be eligible for approval by the Lead DPA. An important parallel here is the enforcement of unilateral undertakings made by companies in their CSR codes. For a long time many corporations and lawyers thought these promises constituted

---

5 This holds true unless specific contractual measures are implemented, see further para. 11.3.5.

6 See WP 133, part 2: Background Paper footnote 10 (Chapter 10, n 7), where it is mentioned that according to civil law of some jurisdictions (e.g. Italy and Spain) unilateral declarations or unilateral undertakings do not have binding effect. See further ICC Report on BCR (Chapter 9, n 20), at 24, where an overview is provided of countries in which unilateral undertakings by the parent company are enforceable (Belgium, Denmark, Germany, the Netherlands, the UK and Hong Kong); countries where they are not enforceable (Spain, Japan) and countries where possibly problems exist (Switzerland and the US).

7 Asser/Hartkamp & Sieburg 6-III 2010, no. 101, at 79, and the literature and case law therein referred to. This is in line with EU developments. See for instance Article 2:107 Principles of European Contract Law: "A promise which is intended to be legally binding without acceptance is binding." See also Article 3.20 Unidroit Principles of International Commercial Contracts 2004 and Article II-1:103 Draft Common Frames of Reference (**DCFR**).

8 Asser/Hartkamp & Sieburg 6-III 2009, no 101 (n 7), at 81, and literature and case law therein referred to.

9 Article 3:296 Dutch Civil Code.

10 This para. draws on Carola Glinski, "Corporate codes of conduct: moral or legal obligation?", in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 119-47.

11 Glinski (n 10), at 123.

moral obligations at best but had no legal effect. However, in many jurisdictions creative legal bases have been developed to enforce CSR codes against the parent company for human rights violations by their group companies or manufacturers in developing countries.[12] Some are very specific to the relevant jurisdictions and I will refrain from discussing these here.[13] Below I summarise briefly the main ground of enforcement in the EU that may be applied to enforce unilateral undertakings in corporate codes of conduct in general and a specific example of enforcement of corporate privacy codes.

11.3.3 Grounds of enforcement in the EU

For codes of conduct that are made public (as will be BCR for customers[14]), various grounds of enforcement can be construed under EU law: non-compliance with the code constitutes (i) a violation of the law on misleading advertising,[15] (ii) an unfair commercial practice,[16] or (iii) a violation of the principles of conformity of goods under contracts of sale.[17]

---

12 For a comprehensive overview of legal basis found for enforcement of CSR codes, see Doreen McBarnet and Patrick Schmidt, "Corporate accountability through creative enforcement: human rights, the Alien Torts Claims act and the limits of legal impunity," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007) at 148 -176. For further reading on the enforcement of unilateral undertakings in the EU and outside, see Wugmeister, Retzer, Rich (Chapter 7, n 61), at 491 – 494. On the Dutch situation, see A.J.A.J. Eijsbouts, "Elementaire beginselen van Maatschappelijk Verantwoord Ondernemen," in: A.J.A.J. Eijsbouts et. al, *Maatschappelijk Verantwoord Ondernemen en het Recht*, Preadviezen NJV 2010-1 (Kluwer 2010), at Chapter 2, at para. 5, 6 and 7.

13 See also para. 15.1 for the enforceability of CSR codes.

14 BCR have to be made known to the data subjects concerned. In case of BCR for Employee Data, this involves publishing the BCR on, for instance, the company intranet rather than on the internet. This therefore does not entail making publication of the BCR available to the general public.

15 See Directive 84/450/EEC relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, [1984] OJ 1984 L250/17. Pursuant to Article 2, 'Advertising' means the making of a representation in any form in connection with a business in order to promote the supply of goods or services; and 'misleading advertising' includes advertising which deceives or is likely to deceive the persons to whom it is addressed, or whom it reaches, and which, by reason of its deceptive nature, are likely to be affected in their economic behaviour. BCR for consumers could qualify as such.

16 See Directive 2005/29/EC on unfair commercial practices, [2005] OJ L149/22. Article 6(2)(b) provides that a commercial practice shall be regarded as misleading in cases of "non-compliance by the trader with commitments contained in codes of conduct by which the trader

Companies can also be held liable if they violate their own (internal) technical norms even if these internal standards exceed what is legally required in general.[18] Parent companies may further be liable based on tort law if a code of conduct was set at a level that was too low or if the code of conduct implies a control over subsidiaries based on which the parent has a duty of care to ensure that group companies comply.[19]
Some of the legal grounds listed above do not provide for adequate remedies for the individual third-party beneficiaries. For instance, the traditional remedy in unfair competition law is an injunction, which generally can only be invoked by consumer associations rather than individual consumers[20] and only in some jurisdictions may consumer associations also sue for damages (e.g. Germany).[21]

11.3.4 Enforcement of corporate data protection policies

For the enforcement of data protection policies, the enforcement action of the US Federal Trade Commission (**FTC**) is particularly relevant. In the past 10 years the FTC has used its authority under Section 5 FTC Act, which prohibits unfair or deceptive trade practices, to take action against companies that misrepresent their privacy practices to consumers.[22] The FTC also enforces a number of sector-specific statutes that include data protection provisions, including the Fair Credit Reporting Act, the Gramm-

---

has undertaken to be bound, where (i) the commitment is not aspirational but is firm and is capable of being verified; and (ii) the trader indicates in a commercial practice that he is bound by the code." Article 2(d) requires that the act by the trader was directly connected with the promotion, sale or supply of a product. From the perspective of BCR, this may be the case if the conditions of sale contain a privacy provision which contain a reference to these BCR.

17 See Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees, [1991] OJ L171/12. Pursuant to Article 2(2)(d), the concept of conformity includes conformity with public statements on the specific characteristics made about products not only by the seller, but also by the producer or his representative, particularly in advertising or on labelling. BCR may constitute such relevant statement as well.

18 Glinski (n 10), at 135.

19 Glinski (n 10), at 141-146.

20 A notable exception is Spanish law. The Directive on unfair commercial practices does not require the introduction of individual rights, but does not prohibit them either (see Recital 9).

21 Para. 8 of the Law against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb-UWG) of 3 July, 2004.

22 An overview of FTC enforcement cases in respect of data protection policies can be found at <www.ftc.gov>. This is an example where a public agency is not only tasked with enforcement of administrative or criminal legislation but also tasked with monitoring and enforcement of businesses to act consistently with their private law obligations, see Scott (Chapter 8, n 25), at 7.

Leach-Bliley Act, the Children's Online Privacy Protection Act (COPPA), the CAN-SPAM Act and the Telemarketing and Consumer Fraud and Abuse Prevention Act (Do Not Call Rule).[23] Some highlights in FTC's enforcement action include the charges it issued against Google, stating that Google had used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. On 30 March 2011, the FTC announced[24] that Google accepted the FTC settlement order barring the company from future privacy misrepresentations, requiring it to implement a comprehensive privacy program, with regular, independent privacy audits for the next 20 years. The settlement with Google marks the first time that the FTC has required a company to implement a comprehensive privacy program to protect the privacy of consumers' information (as opposed to a comprehensive security program), and that the FTC has alleged violations of the substantive privacy requirements of the US Safe Harbor Framework.

---

[23] The Fair Credit Reporting Act, 15 U.S.C. para. 1681 (2010) (regulating the reporting on consumer credit history); Gramm-Leach-Bliley Act, 15 U.S.C. paras. 6801-6809 (2010) (regulating consumer financial data); COPPA, 15 U.S.C. paras. 6501-6506 (2010) (regulating information about children); CAN-SPAM Act, 15 U.S.C. paras. 7701-7713 (2010) (regulating unsolicited electronic messages); and Do Not Call Rule, U.S.C. paras. 6101-6108 (2010) (regulating telemarketing calls).

[24] See press release dated 30 March 2011 "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network. Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data", to be found at http://ftc.gov/opa/2011/03/google.shtm. The FTC announced that Google agreed to settle charges that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. According to the FTC's complaint (i) Google led Gmail users to believe that they could choose whether or not they wanted to join Google Buzz, while the options for declining or leaving Google Buzz were ineffective; (ii) for those who joined Google Buzz, the controls for limiting the sharing of their personal information were difficult to locate and confusing; (iii) Google violated its privacy policies by using information provided for Gmail for another purpose – social networking – without obtaining consumers' permission in advance; (iv) Google misrepresented that it was treating personal information from the EU in accordance with the US Safe Harbor Framework because it failed to give consumers notice and choice before using their information for a different purpose from that for which it was collected. The settlement requires Google (i) to obtain consumers' consent before sharing their information with third parties if Google modifies its sharing practices; (ii) to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information; and (iii) to obtain initial and biennial assessments for 20 years from an independent auditor to ensure that it is following the required comprehensive privacy program.

As multinationals will publish their BCR for Customer Data on the Internet (in order to comply with BCR requirement (xiv),[25] the FTC has authority to take action if a multinational subsequently does not comply with its BCR. Although the FTC Act applies to consumers only, the FTC claims[26] that it has also the authority to prosecute employee privacy codes (as they are also private individuals). This seems questionable as employee privacy codes apply to individuals in their capacity of employee and not in their capacity of consumer and are in most cases not published on the Internet, but on the multinational's **intranet** only. As a result it is difficult to see why this could constitute an unfair or deceptive trade practice.

11.3.5 Solutions to ensure that BCR are externally binding

If Lead DPAs in certain countries have doubts[27] about whether the BCR are externally binding (i.e. the legally enforceable) in their respective jurisdictions, a solution is to put a contract in place between the (Delegated) EU Headquarters and, for instance, the group company in the jurisdiction of the DPA. In all Member States it is possible to grant third-party beneficiary rights in a contract.[28] However, rather than having to resort to such legal solutions, it would simplify matters considerably if European legislators could provide in the revised Directive that BCR can be enforced as unilateral undertakings by the third-party beneficiaries. The issue of external bindingness is by the way not particular to BCR. In the literature regarding TPR, authors comment that the conventional principles of contract law are not adequate to cater for enforceability of TPR by the beneficiaries of TPR and that the law needs to be reformed to accommodate this.[29] As such

---

25 The multinational will have to make its BCR "easily accessible to the individuals concerned." In the case of BCR for Customer Data (i.e. consumers), this may be achieved by the multinational by publishing the BCR on its corporate website.

26 To date the FTC has not taken action against a company for false or deceptive trade practices with respect to employee data, and it is an open question whether it indeed may do so. See Wugmeister, Retzer, Rich (Chapter 7, n 61), at 489 in particular footnote 81.

27 In my experience, the Lead DPAs of the UK, France, Germany and the Netherlands accept that BCR, being unilateral undertakings, are externally binding.

28 WP 74 (Chapter 10, n2), at 12, footnote 11 and WP 133, part 2: Background Paper, footnote 10 (n 7), where it is mentioned that "in the lack of specific legislative provision for the bindingness of such declarations, only a contract with third party beneficiary clauses between the members of the group may give proof of bindingness." See the ICC Report on BCR (Chapter 9, n 20),at 25, for an overview of countries where BCR can be made binding for data subjects by making them third party beneficiaries under a contract (yes in: Belgium, Denmark, the Netherlands, Germany, Spain, the UK, Switzerland); no: Japan and Hong Kong; possibly in: the US).

29 This is discussed in para. 11.4, see in particular n33.

general reform of the law to facilitate enforcement by third-party beneficiaries of unilateral undertakings (like TPR) is outside the scope of this work, I will limit my recommendation to enforceability of BCR. This recommendation is of paramount importance as the enforceability of BCR will be shown to be a requirement under all disciplines against which BCR will be evaluated in this dissertation. These all require that the BCR provide for "sufficient possibilities of redress for the beneficiaries".[30] The enforceability of BCR as unilateral undertakings is a prerequisite for any such form of redress. I will not repeat this recommendation in these Chapters, but it equally applies there.

Recommendation 8
Provide that BCR can be enforced as unilateral undertakings by the beneficiaries of BCR.

11.4 Contractual "supply chain management"

Similar limitations under contract law are presented when TPR are imposed by a party on other parties in the supply chain, through contractual provisions in their supply chain contracts.[31] To a certain extent the BCR regime also relies on supply chain management to ensure protection of the employee and consumer data governed by the BCR. If a multinational contracts with a third party in the context of which personal data of employees or consumers are transferred to such third party, contractual safeguards to protect these data should be put in place. Examples are when a multinational contracts with a third party to arrange all travel of its employees, or to manage its car fleet, corporate credit cards or employee communication devices. Compliance with the material data processing principles under the BCR will only be possible if the multinational imposes on its external supplier sufficient safeguards for the data protection interests of the employees and consumers. To achieve this, the BCR regime requires

[30] See for evaluation of BCR from perspective of PIL: para. 12.3.3; from perspective of accountability; para. 13.2, from perspective of legitimacy of TPR; para. 14.6.3; and from perspective of CSR para. 15.2.9.

[31] As is often done with food standards, environmental standards, CSR codes, etc. on contractual supply chain management in respect of CSR, see McBarnet and Kurkchiyan (Chapter 9, n 41). See further on supply chain management as to food safety requirements, Fabrizio Cafaggi, "Private Regulation, Supply Chain and Contractual Networks: The case of Food Safety," EUI Working Papers RSCAS 2010/10.

that the BCR provide for the obligation of the multinational to enter into written agreements with its external suppliers, which have to meet the following requirements:[32]

- in the case of an external data controller: the written contract should impose the relevant material BCR principles on the supplier;
- in the case of an external processor: the written contract should impose the mandatory processor obligations on such external processor (see Paragraph 7.1.4 above);
- if the external controller or processor is located outside the EU: the data transfer rules in the BCR also have to be complied with, for instance by making use of the EU Standard Contractual Clauses (see Paragraph 7.1.3 above).

In the general literature regarding contractual supply chain management of TPR, there are two issues identified, which are of equal relevance to the contractual safeguards imposed by the multinational on its external suppliers. The first is that the present third-party beneficiary doctrine (in the absence of a specific clause thereto) in most cases does not provide for the possibility for the beneficiaries of TPR to enforce their rights under the TPR also against the third-party supplier.[33] The second issue is that, even in case the contract with the third-party supplier contains a third-party beneficiary clause, enforcement by the beneficiaries against such third-party

---

[32] See BCR requirement (v) in para. 10.2.

[33] See Cafaggi (Chapter 6, n 67) at 31, under reference (see footnote 173) to "Doe v. Wal-Mart 572 F.3d 677 (9th Circ. 2009), where the court denied workers of a supplier of Wal-Mart the status of third party beneficiaries, arguing that the clause incorporated in the contract between Wal-Mart with the supplier did not constitute a promise on behalf of Wal-Mart towards the workers, since it would have been necessary in order to establish third party beneficiary. In the eyes of the court, "the requirement that the suppliers were to provide sufficient working conditions and the clause that gave Wal-Mart the right to conduct inspections of the working si[t]e whether those requirements were kept, concerned purely the relationship between the two contracting parties but had no beneficial effect to the workers themselves." See also Cafaggi (n 31), at 25: "Neither individual consumers nor consumer associations are technically part of these contracts, which makes it difficult to enforce them if violations occur. Legal systems define different ways in which these contracts can be directly enforced by consumers and/or their associations: (1) "*action directe*" by the consumer against the supplier, (2) require unequivocal statements that their contracts are for the benefit of third parties, (3) allow enforcement using implied terms of consumer contracts, (4) grant individual or class remedies under civil liability, (5) qualify violations as unfair commercial practices."

supplier is not very realistic, as already discussed in Paragraph 8.3.[34] A third more general issue raised in the literature regarding contractual supply management of TPR, is the inherent weakness of a chain of contracts along the supply chain replicating the required contractual clauses.[35] This is also a feature of IT outsourcing arrangements, since in most cases the main outsourcing supplier not only involves many of its group companies as a sub-processor but also third parties not part of its group of companies as sub-processor. As a backdrop to the discussion of these three issues, it is important to realise that at present supply chain management especially in the consumer protection area, is arguably the strongest tool to achieve consumer protection in practice. As one author puts it:[36]

> "It is through the contracts between manufacturers and their component suppliers and between retailers and distributors and manufacturers that many of the norms governing standards which can be expected of consumer products are set. A key contemporary example is the power of major supermarkets to set and enforce their standards for such matters as food safety. In many service sectors too contracts have a central role in defining standards. A key example is where service providers operate as a franchise (...)."

This is despite the fact that contractual control of the supply chain rarely results in enforcement through the courts and in effectuating the agreed remedies for breach. Rather the contracts and contractual remedies provide a framework within which exchange occurs and matters are solved not so much by the terms of the contract but by adjustment of continuing relations.[37] Given the fact that by now data processing is increasingly performed in networks whether within multinationals, between multinationals, or between multinationals and individual customers (i.e. internet users), the participants in such networks manage the risks: they accept them, try to limit or minimise them, or transfer them to co-

---

34 Suppliers being often located in countries where contractual enforcement is not easy. See Cafaggi (Chapter 6, n 67) at 32.

35 Cafaggi (n 31), at 13.

36 Scott (Chapter 8, n 25), at 6.

37 Scott (Chapter 8, n 25), at 6 (under reference to Stuart Macaulay., Non-Contractual Relations in Business: A preliminary Study, American Sociological Review, 1963, 28:55-83; Hugh Beale and Tony Dugdale, Contracts Between Businessmen, British Journal of Law and Society, 1975, 2:45-60) reports that "sociological research both in the UK and the United States suggests that where problems do emerge within contractual settings, businesspeople may not be inclined to rely on the letter of their contractual entitlements to pursue litigation. Rather contracts provide a framework within which exchange occurs, but the response to the contract is not dictated by the contract."

contractors or other partners.[38] Based hereon the conclusion is justified that (as with consumer protection) supply chain management will become increasingly important, if not decisive, in achieving data protection in practice.

11.5 How to address the contractual supply chain management issues in BCR?

11.5.1 Enforceability against the external supplier

The WP Opinions do not require imposing a third-party beneficiary clause in contracts the multinational enters into with its external suppliers. However, if the external supplier is established in a non-adequate country, the multinational will have to "adduce additional safeguards with respect to the protection of personal data",[39] which will in most cases be achieved by the multinational and the external supplier entering into the EU Standard Contractual Clauses. The EU Standard Contractual Clauses contain specific third-party beneficiary clauses which (under certain circumstances) enable data subjects to bring an action against the external supplier in case of a data protection breach.[40] As indicated, the WP Opinions do not require imposing an equivalent third-party beneficiary clause in contracts the multinational enters into with external suppliers in the EU or other adequate countries. The underlying reasoning for this is probably that such third-party supplier is directly subject to the data protection laws of the EU or such adequate country which provide for sufficient protection of data. However, this is not automatically the case. One example is provided to clarify this.

BCR for Employee Data often contain a clause that employee data will not be used for direct marketing purposes. The multinational enters into a framework agreement for health insurance for its employees. Individual employees can enter into an individual insurance agreement with the insurance company under this framework agreement. The multinational correctly imposes the terms of the BCR on the insurance company. Under

---

38 Pierre Trudel, "Privacy Protection on the Internet," in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 19, at 332-334. See Raab and Koops (Chapter 8, n 23), at 220, who have attempted to map the landscape of privacy actors in the online data protection arena "showing a remarkable range of diverse and versatile actors with many potential interconnections and interrelationships."

39 See para. 7.1.3, n 35.

40 See Article 11(2) of the EU Standard Contractual Clauses for processors and Articles I(e) and III of the EU Standard Contractual Clauses for controllers.

the current EU law, the insurance company (being a controller in its own right) is in principle authorised to use the data of its customers (i.e. the employees) for direct marketing purposes on an opt-out basis.[41] If the insurance company, despite its contractual restrictions, uses the employee data for direct marketing, the employees will have an interest in being able to act directly against the insurance company.

The only way to address this would be to make a third-party beneficiary clause mandatory in all contractual arrangements with the multinational's external suppliers in the context of which personal data are transferred. This being said, I seriously doubt whether this suggestion would indeed lead to better enforceability of data protection by individuals in practice. Individual data subjects will not sue third-party suppliers, if only for cost reasons which will in most, if not in all, cases outweigh the damages suffered by the individual.[42] I will therefore not recommend that this requirement should be made part of the BCR regime. Rather, my conclusion is that the third-party beneficiary clause in the EC Standard Contractual clauses – though looking good on paper – does not offer any meaningful form of redress for the third-party beneficiaries.[43] Worse, since the EC Standard Contractual Clauses may not be deviated from and the rights of the third-party beneficiaries are prescribed in detail, multinationals contracting with their external suppliers will not consider improving on these, even though they certainly would have (or better: are the only ones that have) the bargaining power to do so. That multinationals are here the party best positioned to ensure better rights for the beneficiaries is not a new insight, but a fact well known in other areas of law. This is one of the reasons for states to resort to TPR as the contracting parties have more power to enforce compliance than does the threat of traditional judicial means. As one author (in the context of supply chain management in respect of food safety) puts it[44]:

> "States are weak enforcers of rules concerning transnational supply chains, so resorting to private regulation is an implicit delegation to industry, in particular retailers, of the task of devising compliance mechanisms to be applied in

41 See for the opt-out possibility for sending direct email to existing customers: Article 13(2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L201, 37; as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (**e-Privacy Directive**).

42 See para. 8.3 for enforcement issues in respect data protection leading to a lack of enforcement in practice.

43 Kuner (Chapter 6, n 52), at 271.

44 Cafaggi (n 31), at 9.

> suppliers' countries. Market accountability through self-enforcing contracts, by threatening contract termination or lack of renewal, may offer better incentives to comply than legal accountability before domestic courts. Litigation in importing countries represents only a last resort mechanism; self-enforcing contracts, based on asymmetric contractual powers and market-share, often provide more effective enforcement mechanisms."

The recommendation to EU legislators concerning BCR is therefore not to focus on traditional judicial legal rights and remedies of individuals, but concentrate on means of redress that actually achieve compliance in practice. If any new requirements are to be formulated to address a potential lack of redress by the beneficiaries of TPR, a practical solution would be that the internal complaints procedure that is required under BCR is made open also for complaints of beneficiaries as to the processing of their data by the external suppliers complemented by an obligation of the multinational to follow these up with its external suppliers. This suggestion will be part of my combined recommendations in Paragraph 13.6, in the context of introducing the accountability principle for data transfers.

11.5.2 Enforceability against the multinational

Rather than relying on ex-post enforcement, a second solution suggested in the literature to improve compliance throughout the supply chain with contractually imposed TPR obligations, is to impose a monitoring obligation on the multinational having adopted the TPR.[45] Most supply contracts already contain a provision regarding monitoring by the multinational of compliance of the external supplier, but a **right** to do so only.[46] This is the same in the context of data protection. Most outsourcing contracts under which a multinational transfers personal data to a supplier will include such monitoring and auditing provisions. Since in outsourcing relations many of the data processing operations of a supplier are similar for different customers, the parties often agree that the data processing operations of a supplier are certified by an external auditor for the benefit of all customers, saving costs and time for all involved. Rather than the multinational monitoring and auditing the operations of the supplier, the supplier will yearly submit a "Third Party Memorandum", a statement of the external auditor, describing the data processing operations of the supplier, the applicable control mechanisms and a certification that the data processing

45 Cafaggi (Chapter 6, n 67) at 32 and Cafaggi (n 31) at 15.

46 Cafaggi (Chapter 6, n 67) at 32; McBarnet and Kurkchiyan (Chapter 10, n 41), at 75.

operations of the supplier are compliant.[47] The right to audit is further one of the mandatory processor provisions which have to be included in all data processing agreements the multinational enters into with a data processor.[48] The question is whether the **right** of multinationals to monitor and audit compliance should be replaced by an **obligation** to do so. In short, I would not be in favour of introducing this obligation in the BCR regime. Large multinationals have thousands of suppliers and introducing ongoing monitoring and auditing obligations in respect of external suppliers involves a disproportionate increase in effort and costs. As indicated before, since it is in their own interest that the data transferred to a third party are properly processed, multinationals mostly put proper safeguards in place, including the right to monitor or audit compliance of the third-party supplier, if so deemed necessary. If critical data processing operations are outsourced, multinationals require periodic audit statements on compliance with security and other requirements under the outsourcing contract. It should be left to the multinationals to assess based on a risk assessment if, and if so, which monitoring and auditing measures are indicated.[49] This approach is

---

47 If a multinational is listed in the US, and the outsourcing can influence the content and reliability of the annual accounts, such a Third Party Memorandum has to meet requirements under Article 404 of the Sarbanes-Oxley Act and the rules of the US Securities and Exchange Commission. This requires a statement to conform to the auditing rules of the US accounting organisation, the "Statement on Auditing Standards No. 70: Service organisations" (in practice often referred to as "**SAS 70**" statement). See Lokke Moerel and Bart van Reeken e.a., *Outsourcing, een juridische gids voor de praktijk,* third edition, Kluwer May 2009, at para. 9.3.8.

48 See on the mandatory processor provisions para. 7.1.4.

49 McBarnet and Kurkchiyan (Chapter 10, n 41), at 63 note: "The supply chain is becoming increasingly recognised as an area of reputational – and indeed insurance – risk, with a number of companies beginning to develop a "risk-based approach to supplier engagement" and "systems to identify higher risk suppliers" (this referring to Vodafone Corporate Social Responsibility Report for 2004 – 2005, at 24 and other examples listed). McBarnet and Kurkchiyan, (Chapter 10, n 41) at 75, further note that "in line with the partnership model, however, the enforcement approach [of multinationals against their suppliers] is not punitive but follows the "compliance model" approach. [The] policy is more about bringing their suppliers into compliance over time than immediately resorting to penalties. Best practice involves on-site monitoring of all suppliers at the outset, to check whether they meet the requirements, identifying and reporting shortcomings and carrying out follow-up assessments of progress towards rectifying them, usually over an agreed period of time. There will also be a "continuous improvement" programme and continued periodic audits". See further at 79: "In terms of legal consequences, non-compliance with the contract is highly unlikely to ever result in a court case (…) As is usual in business contracts more generally, any sanction for non-compliance normally consists of economic leverage rather than legal procedure. (…) perhaps the

very much part of an "accountability principle" for data transfers, and will be further discussed in Paragraph 13.6.

A second solution suggested in the literature to improve compliance with contractually imposed TPR obligations, is to require that TPR contain a provision allowing the pursuit of remedies against the multinational in case it has not imposed proper contractual protections on the external supplier as required by the TPR.[50] This requirement seems to be already implied in the present BCR regime. The BCR regime requires that the multinational impose contractual data protection provisions on its external suppliers. If the multinational fails to do so, the beneficiaries of the BCR can act against the multinational. Explicitly providing so in the BCR does not seem to make much of a difference. Reading the suggestion made in the general literature regarding TPR, it comes very close to introducing the accountability approach[51] to data transfers as included in the APEC Privacy Framework and the countries that have already introduced this principle (see Paragraph 7.4). I will discuss the merits of the accountability approach to data transfers in Paragraph 13.6 and will refrain here from making recommendations conforming to this suggestion.

11.5.3 From 'supply chain' to 'network'

Simply put, the contractual chain (whereby a party to a contract involves a sub-contractor, who, in turn, involves a sub-sub contractor, etc) is as strong as the first link and the outcome for beneficiaries is therefore very much dependent on the contracting power of the parties in the main contract. Another weakness of a chain of identical obligations is that the various parties involved in the chain may be responsible for different parts of the services and it will not be clear with which party the respective obligations as to the beneficiaries may lie. A suggestion in the literature relating to TPR is to approach the supply chain as a contractual network rather than a chain.[52] Effective supply management is achieved when the risk of non-compliance is minimised at the source of the risk. Rather than imposing

---

most persuasive and effective non-legal sanction comprises a refusal to deal with the other party in the future."

50 Cafaggi (n 31), at 25.

51 Cafaggi (n 31), at 25: "This tension may be solved in different ways: by imposing the primacy of a liability driven network, or by disentangling the contractual form of the network from the liability regime. In the latter case, enterprises along the chain will be able to arrange their own internal organisational structure which will be affected by the liability regime but not necessarily entirely shaped by it."

52 Cafaggi (n 31), at 13 and 17 and further para. 8.

requirements on all subsequent parties in the network, a more productive exercise may be to first identify the risks, their source and then allocate responsibilities accordingly. Different solutions are suggested in the literature to incentivise the parties to a "network" to ensure the optimal allocation of the responsibilities over the parties involved. Legislative measures suggested to achieve this are: (i) allocating strict liability with the party with the best negotiation powers (who will use this power to allocate responsibilities); (ii) imposing "network" liability (i.e. all parties are jointly and severally liable for the compliance of the network as a whole);[53] and imposing joint and several liability on "gate keepers".[54] In the context of online data protection potential gate keepers may be ISPs, being intermediaries between individuals and companies as online data processing is concerned and having the capacity to block websites. I will discuss the merits of these suggestions in Paragraph 13.6, as again, these are very much part of an "accountability" requirement in respect of data transfers.

11.6 Conclusion as to contractual issues of BCR

In this chapter I discussed the contractual issues of BCR, which concern the question of enforceability of BCR by third-party beneficiaries and supply chain management issues under BCR. My conclusion is that the enforceability issue of BCR by third-party beneficiaries may and should be solved. The supply chain management issues of BCR are not that easily solved or optimised. Supply chain management is not new and the existing literature on supply chain management of other forms of TPR provides a host of ideas on how to optimise such management. Given the fact that data processing is performed in networks rather than in neat one-to-one relationships, contractual supply chain management will become correspondingly important, and may prove ultimately the strongest tool to achieve data protection in practice. The options I discussed for improving supply chain management have not led to specific recommendations as the merits of these will be further discussed in Chapter 13 as part of introducing the accountability principle for data protection.

---

53 Cafaggi (n 31), at 17 and 25.

54 Scott (Chapter 8, n25), at 9, gives as an example credit card companies having the capacity to issue charge backs to companies breaching consumer contracts. Another example is banks having the capacity to block payments to illegal gambling sites.

12 BCR and EU rules of private international law

12.1 Introduction

BCR, like most transnational private regulation (**TPR**), have to function within many different public and private spheres. For BCR to be acceptable in all different spheres they touch on, they must be aligned with the existing disciplines they interact with.[1] The main discipline BCR touches on is that of private international law (**PIL**). As one author puts it, PIL is the "queen mother of all transnational legal thought".[2] The interaction with PIL is twofold. First there is the traditional function of PIL where, for instance, a choice of law and forum made in BCR has to comply with rules of PIL. This is also called the function of PIL as a "mechanism" or the "touch down" function.[3] Due to these rules of PIL, state law becomes relevant, again, for instance as a choice of law and forum leads to the competence of the courts and questions arise as to enforcement of judgments of such courts.[4] The second function of PIL is that of a potential source of "meta-norms" for BCR.[5] For BCR (operating at the global level) to be acceptable at the national level, BCR will have to "build on the assumption of common reference points" between national jurisdictions.[6] Sidelining, for instance, the underlying policy choices behind PIL instruments and doctrines will not achieve universal acceptance.[7]

Assessing the role of PIL in respect of BCR has been surprisingly difficult for a number of reasons. As to PIL's role as a mechanism, it is surprising how little interest the disciplines of TPR and PIL show in each other's fields. As one author from the TPR discipline recently put it "standard treatments of transnational regulation (…) rarely devote sustained attention to discussion of PIL matters".[8] This lack of interest is reciprocal, as I have not come across any substantive discussion of the role of PIL as to TPR in standard treatments of PIL either. As to the second function of PIL as a potential source of meta-norms, it is relevant that PIL traditionally does not

1 See n 77.

2 C. Joerges, *Rethinking European Law's Supremacy*, EUI Working Papers 2005/12 (2005), at 7.

3 See Bomhoff and Meuwese (Chapter 6, n 75), at 172.

4 See Bomhoff and Meuwese (Chapter 6, n 75), at 171.

5 Especially as to the socio-economic and political implications behind PIL instruments and doctrines. See Bomhoff and Meuwese (Chapter 6, n 75), at 172.

6 Bomhoff and Meuwese (Chapter 6, n 75), at 165. See in more detail para. 6.4.

7 Bomhoff and Meuwese (Chapter 6, n 75), at 172.

8 Bomhoff and Meuwese (Chapter 6, n 75), at 172. Noteworthy is that the authors themselves also do not discuss the PIL issues relating to TPR.

incorporate a regulatory perspective, in the sense that it is intended to achieve a certain desired outcome. Rather it is based on "substantive neutrality" (as to the law applicable) which is traditionally considered the appropriate basis for the main starting point for EU rules of PIL, being choice of law.[9] This being said, underlying meta-norms can be discerned especially in relation to the exceptions to the main principle of choice of law and forum that were considered necessary in instruments of PIL and which are relevant to BCR as well.

12.1.1 PIL as a mechanism

The introduction by a multinational of BCR raises several questions of PIL. Though most of the WP Opinions do not explicitly state so, the WP Opinions seem to be based on the assumption that BCR will apply to the relevant processing of personal data by a multinational, **unless** in a certain jurisdiction stricter national requirements apply. In this case such stricter national requirements must be met in the relevant jurisdiction, i.e. the BCR should provide for a **minimum level of protection** for the processing of personal data by the multinational, setting aside the national data protection laws at least for the relevant minimum level. [10] Further, the WP Opinions require that BCR provide for the possibility of enforcement of BCR via the forum of either (i) the EU group company at the origin of the transfer or (ii) the (Delegated) EU Headquarters,[11] setting aside the jurisdiction that the courts of other Member States may have under applicable rules of PIL. These requirements of the Working Party 29 pose problems with (i) the mandatory nature of the applicability and enforcement regime of the Data Protection Directive and (ii) the EU rules of PIL (and also non-EU rules of PIL for that matter). As to rules of PIL, an additional problem is posed by the fact that the main personal data processed by multinationals under BCR concern personal data of their employees and those of their customers, who are in many cases consumers. As far as employee and consumer contracts are concerned, the rules of PIL create a mandatory regime – both in terms of applicable substantive law and in terms of dispute resolution mechanisms – which may not be set aside to the detriment of the employee or the consumer by a choice of law or forum.

---

9 This concept is still the main principle of the EU rules of PIL. Bomhoff and Meuwese (Chapter 6, n 75), at 174.

10 See for instance WP 153 (Chapter 10, n 7) at 11, where is stated that it is advisable that the BCR state that "where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it takes precedence over the BCR."

11 WP 74 (Chapter 10, n 2), at 19.

12.1.2 Preferences of multinationals

Another problem posed under PIL is due to the fact that multinationals introducing BCR have a strong interest in including a choice of law and forum clause in their BCR. The main reason for this is that it is in the interest of the multinational that all complaints under the BCR are ultimately dealt with by the Lead DPA (and the courts of the Lead DPA) as this DPA negotiated the provisions of the BCR under the applicability of the Lead DPAs own law (i.e. the law under which the provisions of the BCR were drafted). This ensures for the multinational a consistent and predictable interpretation and application of the BCR. For the same reason the multinational has an interest in the Lead DPA having central supervision over the BCR.[12] Again, as under the BCR mainly employee and consumer data are processed, this poses problems as to (i) the mandatory nature of the applicability and enforcement regime of the Data Protection Directive and (ii) EU rules of PIL.

12.1.3 Preferences of beneficiaries BCR?

The background of both the mandatory rules of the Data Protection Directive and the consumer and employee protection regimes under PIL is the protection of weaker parties (i.e. employees and consumers). The question, however, is whether in this case the interests of the employees and consumers are indeed best served by not allowing a choice of law and forum for the jurisdiction of the Lead DPA. In Paragraph 8.3, I discussed that though individuals have proper rights and remedies under the Data Protection Directive, these are difficult to effectuate in practice. I also discussed some alternative options that offer more realistic hope of redress for individuals. One possible alternative I put forward is a choice of law and forum in TPR (in this case BCR). Such choice of law and forum will drastically improve the data protection and the access to remedies for the individuals covered by the BCR. This would work out as follows.

The BCR regime requires that the multinational implement a complaint procedure. If a breach occurs, the individual affected will be able to file a complaint with the group company with which he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The individual will therefore not have to prove which of the group companies was at fault (which is one of the obstacles in practice to bringing and succeeding in a claim). There is also no issue as to which law applies and whether the relevant law provides for data

[12] The WP Opinions require an obligation of the group companies to cooperate with all DPAs, to abide by their advice in respect of the BCR, and to accept to be audited by the DPAs.

protection. Also, if the country of the individual has no privacy protection at all, the BCR apply. The complaint may be filed by the individual in his own language. The group company that received the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and for ensuring the required translations are provided. If the complaints procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the Lead DPA or the courts of the Lead DPA. This procedure will lead to enforceable rights even in jurisdictions where no (adequate) data protection laws are in place or where insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimises costs. None of the cross-border enforcement issues discussed in Paragraph 8.3 apply.

The fact that employees and consumers may actually be best served with a choice of law and forum in BCR, is a factor to be taken into account when evaluating the PIL issues in respect of BCR.

12.2 Applicability, jurisdiction and enforcement

In this Chapter, I will discuss how the applicability, jurisdiction and enforcement regime of the BCR can be best set up in light of the combined requirements of the Working Party 29 and the multinational's preferences as discussed above and the requirements of PIL. For that purpose a number of questions will be discussed:

- **Which instruments of PIL are relevant?** This requires first a discussion of how the data protection regime under the Data Protection Authority should be qualified, as public or private. For instance the Brussels I Regulation[13] applies to civil and commercial matters only (Paragraph 7.1.1).
  The conclusion is that the EU data protection regime is clearly a combination of private and public law, the logical consequence of which is that the different parts should be treated accordingly.
- **Do the rules of PIL take precedence over the applicability and jurisdiction regime of the Directive?** This depends on whether the applicability and enforcement regime of the Data Protection Directive is considered to provide "conflict rules" and as such take precedence over the general conflict rules of.EU PIL. (Paragraph 12.3.2).

[13] EC Regulation 44/2001 of 22 December 2000 on jurisdiction and enforcement [2001] OJ L12/1 (**Brussels I Regulation)**.

The conclusion here is that the applicability and jurisdiction regime of the Data Protection Directive takes precedence over the relevant rules of PIL.

- **Is a choice of law and forum possible under the Directive?** The next question is whether a multinational can make a choice of law and forum in BCR which deviates from the applicability and enforcement regime of the Data Protection Directive. This depends on whether the applicability and enforcement regime of the Data Protection Directive is of a mandatory nature (in which case parties cannot deviate from this regime by making a choice of law and forum in a contract) (Paragraph 12.3.3).
  The answer is that the applicability and enforcement regime is of a mandatory nature and that a choice of law and forum is as a rule not possible. There are, however, good arguments that this rule may find exception if in BCR the law and forum of another Member State are chosen. In light of the uncertainty of whether a choice of law and forum may be made in BCR, the conclusion is that multinationals are advised to set up the applicability and enforcement regime of BCR in such a manner that the pitfall of deviation from the mandatory applicability and jurisdiction regime of the Directive is avoided.
- **How may the applicability and enforceability regime of BCR be set up?** The recommendation is that the BCR should be set up in such a manner that they do not provide for a **minimum** level of protection**,** but rather provide for **supplemental** protection. As all national rights and remedies of individuals thus remain in place, the BCR do not contravene the mandatory applicability and enforcement regime of the Data Protection Directive. In this set up a choice of law and forum in the BCR (as to the supplemental rights and remedies provided) seems to be an option (Paragraph 12.4).
- **What are PIL issues as to the proposed BCR applicability and enforcement regime?**
  PIL questions that have to be answered in respect of the proposed BCR applicability and enforcement regime are:
  (i) whether Rome I and Brussels I Regulation apply to this choice of law and forum made in the BCR (Paragraph 12.6);
  (ii) and if so, whether such choice of law and forum is in conformance with the EU employee and consumer protection regimes of PIL (Paragraph 12.8); and
  (iii) whether the choice of law and forum clause in BCR meets the requirements **as to form** under PIL (Paragraph 12.9).

My overall conclusions and recommendations are presented in Paragraph 12.11.

12.3 Role left for EU rules of PIL?

12.3.1 Qualification of data protection law

To determine which instruments of PIL may be in scope, it is relevant whether data protection law should be qualified as private law, public law or a combination of these. For instance, the Brussels I Regulation[14] applies to civil and commercial matters only. Further, if data protection is to be considered public law, a court or DPA would always have to apply its own law and never a foreign data protection law.[15] The Data Protection Directive does not provide for a classification (i.e. private or public) nor prescribes how the Member States must implement the Data Protection Directive in their national law (i.e. as constitutional rules, mandatory rules or regulatory rules).[16] As a consequence there are many different ways in which Member States have chosen to implement the Data Protection Directive in their national legislation.[17] Also, by studying these national laws it is impossible to

---

14 Article 1 Brussels I Regulation.

15 See Jon Bing, *Data protection, jurisdiction and the Choice of Law*, paper delivered at the 21st International conference on Privacy and Data Protection, Hong Kong, 14 September 1999, at 2, to be found at <www.pcpd.org>. See also Christopher Kuner, Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1) (October 1, 2010), International Journal of Law and Information Technology, Vol. 18, p. 176, 2010. Available at SSRN: http://ssrn.com/abstract=1496847, at 10, also referring to Bing and further to Maria Veronica Perez Asinari, 'International Aspects of Personal Data Protection: Quo Vadis EU?' in: Maria Veronica Perez Asinari and Pablo Palazzi (eds), Challenges of Privacy and Data Protection Law (31 Cahiers du CRID) (Bruylant 2008) 381, 405, stating that Article 4 of the EU Data Protection Directive 'could be considered, in principle, as a mandatory rule', but adding that 'the nature of this Article has not been extensively studied'."

16 C.M.K.C. Cuijpers, *Privacyrecht of privaatrecht. Een privaatrechtelijk alternatief voor de implementatie van de Europese Privacy richtlijn* (diss. Tilburg) (Wolf Legal Publishers 2004), at para. 6.4., in particular at 222; Colette Cuijpers, 'A Private Law Approach to Privacy; Mandatory Law Obliged?', [2007] Scripted, doi: 10.2966/scrip.040407.304, at para. 3.

17 For an overview of the different ways in which the Data Protection Directive is implemented in the national laws of the Member States, see Korff (n 3). In para. 3.4, an overview is given of the different status the various Member States have given to data protection rights (varying from a constitutional status overriding any other national laws, (as in Germany) to a status whereby other laws override the data protection laws (as in Sweden). See further Chapter 13, discussing the different legal bases on which damages can be claimed, varying from the ordinary rules on

come to a preponderant classification of EU data protection law in one single category (i.e. either private or public). As the right to data protection is a fundamental human right and freedom,[18] and the basis for the Data Protection Directive is to implement these rights and ensure a high level of protection,[19] a number of Member States have chosen the constitutional approach to implementation of the Data Protection Directive[20] or have otherwise provided that their data protection laws are of a mandatory nature.[21] The courts and DPAs of these countries will in all probability apply their own rules as *ordre publique* which will be applied regardless of the applicable law.[22] In any event the rules in the Data Protection Directive regarding the DPAs and their duties, powers and decisions are typically of a public nature.

This being said, the Data Protection Directive provides that consent can be given by an individual for a data processing activity (that would otherwise be in violation of the provisions of the Data Protection Directive), and that data processing is allowed to the extent necessary for the performance of a contract to which the data subject is a party, which are both typically of a private nature.[23] The Data Protection Directive further provides for the possibility that a DPA takes enforcement action even if the law of another Member State is applicable to the relevant processing (which also suggests that the object matter is not of a public nature).[24] Finally, under most national implementation laws, claims for damages have to be brought before the civil courts (either based on tort or on enforcement of a right *sui generis*),[25] which is also typical for private law. The conclusion is that EU

civil and administrative liability rules in a country (as in Finland, France and Luxembourg) to liability in tort (as in Ireland and the Netherlands).

18 See n 10.

19 See Recitals 10 and 11 to the Data Protection Directive.

20 See Korff (Chapter 4, n 54). Korff lists the Member States (most notably Germany, Spain, Greece, Italy, Portugal and Austria) that have chosen the constitutional approach to implementation of the Data Protection Directive.

21 See for instance the legislative history to the Dutch Data Protection Act, Kamerstukken II 1997/98, 25 892, nr. 3, at 10.

22 Bing (n 15) at 3; Kuner (Chapter 6, n 8), at 11; and Kuner (n 15), at 10.

23 See Articles 7(a) and (b) Data Protection Directive.

24 See Article 28(6) Data Protection Directive: "each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with para. 3 (...)." These powers include the right to engage in legal proceedings where the national provisions have been violated.

25 Korff (Chapter 6, n27), Chapter 13, discussing the different legal bases on which damages can be claimed, varying from the ordinary rules on civil and administrative liability rules in a country (as in Finland, France and Luxembourg) to liability in tort (as in Ireland and the Netherlands).

data protection law is clearly a combination of the two categories, the logical consequence of which is that the different regimes (public vs private) should be applied concurrently depending on the relevant category.[26]

12.3.2 Do the conflict rules of the Data Protection Directive take precedence over PIL?

Given the mixed nature of EU data protection law, the question is whether the applicability and enforcement regime of the Data Protection Directive (the "conflict rules") take precedence over the general conflict rules of EU PIL or whether they are intended to supplement these.[27] EU rules of PIL provide that conflict rules in relation to specific matters which are contained in Community instruments or in national legislation harmonised pursuant to such instruments, take priority over the conflict rules under PIL.[28] The

---

[26] See Bing (n 15), at 3: "Data protection legislation will typically contain provisions of a public law nature, relating to an authority and its duties and decisions. But the law will also often include civil law provisions, typically on liability for data protection violations. The provisions of data protection legislation may therefore have to be qualified as belonging to different areas of law, to which different relevant connection criteria are assigned. Following the traditional method, different aspects of one case may then have to be decided by different *lex causae*, which easily may lead to distortions as the legislation is conceived as an organic whole where the different provisions support an appropriate solution." See also Kuner (n 15), at 10: "It thus seems preferable to conclude that data protection law should not be considered to be solely public law or private law, but that its characterization should depend on the specific activity or issue in question. Thus, if an action is taken by a data protection authority (for example, an enforcement action such as an audit), then this should be considered to be a matter of public law, but if action is taken by a private actor (such as signing a data transfer agreement with another private party), then it should be considered one of private law (albeit it with a strong regulatory element). There will be many situations when the public and private nature of data protection law become intertwined, and it may be difficult to distinguish between them in a particular case."

[27] The scope of a European Directive is determined by a one-sided applicability rule, i.e. a conflict rule that solely indicates the scope of the directive itself and does not provide a rule about the relation to possible applicability of other rules, see C.A. Joustra, "Europese richtlijnen en Internationaal privaatrecht" (European Directives and Private International Law), [1999] WPNR 6369, at 666, and references to other literature.

[28] See Article 23 of Rome I, and in particular recital 40 thereto and Article 67 Brussels I Regulation. See also L. Strikwerda, *Inleiding tot het Nederlands Internationaal privaatrecht* (Kluwer 2008), at 69, in respect of the predecessor of Rome I. According to Strikwerda, one-sided scope rules take precedence over general conflict-of-law rules as the national court addressed will apply the rules within scope, regardless of the applicable law. See also Cheshire,

conflict rules of the Data Protection Directive are "one-sided" to the extent that they provide the scope of the Data Protection Directive as to when the Directive applies and when the DPAs and courts have jurisdiction, rather than true conflict rules as to which regime takes precedence. However, given that the purpose of the Data Protection Directive is maximum harmonisation of data protection law within the EU,[29] the conclusion is justified that the applicability and jurisdiction regime of the Data Protection Directive should be considered to be conflict rules that take precedence over those in PIL.[30] The fact that the Data Protection Directive itself does not provide for this is not considered to be decisive in this respect.[31]

North & Fawcett, *Private International Law* (Oxford University Press 2008), at 737 (in particular footnote 621) and at 762 and Joustra (n 27), at 666.

29 See Recital 8 Data protection Directive, indicating that the purpose of the Directive is full harmonisation with the exception of specific discretionary powers in a limited number of areas. See further Joined Cases C-465/00, C-138, C-139/01 *Österreichischer Rundfunk/Neukomm* [2003] ECR I-04989, para. 100 and Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, paras. 95-96. See further the EC Communication on the revision of the Directive (Chapter 6, n 34), at para. 2.12.1, where the Commission announces it will "examine the means to achieve further harmonisation of data protection rules at EU level".

30 See also Blok (Chapter 2, (n 29), at 302-303. this is also the opinion of the Working Party 29, see Working Document on Non-EU Based Websites (Chapter 6, n 59), at 6: "as the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of so-called "rule of conflict" and no recourse to other existing criteria of international private law is necessary." See further Peter Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet' (1998) 32 International Lawyer 991, at 994: "Conflict of law rules in such legislation [the Data protection Directive] take precedence over national rules." and "the [Rome] Convention does not take precedence over choice of law rules that are included in European Union legislation".

31 See Blok (Chapter 2, (n 29), at 302 -303; and Joustra (n 27), at 666 (and further literature therein referred to). An example of an EU directive that provides for a conflict-of-law rule that is considered to take precedence over those in PIL, but that does not explicitly provides so, is Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services, OJ L 018, 1. The original proposal for Rome I explicitly acknowledged this Directive as one that contains a conflict-of-law rule which takes precedence over the conflict rules of Rome I, i.e. falls within the scope of Article 23 Rome I). See Article 22(a) original proposal Rome I and Annex I thereof, which was omitted in the final version. See Cheshire, North & Fawcett (n 28), at 762.

12.3.3 Choice of law and forum

The next question is whether the multinational can make a choice of law and forum in BCR which deviates from the applicability and jurisdiction regime of the Data Protection Directive. The answer to this question depends on whether the Directive should be considered to impose rules of mandatory law (or not). If the provisions (including the applicability and jurisdiction provisions) of the Data Protection Directive are of a mandatory nature, these cannot be deviated from by contract. Given the status of data protection as a fundamental human right and freedom[32], the (sometimes silent) assumption in the literature is that the Data Protection Directive is indeed of a mandatory nature.[33] The fact that the Directive itself does not provide that

---

[32] See n 10. The constitutional character of the right to data protection as opposed to the right to privacy is challenged by Peter Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (Boom Juridische Uitgevers 2002), in particular Chapter 3 and 5; see also Cuijpers (referring to Blok) (n 16), at 312.

[33] The scarce literature that does explicitly discuss the issue predominantly confirms the mandatory nature of the Directive: Blok (Chapter 2, (n 29), at 303; Lucas Bergkamp, *European community Law for the New Economy* (Intersentia 2003), at 123; Stefano Rodotà, "Data Protection as a Fundamental Right," in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 3; Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective*, diss. TILT (Boxpress, Oisterwijk), at 196-208. See also: Colette Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged?", SCRIPT-ed 4, no.4 (2007), at 306, which acknowledges that the general assumption in literature is that the Directive is of a mandatory nature. The arguments presented by Cuijpers are each discussed and (convincingly) rejected by Purtova (above), at 197 et seq. The main argument of Cuijpers (this n), at 311, is that the Directive cannot be of a mandatory nature as it facilitates the freedom to contract, e.g. where it provides that consent can be given by a data subject for a data processing and where it allows data processing to the extent necessary for the performance of a contract to which the data subject is a party. Cuijpers ignores that this 'contractual' legal basis for processing is strictly safeguarded by the Directive (i.e. is a 'controlled' legal basis for processing) and remains subject to the other protection provisions of the Directive like the principle of proportionality (see n 30). Further, Cuijpers ignores that 'consent' is a fundamental element of a rights-based approach to data protection. Consent comes into play if any act would otherwise be in violation of the consenting party's right. As Brownsword puts it: "Where a data protection regime is underwritten by an ethic of rights and where (as I take it) the ethic is based on a choice (or will) theory of rights, there is no escaping the fact that consent must be central to this regime. This is because, quite simply, consent is an integral dynamic within such rights-based approach." See Brownsword (Chapter 7, n 32), Chapter 3, at para. 4.2 (The Centrality of Consent). Further, on how the fundamental right to data protection safeguards data subjects and leads to the conclusion that consent has (and should have) a limited value as an

its provisions are of a mandatory nature is (again) not considered to be decisive in this respect.[34] Despite some (isolated) criticism of the mandatory nature of data protection,[35] it is not expected that this will change in the future. The status of data protection as a fundamental right and freedom has recently been strengthened by its implementation in the recently adopted Treaty on the Functioning of the European Union (**TFEU**).[36] Also, the recent EC Communication on the revision of the Directive[37] indicates that the Commission "building on these new legal possibilities [i.e. in TFEU] will give the highest priority to ensuring respect for the fundamental right to data protection throughout the Union". This EC Communication on the revision of the Directive further points strongly in the direction of further approximation of EU data protection laws and this at the highest level of the equation.[38] Data protection being a fundamental human right, the question is whether there is any room left for the freedom to contract, which is (also) a European fundamental right and freedom.[39] It is clear that according to the European Court of Justice (**ECJ**) the right to data protection 'is (...) not absolute but must be balanced against other fundamental rights'.[40] According to the ECJ such balancing is in the first place made in the

---

independent legal ground for data processing, see Rouvroy and Poullet (Chapter 7, n 31), at 72-76.

34 See (Chapter 2, (n 29), at 303. This refers to EU directives that cannot be deviated from by contract, but whereby the Directive itself does not explicitly provide so. Examples listed by Blok are the Directive 2003/33/EC, [2003] OJ L152 (Tobacco), and Directive 2001/83/EC, [2001] OJ L311 (advertising of pharmaceuticals. Again, for a different viewpoint, see Cuijpers (n 16), at 221 -222 and Cuijpers (n 16), at 304, where Cuijpers argues that the Directive does not impose mandatory rules of law based inter alia on the absence of a clause in the Directive prescribing mandatory law, this (a-contrario) referring to a number of directives which do contain clauses requiring the mandatory character of one or more of its provisions. That a-contrario arguments are often unreliable is evidenced by the foregoing examples given by Blok of directives that do not contain a clause requiring the mandatory character and yet do have a mandatory character.

35 Cuijpers (n 16), at 222-223; Cuijpers, (n 16), at 304.

36 See n 10.

37 See EC Communication on the revision of the Directive (Chapter 6, n 34), at para. 2.2.1. and 2.2.3.

38 See EC Communication on revision of the Directive (Chapter 6, n 34), at para 2.1, where the Commission states that it intends to strengthen the individuals' rights, by *inter alia* increasing transparency for data subjects, enhancing control over one's own data, strengthening the principle of data minimisation, and improving the modalities of exercise of the rights of access, rectification, erasure or blocking of data and ensuring informed and free consent.

39 See for example Joined Cases C-90/90 and C- 91/90 *Jean Neu* [1991] ECR I-3617 para. 13.

40 See Case C-275/06 *Promusicae* [2008] ECR I-271 paras. 63, 65 and 68. See also Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para. 79.

Directive itself and further by the adoption of the implementation laws by the Member States and their application by the national authorities.[41] The Commission also indicates in the EC Communication on revision of the Directive that "other relevant fundamental rights enshrined in the Charter (…) have to be taken fully into account while ensuring the fundamental right to the protection of personal data". [42] It is not clear whether the ECJ and the Commission intend to imply that (as these other fundamental rights are already taken into account when drafting the Directive and the implementation laws itself) there is little room left for (a further) balancing of the right to data protection against other fundamental rights,[43] or intend to indicate that in all cases a further balancing should be undertaken.[44] In any event it is clear that the conclusion should not be that the freedom to contract would have priority, as being the 'more important' right.[45] Rather the conclusion seems to be that the rights under the Data Protection Directive cannot be contracted away. At the most, in a specific case, the right to data protection has to be balanced against the freedom to contract and in weighing the interests in the particular case involved, priority may be given to one over the other. Applying this conclusion to the question of whether a choice of law and forum in BCR is possible, the outcome is that this is not

41 Case *Bodil Lindqvist* (n 40), para. 82: "The mechanisms allowing those different rights and interests to be balanced are contained, first in Directive 95/46 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for. Second, they result from the adoption, by the Member States, of national provisions implementing that directive and their application by the national authorities."

42 See EC Communication on the revision of the Directive (n 34), at 4.

43 See Rodotà (n 33), Chapter 3, at 80: "2. Being aimed at affording a strong protection to individuals, the right to data protection may not be considered as subordinate to other rights. It means we have to go beyond the simple balancing test technique, because the very nature of data protection as 'fundamental right' (Y.Poullet). 3. Accordingly, restrictions or limitations are only admissible if certain specific conditions are fulfilled, rather than merely on the basis of the balancing of interests. Article 8 of the Convention for the protection of human rights provides that 'there shall be no interference by a public authority with the exercise of these rights except such as is in accordance with the law and is necessary in a *democratic* society'."

44 As seems to be implied by Purtova (n 33), at 203.

45 See Rodotà (n 33), at 80: "Being aimed at affording a strong protection to individuals, the right to data protection may not be considered as subordinate to other rights. It means we have to go beyond the simple balancing test technique, because the very nature of data protection as 'fundamental right' (Y.Poullet)."; Purtova (n 33), at 203; Olha Cherednychenko, "EU Fundamental Rights, EC Fundamental Freedoms and Private Law," European Review of Private Law 1 (2006), at 36. Differently, see Cuijpers (n 11), at 306 and 317 who advocates that the freedom to contract takes priority over the right to data protection.

possible if this in any way diminishes the rights and remedies of individuals under the Directive. Only if such choice were not in any manner to lead to diminished protection, is there room for balancing the right to data protection against the freedom to contract. This requirement seems only to be met if a choice of the law of another Member State were made (than would apply pursuant to the regime of the Directive).[46] Due to the maximum harmonisation of the laws of the Member States, such choice would not in any way diminish the protection afforded by the Directive to data subjects. Balancing the two fundamental rights here could weigh in favour of the freedom to contract.[47]

A similar balancing may be made in case the **forum** of another Member State is chosen. Again, given the high level of harmonisation, the data protection afforded to individuals should not be diminished if another DPA were competent. As all DPAs have a duty to cooperate in the enforcement, this entails only a shift in which DPA takes the lead in enforcement. As to jurisdiction of the courts of the Member States, the Data Protection Directive provides that "decisions by the DPAs may be appealed against through the courts". It is left to the Member States to provide for the jurisdiction rules of their courts in data protection cases and most Member States have not enacted special rules, but rely on their civil procedural law (which are primarily determined by EU rules of PIL). Under these rules a choice of forum is in principle possible.[48] Again, as with a choice of law, it seems that the protection afforded to data subjects would not be diminished if a choice of forum could be made for the DPA and the courts of another Member State.

It should be noted that even if a choice of law and forum is possible, such agreement will be valid only between the parties that have agreed. As a DPA

---

46 This is assuming that the Data Protection Directive does indeed provide for the highest level of data protection overall.

47 Blok (Chapter 2, (n 29), at 303 is of the opinion that due to the mandatory nature of the Directive, a choice of law is not possible, but in general comments that the outcome could be different if the law chosen to apply is the law of another Member State, since in that case the data protection afforded to the data subject should not be diminished given the full harmonisation of data protection law across the EU. Cuijpers (n 16) at 317, also comes to the conclusion that a choice of law is possible, but this is based on the starting point that the Directive is not of a mandatory nature and that therefore deviation by a choice of law should as a rule be possible.

48 See Article 23 Brussels I Regulation. This freedom is not unlimited. Specific requirements apply for contracts with weaker parties, such as employees and consumers and further requirements apply as to form. These are discussed in para. 12.6 below.

is not a party to such agreement, and may therefore ignore the choice of another DPA and further any obligation the controller has vis-à-vis the DPA will remain in place (such as notification duties, the obligation to appoint a representative on EEA territory if the controller is established outside the EEA, permit requirements, etc).[49]

Further, any such choice of law and forum will be subject to general rules of PIL. For instance, Article 3(4) of Rome I provides that if the law of a non-Member State is chosen (e.g. to avoid the protection afforded by the Data Protection Directive), while all other elements relevant to the situation at the time the choice is made are located in one or more Member States, "the parties' choice of applicable law other than that of a Member State shall not prejudice the application of provisions of Community law (…), which cannot be derogated from by agreement."[50] In other words, according to PIL a choice of law will be possible, but does not set aside mandatory provisions of Community law.[51]

Based on the above, the conclusion is that there are good arguments that a choice of law and forum should be possible in respect of data protection, provided the law and forum of another Member State are chosen. This conclusion seems to be in line with rules of PIL "as a mechanism" as well as with the underlying choices in the European PIL instruments (whereby a choice of law of another state is possible as long as the protection provided for by Community law is not set aside). In the context of BCR the law chosen should preferably be the law of the Lead DPA, this being the law under which the BCR are drawn up. As to forum, this should preferably also be the Lead DPA and the courts of the country of the Lead DPA. Besides the fact that this DPA reviewed and approved the BCR (which ensures a uniform interpretation of the BCR also in future disputes), the (EU) Delegated Headquarters is also established in that country, which will ensure optimal enforceability of the BCR.

---

49 Blok (Chapter 2, (n 29), at 303; and Cuijpers (n 16), at para. 6.6.5.

50 Article 3(3) Rome I further provides that if the law of one country is chosen,, while all other elements relevant to the situation at the time of choice are located in a different country, the choice of the parties shall not prejudice the application of the law of that other country. This provision is less relevant to the processing of data by multinationals, as such processing will in most cases be of a cross-border nature and therefore involve more countries.

51 Article 3(4) Rome I, is a codification of case law of the ECJ. For an overview of prior case law, see Cheshire, North & Fawcett (n 28), at 737. See further Strikwerda (n 28), at 67. Such a choice of law and forum would further have to comply with the employee and consumer protection regime of Rome I and the Brussels I Regulation, see para. 12.6 below.

Given the identified uncertainties as to whether indeed a valid choice of law and forum can be made in respect of data protection (even if limited to the rights and remedies of a private nature and limited to a choice of law and forum of one of the Member States), I recommend that European legislators ensure that in BCR such choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA and further that the Lead DPA will have central supervision in respect of such BCR, and may involve other DPAs if so required for enforcement on the territories of the other Member States. If European legislators were to introduce the country-of-origin principle also for data protection (as per *Recommendation 1)*[52], it would seem that the possibility of a choice of law and forum would no longer be necessary as in that case the data processing operations of the multinational would already be governed by the data protection laws of the Member State of origin of the multinational. However, as BCR apply to the data processing operations of the multinational on a worldwide basis (i.e. also to data processing operations not governed by the EU data protection laws), the possibility of a choice of law and forum remains relevant for such non-EU data processing operations.

Recommendation 9
Provide that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA and further that the Lead DPA have central supervision in respect of such BCR, and may involve other DPAs if so required for enforcement in the territories of the other Member States.

If this Recommendation is followed, a multinational having BCR would have to comply with the data protection law of one Member State only. This is certainly an improvement compared to the present situation in which the applicability regime of the Data Protection Directive is based on an accumulation of applicable data protection laws of the Member States.[53] However, ultimately multinationals would be best served if they could apply one uniform data processing regime on a global basis. In other words, they would be best served if they could apply the BCR regime on a global basis, **including in the EU**. I do not see any convincing reason why this would not be acceptable to EU legislators. At present, the multinational applies the laws of the Member States in the EU and the BCR outside the EU. If data

[52] See para. 8.4.3.

[53] See para 2.3.6.

originating from the EU are transferred to a non-adequate country, the protection such data obtain is that of the adequate level provided for by the BCR. If it is acceptable that EU data obtain an adequate level of protection outside the EU, this adequate level of protection should also be acceptable for protection of EU data within the EU. It is more a matter of setting the right level for adequacy, and in that sense the general assumption that the level of data protection provided by the Data Protection Directive is the highest (or in any event higher than an "adequate level" of a protection) is something of a myth. The material processing rules under the Data protection Directive and those under countries that obtained an adequacy ruling are in most cases approximately the same. If the Data Protection Directive is considered stricter, this often concerns more formal requirements like timeframes for responding to requests of individuals, notification and permit requirements, etc. Multinationals implementing IT systems processing data on a cross-border basis verify compliance with these material data processing rules. The actual protection afforded to individuals is in the tuning of these systems (what data are processed, access controls, decisions on security). Subsequent notification of these processing operations to the DPAs, or a 10-day instead of a 4-week period to reply to access requests, do not provide additional material protection to individuals. These are "national hurdles" to take. Some of this thinking can be recognised in the various opinions and recommendations made in respect of the revision of the Directive. These all focus on "privacy by design"[54], on enforcement ex-post to the detriment of requirements ex-ante like notification, permit requirements[55], and "specify the criteria and

[54] See the Rand Report (Chapter 6, n 27), at 44 and the WP Contribution on the Future of Privacy (Chapter 6, n 33), at para. 4 at 12 et seq., urging the Commission to introduce 'privacy by design' as a new principle in the revised Directive. The EC Communication on the revision of the Directive (Chapter 6, n 34), at 12, states the Commission's intent to "further promot[e] the use of PETs and the possibilities for the concrete implementation of the concept of 'Privacy by Design'"; and the EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at paras. 108-115 et seq.

[55] The Rand Report (Chapter 6, n 27), at para. 3.3.2 at 28, concludes that the ex-ante measures to ensure transparency of processing via information and notification requirements are largely ineffective. See also the WP Contribution on the Future of Privacy (Chapter 6, n 33), at 21, where the Working Party 29 advocates a simplification or reduction of the notification requirements, also because the accountability principle would achieve the same purposes. The EC Communication on revision of the Directive (Chapter 6, n 34), at 10, pleads for "simplification" of the current notification regime. In a recent speech, Neelie Kroes, the Vice-President of the European Commission responsible for the Digital Agenda, compares the notification requirement to a "formality," see "Towards a European Cloud Computing Strategy", speech for World Economic Forum Davos, 27 January 2011, available at http://europa.eu). The

requirements for assessing the level of data protection in a third country or an international organisation" and further "to define core EU data protection elements, which could be used for all types of international agreements."[56] If the protection in BCR is indeed set at the required adequacy level (and includes all core EU data protection elements), there are no objections to applying the provisions of the BCR also within the EU instead of the data protection laws of the Member States.

Recommendation 10
Provide that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States.

12.4 The applicability, supervision and enforcement regime of BCR: how it may work

At this time it is uncertain whether a choice of law and forum may be made in BCR (hence *Recommendation 9*), and further whether in the EU the BCR rules may be applied instead of the national laws of the Member States (hence *Recommendation 10*). Hereafter I discuss how the applicability and enforcement regime of BCR may currently be best set up (i.e. in the situation that these recommendations are not implemented). At present, multinationals are best advised to set up the applicability and enforcement regime of BCR in such a manner that the pitfall of deviation from the mandatory applicability and enforcement regime of the Data Protection Directive is avoided. However, even if the applicability and enforcement regime is set up in such a manner, some PIL issues remain. Below I first discuss how the applicability and enforcement regime may be best set up (Paragraphs 12.4.1 - 12.4.3) and thereafter I discuss whether this applicability and enforcement regime (if drafted as suggested), is indeed valid and binding under rules of PIL and in particular the employee and consumer protection regime thereof (Paragraphs 12.5 - 12.10).

12.4.1 How should the applicable law regime be set up under BCR?

The BCR should not provide for a **minimum** protection where the applicable national data protection rules apply only if they provide for

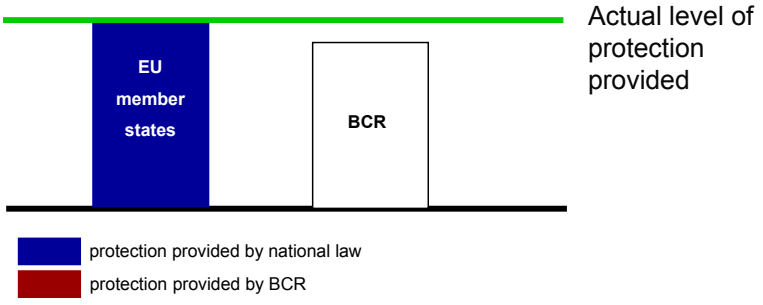
EDPS Opinion on the revision of the Directive (n 35), at para. 62 at 15, supports the initiative to restrict application of the notification obligation to processing operations that are expected to bear more risk of violation.

[56] EC Communication on the revision of the Directive (Chapter 6, n 34), at 16.

more data protection, but rather the reverse. The BCR should provide that any processing by the multinational of personal data will remain governed by applicable national law and that the BCR provide for **supplemental** protection only. In other words, the BCR apply only if the BCR contain rights or remedies that go beyond those provided by applicable national law. If rights and remedies are equal under national law and the BCR, national law prevails. The BCR therewith does not provide for a minimum protection, but provides a "top on" protection until an adequate level of data protection is achieved. The scope of applicability of BCR is illustrated by the following examples.

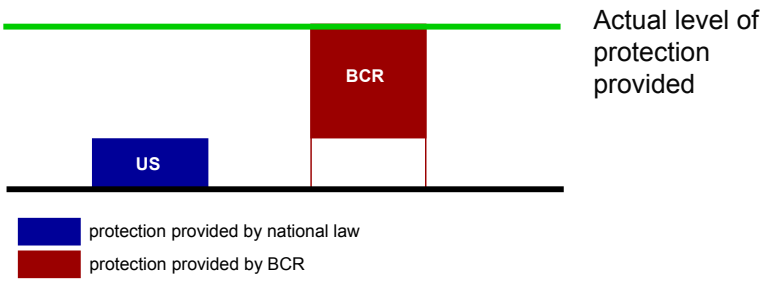
Example 1

- National law provides more protection than the BCR (e.g. in the EU)



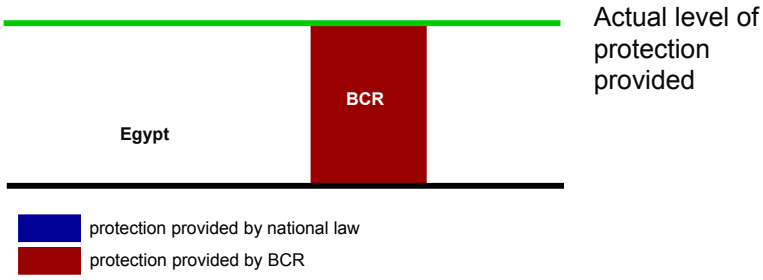
Example 2

- National law provides some protection, BCR provide supplemental protection (e.g. in the US)



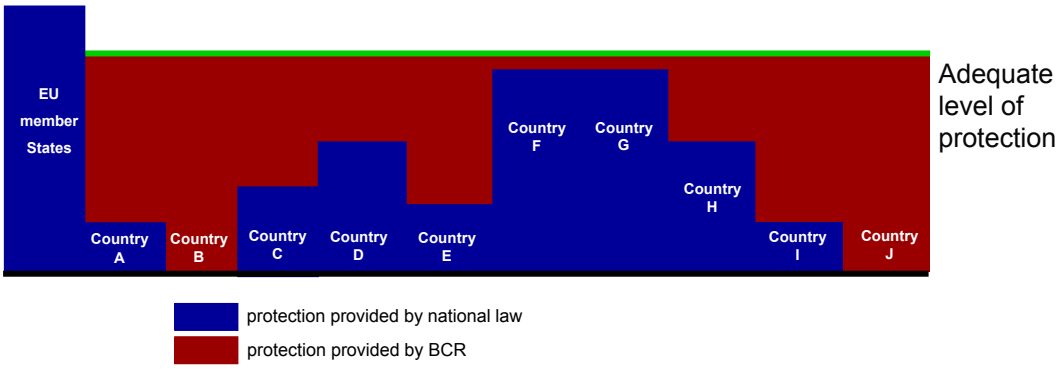
Example 3

- National law provides no data protection (e.g. in Egypt)



Example 4

- BCR provide a 'top on' or 'blanket of protection' to ensure an adequate level



As the BCR do not contravene the applicability regime of the Data Protection Directive, since it provides for supplemental rights in jurisdictions only (which are not governed by the Data Protection Directive), a choice of law in respect of this supplemental protection would seem to be a valid option.

12.4.2 How should the enforcement regime for BCR be set up?

In line with the choice of the law of the Lead DPA, also a choice should be made for the forum of the DPA. As a consequence any complaints and claims of an individual concerning any **supplemental** rights granted under the BCR may be brought by the individual against the (Delegated) EU Headquarters.

Again, as under BCR individuals keep their own rights and remedies, the BCR do not contravene the enforcement regime of the Data Protection Directive and a choice of forum would seem to be a valid option.

12.4.3 How should supervision of BCR be set up?

To ensure central supervision by the Lead DPA, the BCR could provide that the BCR will be supervised by the Lead DPA only. This is a clear deviation from the requirements listed in the WP Opinions (see Paragraph 10 above), which prescribe that in respect of the BCR, all group companies should have a duty to cooperate with all DPAs and abide by their advice regarding the BCR and submit to their audits.[57] There is no valid reason for the Working Party 29 to require that indeed all DPAs have rights of supervision and auditing in respect of BCR. After all, as the individuals retain all their rights and remedies under applicable national law, the BCR do not take away any existing jurisdiction, supervision or enforcement powers from the DPAs. This requirement of the Working Party 29 seems to be inspired more by the wish of certain DPAs not having audit rights under their national law,[58] to remedy that inadequacy rather than by a legitimate concern for proper supervision of BCR. Such supervision is adequately addressed by granting the Lead DPA central supervisory and enforcement powers (including full audit rights) in respect of BCR (as per *Recommendation 9*).[59] As it is the expectation that the lack of proper harmonisation of enforcement powers of the DPAs will be addressed in the revised Directive[60] (see *Recommendation 5*), this requirement of the Working Party 29 will probably solve itself.

If the BCR are drafted as suggested, the question arises whether such choice of law and forum clauses in BCR are indeed valid and binding under applicable EU rules of PIL and in particular the employee and consumer

57 The WP Opinions require an obligation to of the group companies to cooperate with all DPAs, abide by their advice in respect of the BCR, and accept to be audited by the DPAs.

58 Which is, for instance, the case in the UK.

59 The Dutch DPA (acting as Lead DPA) has approved BCR that contain central supervision (including auditing) by the Lead DPA only.

60 See para. 10.6.

protection regimes of these rules. First a short overview is given of the relevant provisions of EU PIL concerning choice of law and forum clauses in employee and consumer contracts.

12.5 Choice of law and forum

12.5.1 Employee contracts

Insofar as applicable law is concerned, Article 8(1) of EC Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations (**Rome I**)[61] provides that an individual employment contract will be governed by the law chosen by the parties. However, such choice of law may not have the result of depriving the employee of the protection afforded to him by the mandatory rules of the labour law which would be applicable in the absence of a choice of law clause (i.e. the mandatory provisions of the labour law of the place where he habitually carries out his work). A choice of another law in the employment contract cannot set aside these mandatory provisions to the detriment of the employee.

As far as a choice of forum is concerned, Article 21(2) of EC Regulation 44/2001 of 22 December 2000 on jurisdiction and enforcement (**Brussels I Regulation**)[62] provides that a choice of forum clause is valid only if it **allows** the employee to bring proceedings before a court or courts other than those indicated in Article 19 Brussels I Regulation (being the courts of the place where the group company is domiciled or the courts of the place where the employee habitually carries out his work). In other words, choice of forum clauses in employee contracts may only **add** a competent court and any agreement to the contrary will have no legal force.[63]

12.5.2 Consumer contracts

For consumer contracts, more or less similar rules apply as to employee contracts. As to a choice of law clause in a consumer contract, Article 6(2) Rome I provides that the consumer may always rely on the mandatory rules of the law of his habitual residence, and to that extent set aside a choice of law clause referring to another law. Further, pursuant to Article 17(2) Brussels I a choice of forum clause in a consumer contract is also valid only if it **allows** the consumer to bring proceedings before another court than those indicated in Article 16(1) Brussels I Regulation (being the courts of the place where the group company is domiciled or the courts of the place where the consumer is domiciled). Also in consumer contracts a choice of forum

61 [2008] OJ L177/6.

62 [2001] OJ L12/1.

63 Article 23(5) Brussels I Regulation,

clause may therefore only add a competent court and any agreement to the contrary will have no legal force.[64]

A prerequisite for applying the above rules is that the contract is entered into by the company while it (i) pursues its commercial activities in the Member State where the consumer has his habitual residence or (ii) directs such activities (also) to that Member State, in both cases provided the contract falls within the scope of such activity. [65]

A general requirement for all choice of forum clauses is that an "agreement conferring jurisdiction" must be either in writing or evidenced in writing (Article 23(1)(a) Brussels I Regulation).

12.6 Relevance of Rome I and the Brussels I Regulation for BCR

The limitations in respect of choice of law and forum clauses in employee and consumer contracts as set out above, may well be of relevance to the choice of law and forum clauses in BCR.

BCR for Employee Data. The requirement in the WP Opinions that the BCR be internally binding within the organisation of the multinational (i.e. on all group companies and on employees) and externally binding for the benefit of the employees (must create rights for employees) will in many cases be complied with by the multinational by making the BCR binding on employees. In this case there is little doubt that the employee protection regimes of Article 8(1) Rome I and Articles 19 and 21(2) Brussels I Regulation apply (**employee protection regime**).

BCR for Customer Data. The requirement in the WP Opinions that the BCR be externally binding for the benefit of the consumers may be complied with by the multinational making the BCR part of the individual consumer contracts by including a clause to that effect. Also in that case, there is little doubt that the consumer protection regimes of Article 6(2) Rome I and Articles 16 and 17(2) Brussels I Regulation apply (**consumer protection regime**).

However, also if the BCR are **not made part** of the individual employee or consumer contracts, it cannot be excluded that the employee and consumer protection regime under Rome I and the Brussels I Regulation may be of relevance. Even if the BCR are **not made part** of the individual contracts,

---

64 Article 23(5) Brussels I Regulation.

65 Article 6(1) Rome I and Article 15(1)(c) Brussels I Regulation.

the BCR will in most cases still be closely connected to these employee or consumer contracts, if only for the reason that the data processed under the BCR are (in most cases) processed by the multinational in the context of the performance of these contracts. Employee data will be processed for salary payment purposes or for employee performance evaluation purposes; consumer data are processed for administering the purchase orders, delivery and payment under the consumer contracts, etc. This entails the risk that these data will be considered processed (also) as part of the individual employment or consumer contract and that any choice of law or forum clause in this respect (though being part of the BCR) should be subject to the employee and consumer protection regimes (**assumption 1**).

Multinationals under their BCR also process data of individuals with whom they have not (yet) entered into an employee or consumer contract. Examples are data processed by the multinational of job applicants and prospective customers. Most companies have a database with current and potential job applicants and further extensive marketing databases with data of potential customers. With all these individuals no employee or consumer agreement is in place. The marketing databases further contain the data of their existing customers, which data are not necessarily just processed in the performance of the respective consumer contracts but will also be processed to market other products or services of the multinational. However, also in those cases the processing of data still seems to be very closely connected with the (potential) contracts to be concluded (i.e. data of job applicants are processed with a view to entering into an employment agreement and data of prospective customers are processed with a view to entering into a consumer agreement). From a protection perspective[66] it may be argued that it is logical to apply the employee and consumer protection regimes also to these cases (**assumption 2**).

Below I will evaluate whether these assumptions are correct. In summary, an evaluation of the case law of the ECJ does not per se support assumption 1 and in any event does not support assumption 2. Taking as a starting point that the employee and consumer protection regimes should be interpreted restrictively, the conclusion will be that these regimes should not apply to BCR. First however, the requirements for applicability of the employee and consumer protection regimes will be discussed.

For applicability of both the employee and the consumer protection regimes under both Rome I and the Brussels I Regulation, it is required that a

[66] The protection element is explicitly expressed in Recital 13 of Brussels I Regulation and Recitals 23 and 24 of Rome I.

"contract is concluded" with the employee or consumer or that it is "a matter relating to such contract". These requirements are most extensively dealt with by the ECJ in its case law concerning the consumer protection regime in respect of forum clauses under the Brussels I Regulation. As the substantive scope and the provisions of Rome I, Rome II and the Brussels I Regulation are intended to be aligned to ensure consistency, this case law is also of relevance to choice of law clauses under Rome I.[67]

[67] Recital 7 of Rome I provides that the substantive scope and provisions of Rome I should be consistent with the Brussels I Regulation and Rome II. Recital 7 of Rome II contains a similar statement. Recital 24 of Rome I further indicates that the conditions for applying the consumer protection rule are brought in line with those of the Brussels Convention to ensure consistency, and Recital 24 of Rome I states that for Article 15(1) Rome I to be applicable, since "it is not sufficient for an undertaking to target its activities to the Member State of the consumer's residence or at a number of Member States including that Member State; a contract must also be concluded within the framework of its activities." For the reverse situation, see Case 9/87 *Arcado* [1988] ECR 1988 01539, para. 15, where the ECJ, in a judgment concerning the interpretation of Article 5(1) Brussels Convention, in its turn refers to the scope of Article 10 (of the predecessor of) Rome I ([1980] OJ L266/1). The fact that the concepts under Rome I, Rome II and the Brussels I Regulation should be aligned does not mean that they are by definition identical in all cases. Concepts in all PIL instruments should be understood autonomously. It has been repeatedly held by the ECJ that the concepts used in the Brussels Convention – and in particular those featured in Article 5(1) and (3) and Article 13 – must be interpreted independently, by reference principally to the system and objectives of this regulation, in order to ensure that it is uniformly applied in all contracting States. On this, see in particular: Case C-27/02 *Engler* [2005] ECR I-481, para. 33; Case 150/77 *Bertrand* [1978] ECR 1431, paras. 14, 15 and 16; Case C-89/91 *Shearson Lehman Hutton* [1993] ECR I-139, para. 13; Case C-269/95 *Benincasa* [1997] ECR I-3767, para. 12; Case C-99/96 *Mietz* [1999] ECR I-2277, para. 26; and Case C-96/00 *Gabriel* ECR I-6367, para. 37). Further, Recital 11 of Rome II states that the concept of a non-contractual obligation varies from one Member State to another and that therefore this concept should be understood to be autonomous. Rome I and II must be construed together so that the scope of each other excludes the other. An obligation is either contractual (and covered by Rome I) or non-contractual (and covered by Rome II): see John Ahern & William Binchy, *The Rome II Regulation on the Law Applicable to Non-contractual Obligations: a new international litigation regime* (Martinus Nijhoff Publishers 2009), at 60 (Chapter 'The Scope of 'Non-Contractual Obligations" by Andrew Scott). If the concept of non-contractual obligations under Rome II is to be construed autonomously, this will by definition also apply to the concept of contractual obligations under Rome I.

12.6.1 Contract concluded

The ECJ ruled that applicability of the consumer protection regime under the Brussels Convention[68] (the predecessor of the Brussels I Regulation)[69] requires a 'contract concluded' by a consumer 'for the supply of goods or a contract for the supply of services' (*Engler*).[70] The ECJ further ruled that the specific rules for jurisdiction in consumer an employee contracts in the Brussels Convention[71] constitute **a derogation** from the basic rule of the Brussels Convention,[72], which confers jurisdiction on the courts of the contracting state in which the defendant is domiciled. According to the ECJ (referring to its settled case law[73]), these specific rules of jurisdiction must give rise to a **strict interpretation** which cannot go beyond the cases envisaged by the Brussels Convention **and in all cases require a contract concluded by the consumer or employee.**[74]

In *Engler*, a professional vendor sent a letter on its own initiative to the consumer's domicile, without any request by her, designating her by name as the winner of a prize. Though the letter included a catalogue and order form, no contract was concluded. The ECJ held:

> "Although it is indisputable that in a situation of that kind the claimant in the main proceedings is a consumer covered by the first paragraph of Article 13 of the Brussels Convention and that the vendor made contact with the consumer in the manner provided for in point 3(a) of that provision, by sending her a personalised letter containing a prize notification together with a catalogue and an order form for the sale of its goods in the Contracting State where she resides in order to induce

---

68 See Article 13(3) Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, [1972] OJ L299/31 at 32, as amended by Conventions on the Accession of the New Member States to that Convention, consolidated text [1998] OJ C27/1.

69 See Article 16 Brussels I Regulation. The Brussels I Regulation should be interpreted in the light of the case law decided under the Brussels Convention, see the opinion of the A-G Leger in Case C-281/02 *Owusu* [2005] ECR I-1383.

70 Case C-27/02 *Engler* [2005] ECR I-481. This case concerned a letter personally addressed to an Austrian national (Ms Engler) and sent by a German mail order company, which gave Ms Engler the impression that she had won a prize.

71 As provided for in Articles 13 to 15 of the Brussels Convention, currently Articles 16 and 19 of the Brussels I Regulation.

72 Article 2 first para. Brussels Convention.

73 See, in particular, Case 150/77 *Bertrand* [1978] ECR 1431, para. 17; Case C-89/91 *Shearson Lehman Hutton* [1993] ECR I-139, paras. 14 to 16; Case C-269/95 *Benincasa* [1997] ECR I-3767, para. 13; and Case C-99/96 *Mietz* [1999] ECR I-2277, para. 27.

74 Case C-27/02 *Engler* [2005] ECR I-481, para. 43

> her to take up the vendor's offer, the fact remains that in this case the vendor's initiative was not followed by the conclusion of a contract between the consumer and the vendor for one of the purposes referred to in that provision and in the course of which the parties assumed reciprocal obligations. It is common ground that, in the case in the main proceedings, the award of the prize allegedly won by the consumer was not subject to the condition that she orders goods from Janus Versand and no order was in fact placed by Ms Engler. Furthermore, it does not appear anywhere in the file that, by claiming the award of the promised 'prize', Ms Engler assumed any obligation towards that company, even by incurring an expense in order to obtain the award of the prize. In those circumstances, an action such as that brought by Ms Engler in the case in the main proceedings cannot be regarded as being contractual in nature for the purposes of Article 13, first paragraph, point 3, of the Brussels Convention. Contrary to the submissions of Ms Engler and the Austrian Government, that finding is not invalidated by the objective underlying that provision, namely to ensure adequate protection for the consumer as the party deemed to be economically weaker, or by the fact that, in this case, the letter was sent by Janus Versand to the consumer in person accompanied by a claim form entitled 'request for trial without obligation' and clearly intended to induce her to place an order for goods sold by that company. As is apparent from its wording, Article 13 clearly covers a 'contract concluded' by a consumer 'for the supply of goods or a contract for the supply of services'."

In 2009, the ECJ expanded on this ruling in respect of the consumer protection regime under the Brussels I regulation (*Ilsinger*).[75] The facts in *Ilsinger* were identical to those in *Engler*, but for the fact that the consumer had in fact placed an order for goods with the vendor although this was not a condition for being awarded the prize. The ECJ explicitly held that its earlier case law in respect of Article 13 Brussels Convention was still valid as the clauses (Article 13 Brussels Convention and Article 15 Brussels I Regulation) both contain a similar requirement for the conclusion of a consumer contract. The ECJ, however, subsequently held that Article 15 Brussels Convention did apply in the case at hand as now the requirement of a consumer contract was being met (as evidenced by the placement of the order by the consumer).[76] The consumer could rely on the protection regime and initiate proceedings before the court of her own country. This is noteworthy as the promise of the prize by the vendor was a **unilateral**

---

[75] Now in respect of Article 15 Brussels I Regulation, the successor to Article 13 Brussels Convention. See Case C-180/06 *Ilsinger*, [2009] OJ C153/3, para. 58.

[76] See Case C-180/06 *Ilsinger*, [2009] OJ C153/3, para. 59.

undertaking which was not tied in with a requirement for the ordering of the goods.

12.6.2 Matters relating to a contract

The employee and consumer protection regimes further apply "in matters relating to" an employee or consumer contract. According to the ECJ "matters relating to a contract" means that the claim must be contractual in nature but extends to claims "which are so closely linked to the employee or consumer contract as to be indivisible".[77]

12.6.3 Application of ECJ case law to BCR

Based on the case law above, it may well be argued that even if the BCR for Customer Data are not made part of the individual consumer contracts, the consumer protection regime is applicable to the BCR. Though the BCR are in that case a unilateral undertaking independent from a consumer contract, it may be argued that the protection regime would apply from the moment the company indeed enters into a consumer contract with a consumer (however, still not in case no contract is entered into with the consumer). A similar argument can be made as to BCR for Employee Data. Even if the BCR are not made part of an employment agreement, it may be argued that the employee protection regime applies from the moment the company indeed enters into an employment agreement. Further, if indeed an individual employment contract or consumer contract is concluded, it can easily be argued that the processing of data of the relevant employee or consumer is "a matter relating" to such contract.

The arguments against this conclusion are that the data protection rights under the Data Protection Directive are to be enforced under national data protection law (or tort law)[78] and therefore are in themselves not contractual in nature. Further, the BCR do not relate to the individual employee or consumer contract as the BCR apply **irrespective** of whether an employee or consumer contract is concluded. The BCR contain general undertakings by a multinational to process data of **any individual** the company has dealings with. As indicated, besides employees and consumers with whom the multinational has actually entered into a contract, the BCR also apply to the processing of data of job applicants, ex-employees, independent contractors, contact persons of corporate customers of company, its suppliers or other business contacts as well as of individuals who take part

77 Cheshire, North & Fawcett (n 28), at 268 and ECJ case law listed in footnote 268.

78 The legal basis for enforcement of data protection rights varies per Member State. See Chapter 8, n 23.

in research projects or pilots undertaken by the company and to marketing data of consumers who may be interested in products or services of the company.
Further, the distinction that can be made with *Ilsinger* is that there the promise by the vendor to the consumer was made on an **individual basis** and was closely connected with the contract entered into (was intended to entice the consumer into entering into the relevant contract). At first glance this seems an artificial distinction, but in future case law of the ECJ this may well prove to be decisive. BCR are not directed specifically to an individual consumer to entice that consumer into a contract. That this may be a relevant distinction is supported by the employee protection regime which specifies explicitly that it applies to **individual** (as opposed to collective) employee contracts only.[79] The general opinion is that agreements between employer and employee or employee representatives do not qualify as such nor collective employment contracts and also not employee regulations and collective regulations (even if made on behalf of or for the benefit of the employees), unless these are made a part of the individual contracts.[80]

Taking as a starting point that the employee and consumer protection regimes should be interpreted restrictively, the conclusion should be that these regimes do not apply to BCR. This conclusion is further supported by the fact that BCR (providing for supplemental protection only) do not take away any rights or remedies related to the employee and consumer contracts. All rights and remedies of employees and consumers under applicable law remain in place. The choice of forum clause in the BCR is meant to provide a forum to enforce **additional** rights and remedies (above any existing national rights and remedies) which the BCR may grant. Since this forum clause is not meant to **take away** any dispute settlement mechanisms which are available under applicable national law, the choice of forum clause does not seem to run contrary to the underlying protection objectives of the PIL regimes for employment and consumer relationships. In fact such choice of law and forum may well lead to improved redress.

---

79 Article 18 Brussels I Regulation. The element 'individual' is not included in the provision in respect of the consumer protection regime. However, the text of Article 15 Brussels I Regulation clearly applies to individual consumer agreements "in matters related to a contract concluded by a person, the consumer, (…)." The specific insertion of the element 'individual' in the provision of the employee protection clause functions to make it clear that collective employment agreements are excluded, which inclusion is not required in the consumer protection clause as there is no equivalent concept for consumer contracts.

80 Report Jenard/Moller, [1990] OJ C189/77, para. 60. P.H.L.M. Kuypers, *Forumkeuze in het Nederlands internationaal privaatrecht* (Kluwer 2008), at 468.

It is clear that this is still an open issue which ultimately has to be decided by the ECJ. It is therefore recommended that European legislators provide that in BCR (as to the supplemental protection provided by the BCR) a choice of law and forum may be made. As this is already a (sub) part of *Recommendation 9*, this does not lead to a separate recommendation here.

12.6.4 Relevance of Rome II?

If the consumer and employee protection regimes of Rome I do not apply as there is no employee or consumer contract, the question may arise whether the choice of law clause in the BCR should then be decided based on EC Regulation 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (**Rome II**).[81] Rome II also contains employee and consumer protection regimes as to a choice of law in respect of non-contractual obligations vis-à-vis employees or consumers. At first sight Rome II may seem applicable as in many jurisdictions a breach of data protection qualifies as a tort. However, also in this event a choice of law in BCR will be decided based on Rome I, this to the detriment of Rome II.[82] Again, a parallel should be sought with the case law of the ECJ in respect of the employee and consumer protection regime under the Brussels Convention. In *Engle*r, the ECJ held that the consumer protection regime was not applicable as there was no contract concluded, but subsequently ruled that this did not automatically entail that the action is not contractual in nature for purposes of Article 5(1) Brussels Convention. In *Engler* the ECJ had to decide whether the claim for the prize promised in the letter sent by the vendor should subsequently be considered as being **contractual in nature** for the purposes of Article 5(1) or as being **tortuous for purposes** of Article 5(3) Brussels I Regulation:

> "It follows that the finding made in paragraphs 38 and 44 of the present judgment that the legal action brought in the main proceedings is not contractual in nature for the purposes of the first paragraph of Article 13 of the Brussels Convention does not in itself prevent that action from relating to a contract for the purposes of Article 5(1). In order to determine whether such is the case in the main proceedings, it must be observed that it is clear from the case-law, first, that although Article 5(1) of the Brussels Convention **does not require** the conclusion of a contract (…)."

From this case and other case law of the ECJ it may be derived that the ECJ gives a very broad meaning to what constitutes a "contractual obligation"

---

81 [2007] OJ L 99/40.

82 Rome I and Rome II must be construed together, see n 67.

under Article 5(1) Brussels I Regulation. For Article 5(1) Brussels I Regulation to apply, "the establishment of a legal obligation freely consented to by one person towards another and on which the claimant's action is based" is sufficient.[83] It is therefore **not** required that a contract be concluded; an obligation freely assumed by one party towards another is sufficient.[84] An example of a unilateral undertaking that the ECJ considers qualifying as an "obligation freely assumed" is *Engler*, which concerned the letter sent by the professional vendor on its own initiative to the consumer's domicile, without any request by her, designating her by name as the winner of a prize. The ECJ decided that such a letter, sent to addressees and by the means chosen by the sender solely on its own initiative, constituted an obligation 'freely assumed'. The ECJ further held that:

> "as the addressee of the letter expressly accepted the prize notification made out in her favour by requesting payment of the prize, at least from that moment, the intentional act of a professional vendor in circumstances such as those in the main proceedings must be regarded as an act capable of constituting an obligation which binds its author as in a matter relating to a contract."

In line with the above case law, there seems little doubt that the unilateral undertakings contained in BCR qualify as "freely assumed" and will constitute contractual obligations, this at least from the moment that the BCR are enforced by an employee or consumer, as this will constitute acceptance. The consequence is that a choice of law made by the multinational in BCR should be assessed based on Rome I rather than Rome II.[85]

12.7 Summary conclusion re: applicability of employee and consumer protection regimes

---

[83] Case C-27/02 *Engler* [2005] ECR I-481, para. 51; Case C-26/91 *Handte* [1992] ECR I-3967, para. 15; Case C-51/97 *Réunion européenne and Others* [1998] ECR I-6534, para. 17; Case C-334/00 *Tacconi* [2002] ECR I- 7357, para. 23; and Case C-265/02 *Frahuil* [2004] ECR I-0000, para. 24.

[84] Case C-334/00 *Tacconi* [2002] ECR I- 7357, para. 22.

[85] For a similar conclusion based on an analysis of the various definitions of contractual obligations in the contracting states prior to the above ECJ case law, see Richard Plender, *The European Contracts Convention, The Rome Convention on the Choice of Law for Contracts* (Sweet & Maxwell 1991), at 51 and footnote 11. Plender also concludes that an obligation may be contractual for the purposes of the Rome Convention, although the forum characterises the appropriate remedy as one in tort (at 52).

In summary, the conclusion is that the employee and consumer protection regimes in Rome I and the Brussels I Regulation will apply in those cases where the BCR are made part of the employee or the consumer contract by including a clause to that effect. Insofar as a company processes employee and consumer data under the BCR without making the BCR part of the individual consumer and employee contracts, the conclusion is that the employee and consumer protection regimes in Rome I and the Brussels I Regulation should not apply. However, from the above it is clear that the latter is still an open issue which should be ultimately decided by the ECJ. In the meantime, multinationals are well advised to draft their BCR in such a manner that these regimes are (as much as possible) complied with. Below, I will evaluate such choice of law and forum clause in BCR against the employee and consumer protection regimes under PIL.

12.8 Are the choice of law and forum clauses validly entered into?

Pursuant to Article 10 of Rome I, the existence and validity of a contract or any term thereof (including the choice of law and forum clauses) must be determined by the law which would govern the contract if the contract or term were valid. This provision also applies to unilateral undertakings which fall within the scope of the employee or consumer protection regime of Rome I.[86] The law chosen to apply to the BCR therefore decides whether BCR are binding and whether the choice of law clause made therein is valid. As discussed in Paragraph 11.3.1, most Member States consider that rights may be granted to third parties by means of unilateral undertakings.[87] In that case the choice of law and forum clauses will also be validly made. If a Member State does not consider that third-party beneficiary rights may be

[86] See also Strikwerda (n 28) in respect of the predecessor of Rome I, at 166. Article 11(3) Rome I is not of relevance here as it relates to a "unilateral act intended to have legal effect relating to an existing or contemplated contract." Unilateral acts that are intended to have legal effect and that relate to an existing or contemplated contract, are for instance an offer, remission of a debt, declaration of rescission or notice of termination. See Cheshire, North & Fawcett (n 28), at 748 and the *Report on the Convention on the law applicable to contractual obligations* by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris I, [1980] OJ C282 , at 29. BCR are independent unilateral undertakings rather than unilateral acts and are not in relation to a contemplated or existing agreement. For purposes of Rome I, they should rather be considered as a 'contractual obligation' within the scope of Article 5(1) of Rome I itself, rather than a unilateral act relating to such contractual obligation.

[87] See WP 133, part 2: background to Paper footnote 10 (n 7), where it is mentioned that according to the civil law of some jurisdictions (e.g. Italy and Spain), unilateral declarations or unilateral undertakings do not have binding effect.

granted by a unilateral undertaking, the contractual solutions should be followed as explained in Paragraph 11.3.5.

12.9 Are the choice of law and forum clauses themselves valid and binding?

Assuming that the choice of law and forum clauses are validly **made**, the question arises whether the choice of law and forum clauses **themselves** are valid and binding. From Paragraph 12.5, it follows that the choice of law clause cannot set aside the mandatory provisions of (i) the labour law of the place where the employee habitually carries out his work or (ii) the consumer law of the place where the consumer is domiciled. As the BCR only applies if they provide additional rights and remedies in favour of the employee or the consumer, the choice of law clause is not in violation of the provisions of Rome I. From Paragraph 12.6.3 it follows that the choice of forum clause cannot set aside the jurisdiction of the courts indicated by the Brussels I Regulation. The forum clause in the BCR can therefore only create **additional forums** in favour of the employee or the consumer. This is clearly a broader protection provided to the employee or consumer than the choice of law clause (which is in principle valid, as are any mandatory provisions of the labour law of the employee or the consumer law of the consumer). If the employee and consumer protection regime were to indeed apply to BCR, the conclusion should then be that the choice of forum clause would not hold as the choice of forum in the BCR as it is meant as an **exclusive forum** for the additional rights granted to the employees and consumers and not as an **alternative forum**. As a side note I mention that in practice this does not pose much of a problem. The benefits for individuals provided by the complaints procedure in BCR (as supported by enforcement by the Lead DPA and the courts of the Lead DPA) entail in practice that individuals prefer to follow this procedure rather than addressing their own court. This being said, it would obviously be welcomed if European legislators were to provide that a valid choice of forum clause could be made in BCR. This is already part of *Recommendation 9*.

12.10 Choice of forum should be (evidenced) in writing

12.10.1 BCR as unilateral undertakings

The next[88] problem is that Article 23 (1)(a) of the Brussels I Regulation requires that an "agreement conferring jurisdiction be "**either in writing or evidenced in writing**". This requirement should also be interpreted in an autonomous manner.[89] Specific requirements under applicable national law should be ignored.[90] The ECJ interprets Article 23 Brussels I Regulation in a strict manner.[91] Case law of the ECJ shows that the "in writing" requirement is satisfied only when there is a **written contract** which contains a choice of jurisdiction and that any variant on this causes problems.[92] Case law further shows that the alternative "evidenced in writing" is foremost designed to deal with the situation where there is an oral contract which is confirmed in writing.[93] When applying this case law to the BCR, it seems difficult to conclude that the forum clause is made in writing (as the BCR are unilateral undertakings only) or is evidenced in writing (as in respect of BCR, there is no oral contract which is confirmed in writing). Rather the reverse, BCR contain an offer in writing and if there is acceptance, this is a tacit acceptance by the employee or consumer which is not confirmed in writing. This leads to the conclusion that the choice of forum clause in BCR does not meet the requirements as to form. This entails that employees or consumers may enforce the additional rights and remedies granted in the BCR against the company, but that the company in its turn may not invoke the choice of forum clause against the employees or consumers (as this forum clause does not meet the stricter requirement that such clause has been concluded in writing or evidenced in writing). This seems a very undesirable outcome. National case law in some Member States shows that national courts under circumstances honour a choice of forum clause, which is contained in a written offer which has been tacitly agreed by the other party.[94] Tacit acceptance may for instance be concluded if a plaintiff bases its claim on the BCR with a choice of forum clause, without

---

88 The requirements of Article 23 Brussels I Regulation also apply in the case of a choice of forum clause in employee and consumer contracts. See for an overview of literature and case law, see P.H.L.M. Kuypers (n 80), at 490. See further Cheshire, North & Fawcett (n 28), at 271 and 275. The use of jurisdiction clauses in consumer cases must not infringe the Unfair Terms in Consumer Contracts Regulations 1999 SI 1999/3159, pursuant to which jurisdiction clauses that have not been individually negotiated and exclude or hinder the consumer's right to take legal action (like confer exclusive jurisdiction on the seller's place of business) must be regarded as unfair.

89 See case law ECJ in n 67.

90 Case C 159/97 *Castelletti* [1999] ECR I-1597, para. 39.

91 Cheshire, North & Fawcett (n 28), at 291.

92 Cheshire, North & Fawcett (n 28), at 291.

93 Cheshire, North & Fawcett (n 28), at 292 and case law referred to in footnote 759.

94 P.H.L.M. Kuypers (n 80), at 318.

indicating that he does **not** accept the choice of forum.[95] However, this does not add much as the same result would also be achieved by Article 24 Brussels I Regulation, pursuant to which the court of a Member State before which a defendant appears will have jurisdiction. If the employee or consumer addresses the forum chosen in the BCR and the multinational appears in court, such court will have jurisdiction.[96] However, if the employee or consumer addresses **its own court**, the multinational will not be able to invoke the forum clause against the employee or consumer.

12.10.2 Contractual solution

In Paragraph 11.3.5, I discussed that a solution to solve the issue that in certain countries unilateral undertakings cannot be considered to confer rights on third parties, is to have the (Delegated) EU Headquarters enter into a contract with one of its other group companies containing a third-party beneficiary clause for the benefit of the employee or consumer. The question is then whether the requirements as to form (i.e. the forum clause should be in writing or evidenced in writing) also apply in relation to the third-party beneficiaries. Case law makes clear that a third-party beneficiary may invoke a choice of forum clause which is made on his behalf even though the third party has not satisfied the requirements as to form.[97] Case law, however, does not seem to support the reverse situation. The choice of forum clause cannot be invoked **against** a third-party beneficiary who has not separately consented to the choice of forum clause.[98] Again, to solve all issues identified above as to the form requirements for a choice of forum, it

95 P.H.L.M. Kuypers (n 80), at 319.

96 Cheshire, North & Fawcett (n 28), at 296.

97 See for instance Case 201/82 *Gerling* [1983] ECR 2503, where the ECJ decided that a choice of forum clause in an insurance contract, which was made for the benefit of the policy beneficiary, could be invoked by the beneficiary even if he had not signed the insurance contract.

98 If a third party succeeds to the rights and obligations of an original party under a contract that complies with the requirements of Article 23 Brussels I Regulation, the third party cannot avoid the obligations in respect of jurisdiction by arguing that he did not (separately) consent to the jurisdiction clause. See Case 71/83 *Tilly Russ* [1984] ECR 2417, which concerned a bill of lading and the binding effect of a choice of forum clause as against the (third-party) holder of the bill of lading who, under the applicable national law, had become a party to the transportation agreement. The choice of forum could be invoked vis-à-vis such a third party. If a third party is not a successor to the rights and obligations of one of the original parties to the agreement, the choice of forum clause can be invoked vis-à-vis him only if he has accepted the jurisdiction clause in the original agreement as per the requirements of Article 23 Brussels I Regulation. See, Case C-387/98 *Coreck Maritime* [2000] ECR I-9337.

would be welcomed if European legislators provided that a valid choice of forum clause may be made in BCR (as per *Recommendation 10*).

12.11 Conclusions: How the applicability, supervision and enforcement regime of BCR may work

As indicated at the beginning of this chapter, it is in the interest of the multinational that all complaints under its BCR are ultimately dealt with by the DPA (and the courts of the Member State of such DPA) that negotiated the provisions of the BCR under applicability of the DPA's own law (i.e. the law under which the provisions of the BCR were drafted). This ensures for the multinational a consistent and predictable interpretation of the BCR. For the same reason the multinational has an interest in the Lead DPA having central supervision over the BCR. It is clear that even if the BCR are drafted as recommended and provide for supplemental protection only, many PIL issues arise in respect of a choice of law and forum clause in BCR. This is the case, despite such choice of law and forum not being contrary to the underlying policy choices of the consumer and employee protection regimes of Rome I and the Brussels I Regulation. To the contrary, such choice of law and forum will drastically improve the data protection and the access to remedies for the individuals covered by the BCR.

13 BCR and the "accountability principle"

13.1 The accountability principle in the field of data protection

In December 2009, the Working Party 29 together with the Working Party on Police and Justice (**WPPJ**) issued a joint paper "The Future of Privacy"[1] in which they expressed the view that the present European legal framework for data protection has not been successful in ensuring that the data protection requirements translate into effective mechanisms that deliver real protection.[2] To improve this situation, the Working Party 29 and the WPPJ proposed to the European Commission to include the "principle of accountability" in the revised Data Protection Directive.[3] With the acknowledgement that "accountability" may have different meanings in different languages and legal systems,[4] the Working Party 29 and WPPJ proceeded with describing the measures which "accountability" requires (rather than focusing on a definition). In short, this principle entails that the controller is required:

(i) to implement appropriate and effective measures to put the material processing principles of the Data Protection Directive into effect;
(ii) to demonstrate these measures to the DPA on its request.

The EDPS supports the proposal of the Working Party 29.[5] In its turn the European Commission in its EC Communication on revision of the Directive indicated that it "will explore ways of ensuring that data controllers put in

---

1 See n 33.

2 WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 8 at 6: "[T]he main principles of data protection are still valid despite these important challenges. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice." Also at para. 78 at 10: "In practice Article 17 (1) has not been successful in making data protection sufficiently effective in organizations, also due to different approaches taken in the national implementing measures."

3 WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 79.

4 WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 21 at 7: "The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning – even though defining what exactly accountability means is complex. In general terms though, its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can suffient trust be developed."

5 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 7.2.

place effective policies and mechanisms to ensure compliance with data protection rules. In doing so, it will take into account the current debate on the possible introduction of an "accountability" principle.[6]

The principle of accountability is not new and is already applied in some other fields of law.[7] The principle has also from the start been applied in the field of data protection. The accountability principle is one of the main principles in the OECD Privacy Guidelines,[8] the APEC Privacy Framework,[9] the Canadian PIPED Act,[10] and also of the more recent Madrid draft

---

6 EC Communication on the revision of the Directive (Chapter 6, n 34), at 11 – 12.

7 For instance the Securities and Exchange Commission requires that companies implement a code of ethics and evidence of effective implementation procedures. See http://www.sec.gov/about/laws/secrulesregs.htm. For other examples, see para. 13.2 below. Under EU law, investment managers have to show sufficient and proper administrative organisation in order to obtain authorisation (see e.g. Article 5 of the Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC).

8 See Chapter 6, n 38, at 14: "A data controller should be accountable for complying with measures which give effect to the principles stated above." The principles stated above concern the material processing principles.

9 See Principle 26: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

10 Personal Information Protection and Electronic Documents Act, 200, C.5, to be found at <www.laws.justice.gc.ca>. See Schedule I, section 4.1, where the first Principle requires developing and implementing policies and practices to uphold the 10 fair information principles, including implementing procedures for protecting personal information and establishing procedures for receiving and responding to complaints and inquiries:
"Principle 1 — Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

proposal for International Standards,[11] ISO draft standard 29100 setting a privacy framework,[12] the draft Australian Privacy Principles,[13] the FTC

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

[11] See Madrid draft proposal for International Standards (Chapter 7, n 21), Article 11: "[T]he responsible person shall: a. take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation; and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in para. 23."

[12] As issued by the Centre for Information Policy Leadership, to be found at <www.informationpolicycentre.com>. The Centre is also engaged in an initiative to explore the effects of the principle of accountability in respect of data protection.

[13] Australian Government, Australian Privacy Principles (Chapter 6, n 52). The Exposure Draft does not use the word "accountability," but contains provisions that are close in content to the two-fold structure of the accountability principle as envisaged by the Working Party 29 and the European Commission. This requires that a controller must: 1) take organisational and technological measures to comply with the data protection rules; and 2) be able to demonstrate compliance in case of an audit. Principle I (2) of the Australian Privacy Principles, on "open and transparent management of personal information," requires that "an entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles.

(3) An entity must have a clearly expressed and up-to-date policy (the privacy policy) about the management of personal information by the entity.

(4) Without limiting subparagraph (3), the privacy policy must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

Proposed Framework for Consumer Privacy[14] and the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011.[15]

(g) if the entity is likely to disclose personal information to overseas recipients-the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

Pursuant to Part B, paragraph 19 of the Exposure Draft, the same requirement applies in case of the transborder data transfers: "This Act extends to an act done, or practice engaged in, outside Australia by an agency. This Act and an approved privacy code extend to an act done, or practice engaged in, outside Australia by an organisation that has an Australian link."

[14] The FTC does not use the term accountability, but principle 1 of the FTC Proposed Framework for Consumer Privacy (Chapter 9, n 36), at 1, requires companies to have comprehensive data management procedures in place: "Companies should promote consumer privacy throughout their organisations and at every stage of the development of their products and services.

- Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.
- Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services".

Confusingly, the FTC labels this principle "Privacy by Default", which term has a different meaning under EU law, see EC Communication on the revision of the Directive (Chapter 6, n 34), para. 2.2.4, at 12. See further

[15] Sections 102 (Accountability) and 103 (Privacy by Design) of The Kerry-McCain Commercial Privacy Bill of Rights Act of 2011:

SEC. 102. ACCOUNTABILITY.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information it collects—

(1) have managerial accountability, proportional to the size and structure of the covered entity, for the adoption and implementation of policies consistent with this Act;

(2) have a process to respond to non-frivolous inquiries from individuals regarding the collection, use, transfer, or storage of covered information relating to such individuals; and

(3) describe the means of compliance of the covered entity with the requirements of this Act upon request from— (A) the Commission; or

(B) an appropriate safe harbor program established under section 501.

SEC. 103. PRIVACY BY DESIGN.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by—

(1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on—

(A) the reasonable expectations of such individuals regarding privacy; and

(B) the relevant threats that need to be guarded against in meeting those expectations; and

(2) maintaining appropriate management processes and practices throughout the data life cycle that are designed to ensure that information systems comply with—

13.2 The accountability principle according to general literature

According to the extensive literature on accountability in the public policy literature and fields of law other than data protection, the main purpose of "accountability" is to use the law to hold businesses accountable "for taking their responsibilities seriously by using various mechanisms to encourage or enforce business to put in place internal governance structures, management practices and corporate cultures aimed at achieving responsible outcomes."[16] The law attempts to constitute corporate consciences "to want to do what they should do" and not just to produce legally compliant outputs.[17] The regulatory initiatives to seek to do this are often called "meta-regulation", i.e. the regulation of internal self-regulation.[18] The underlying assumption is that organisations, not being individuals, can only be responsible by building responsibility into their practice and structure. Accountability is part of risk-based regulation,[19]

(A) the provisions of this Act;

(B) the privacy policies of a covered entity; and

(C) the privacy preferences of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 202."

16 Parker (Chapter 9, n 43), at 207.

17 Parker (Chapter 9, n 43), at 208.

18 Many other terms are used in this context. See for an enumeration Gilad (Chapter 10, n 53), at 485: "system-based regulation, enforced self-regulation, management-based regulation, principles-based regulation". Another label is 'horizontal supervision' (whereby actions are adjusted by the supervisory authority and the supervised entity in cooperation) as opposed to vertical supervision, which is the traditional *command and control* model, whereby any actions of the supervised entity are corrected top down by the supervisory authority. See A.T. Ottow, *De Markt Meester? De zoektocht naar nieuwe vormen van toezicht* (Boom Juridische Uitgevers 2009) in particular para. 2.1. On the expansion of regulation from government to governance, see Ramses Wessel and Jan Wouters "The Phenomenon of Multilevel Regulation: Interactions between Global, EU and National Regulatory Spheres," in: Andreas Follesdal, Ramses A. Wessel and Jan Wouters (eds.) *Multilevel regulation and the EU, The interplay between global, European and national normative processes* (Martinus Nijhof Publishers 2008), at 22 -47.

19 McBarnet (Chapter 8, n 23), at 34 – 36. For risk-based regulation in respect of CSR see Parker (Chapter 9, n 43), at 228: "To the extent that scholars and policy makers focus on achieving CSR through corporate governance processes (i.e., meta-regulation), it signifies a decisive move in the direction of abandoning traditional "command and control" state regulatory schemes in favour of "responsive regulation", which is supposed to facilitate – yet not enforce and dictate – self-regulation programs and "compliance-oriented" regulation, which is carried out through corporate consent and voluntary organizational processes of reflexive learning." As to risk-management by multinationals of their supply chain, see McBarnet and Kurkchiyan (Chapter 9,

where companies themselves prioritise and tailor their compliance efforts dependent on the level of risk involved. Meta-regulation is expected to be able to achieve more sustainable compliance with traditional regulatory goals "because it latches onto companies' inherent capacity to manage themselves".[20] The aim of meta-regulation therefore is to make sure the relevant values are "built into the practice and structure of the company".[21] In order to achieve these objectives, meta-regulation requires companies "to put in place formal governance structures and management systems that help to produce a responsible culture and management in practice"[22], while recognising that regulators may not know exactly what the right processes and even the results would look like in each situation and further that these may change over time.[23] More fundamental, one of the underlying drivers for meta-regulation is the recognition in the general policy literature that prescriptive regulation (where regulators prescribe the desired behaviour) has "inherent limitations to achieve the underlying regulatory objectives due to "regulators" imperfect access to factual information and to theoretical knowledge (e.g. of the solutions that could most effectively and efficiently mitigate risks to regulatory objectives). More fundamental, prescriptive regulation is an inherently limited tool for managing complex,

---

n 41), at 63 cited in n 41. See further Julia Black, "The Emergence of Risk Based Regulation and the New Public Management in the UK," in: [2005] Public Law.

20 Parker (Chapter 9, n 43), at 212. The fact that meta-regulation "latches onto companies' inherent capacity to manage themselves"' is at the same time seen by many as the main weakness of meta-regulation. See for instance Black (n 19), at 512-549: "the firm's internal controls will be directed at ensuring the firm achieves the objectives it sets for itself: namely profits and market share. Whilst proponents of meta-regulation are correct to argue that its strength lies in the ability to leverage off a firm's own systems of internal control, and indeed regulators should fashion their own regulatory processes on those controls, this difference in objectives means that regulators can never rely on a firm's own systems without some modifications. The problem then arises, however, of locating those differences and ensuring both regulator and regulated understand them." See for an overview of studies that have assessed the impact on compliance of introduction of regulation based on accountability Gilad (Chapter 10, n 53), at para. 3, at 491-492, concluding that "on the whole, the above studies seem to point to the positive impact of process-oriented regulatory institutions on firms' performance."

21 Parker (Chapter 9, n 43), at 215.

22 Parker (Chapter 9, n 43), at 216.

23 Parker (Chapter 9, n 43), at 217.

heterogeneous, and dynamic social realities, which leads to both excessive and insufficient regulation. "[24]

According to the extensive literature on what it takes for organisations to be internally committed to legal compliance, this requires at least[25]:

- high level policies setting out the legal and ethical obligations the company wishes to adhere to;
- institutionalisation of these policies within management and employee accountability and performance measurement systems and the company's standard operating procedures;
- clear communication and training in programmes for raising awareness of the existence and the substance of policies;
- internal reporting and monitoring systems;
- complaint procedures and a possibility of whistle blowing;
- internal and external reviews or audits of the performance of the compliance system, which feed back to the highest level; and
- external disclosure in the annual reports in a comparable format.

13.2.1 External disclosure requirement

The requirement of external disclosure in a comparable format, is increasingly being discussed in the literature as a necessity to ensure that external stakeholders have access to information on the relevant compliance efforts of the company and any related shortcomings and remedial efforts. Reporting in a standard format further facilitates comparison between companies and inclusion of performance in indices, which appears to be a strong incentive to enforce compliance. [26] This is also advocated in the law and economics approach, according to which "the law should be concerned

---

[24] Gilad (Chapter 10, n 53), at 493, referring to C. Sunstein, Problems with Rules. California Law Review,[1995], 83, 953-1026; and J. Black, *Rules and Regulators* [1997], Clarendon Press, Oxford.

[25] Parker (Chapter 9, n 43), at 216.

[26] See: Kevin Campbell and Douglas Vick, "Disclosure law and the market for corporate social responsibility," at 241-278; and Peter Muchlinski, "Corporate social responsibility and international law: the case of human rights and multinational enterprises," at 453, both in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007). Also Gunningham (n 38), at 495. Recent illustrations that reporting and indices are influential are to be found in the Dutch newspapers of September 2010, where Royal Shell was dropped from the Sustainability index. The previous year, the bonus programme of Shell was made dependant on this ranking ("Shell uit duurzaamheid index gezet," Financieele Dagblad 10 September 2010; "Shell geschrapt van lijst schone bedrijven," Volkskrant 9 September 2010).

with promoting efficient solutions within market transactions, for example by improving the flow of information on the basis of which consumers make market decisions."[27] Especially in areas where companies are concerned with reputational damage, this may provide a stronger ability of consumers to secure remedies than the law.[28] This is also the view of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe:[29]

> "Requiring disclosure of information can be a powerful regulatory tool in company law. It enhances the accountability for and the transparency of the company's governance and its affairs. The mere fact that for example governance structures or particular actions or facts have to be disclosed, and therefore will have to be explained, creates an incentive to renounce structures outside what is considered to be best practice and to avoid actions that are in breach of fiduciary duties or regulatory requirements or could be criticised as being outside best practice. For those who participate in companies or do business with companies, information is a necessary element in order to be able to assess their position and respond to changes which are relevant to them. High quality, relevant information is an indispensable adjunct to the effective exercise of governance powers. (...) Disclosure requirements can sometimes provide a more efficient regulatory tool than substantive regulation through more or less detailed rules. Such disclosure creates a lighter regulatory environment and allows for greater flexibility and adaptability. Although the regulatory effect may in theory be more indirect and remote than with substantive rules, in practice enforcement of disclosure requirements as such is normally easier."

13.2.2 Learning-oriented approach

The latest empirical and theoretical research in the public policy arena[30] suggests that a specific innovative form of meta-regulation is best placed to overcome some of the weaknesses of the prevalent forms of regulation based on the accountability principle. In cases where the regulator knows the result it is trying to achieve, but does not know the means for achieving it, or if circumstances are likely to change in ways that the regulator cannot

---

[27] Scott (Chapter 8, n 25), at 1.

[28] Scott (Chapter 8, n 25), at 4.

[29] Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe, Brussels, 4 November 2002 (Chapter 8, n 30), at para. 3 at 961 - 962 (Disclosure of Information as a Regulatory Tool).

[30] This paragraph draws on Gilad (Chapter 10, n 53), at 486-506, which gives a good overview of the empirical and theoretical research in the public policy arena and further identifies the topics which require further empirical research.

predict, or when the regulator does not know the precise result that it desires, research shows that prescriptive regulation will be ineffective.[31] In those cases a more open-ended learning-oriented approach has been shown to produce better compliance results.[32] In such a learning-oriented approach, regulators set broadly defined goals and companies are encouraged to experiment with more efficient and effective means to achieve these goals. The companies are expected to continuously evaluate their efforts in light of the regulatory goals and implement potential improvements (also labelled "double loop learning").[33] The companies have to feed their self-evaluations to the regulators.[34] The regulators subsequently assess and benchmark the companies' relative performance and disseminate examples of successful solutions (also labelled "triple loop learning").[35] The

---

31 Gilad (Chapter 10, n 53), at 485 and 489, citing C.L. Ford, New Governance, Compliance, and Principles-based Securities Regulation, American business Law Journal [2008], 45, 1-60: "open-ended, learning systems are preferable…where the regulator "knows the result it is trying to achieve but does not know the means for achieving it, when circumstances are likely to change in ways that the [regulator] cannot predict, or when the [regulator] does not even know the precise result that [it] desires."

32 Gilad (Chapter 10, n 53), at 485. At 503, Gilad notes that the empirical research has shown "that organizational complexity hinders corporations' capacity for compliance and learning from failures. (…) The empirical question, which remains to be answered, is whether a meta-regulatory approach, which holds regulatees accountable for continuous improvement and provides them with examples of how other organizations cope with internal complexity, can support organizations' capacity building."

33 The first loop of learning being the development and implementation of the first set of compliance measures. See for a description of the double and triple loop learning cycle: Gilad (Chapter 10, n 53), at 488, referring to C. Parker, *The Open Corporation: Effective Self-regulation and Democracy*, [2001], Cambridge University Press, New York, NY: "Meta-regulation expects organisations to not only identify risks and devise internal control systems, but also to continuously evaluate the efficacy of their internal systems and incrementally improve them in light of this evaluation (i.e. double-loop learning). (…) Regulators should consciously engage in learning about the industries and the problems they are trying to manage, assess the impact of their strategies, and continuously improve their regulatory strategies accordingly (i.e. triple-loop learning)."

34 Gilad (Chapter 10, n 53), at 493.

35 Gilad (Chapter 10, n 53), at 487-498, see also at 499. Gilad at 489 provides as an example of this incremental learning model the "Treating Customers Fairly" initiative as launched by the UK Financial Services Authority (FSA), to be found at http://www.fsa.gov.uk/pages/Doing/Regulated/tcf/library/index.shtml. The intiative required firms to evaluate their corporate culture against the duty "to treat its customers fairly", set up appropriate systems and controls, consistently measure their performance, and provide evidence that the solutions that they were implementing were resulting in change to outcomes.

regulators therefore do not evaluate the systems and controls *ex-ante*, but "rather make their judgements based on the basis of organisations' ongoing evaluation of the (…) outcomes of the changes that they introduce".[36]

The empirical research also indicates that the learning-oriented approach is also best placed if a regulator is faced with an industry that is impervious to regulatory prescription because of widespread business resistance or lack of commitment or capacity for compliance.[37] In short, the learning-oriented approach is more likely to enhance an organisation's self-regulatory capacity and overcome regulatory resistance[38] by enhancing the internal awareness of the risks involved, implementing proper governance including centres of expertise, providing managers with additional sources of information and control, thus driving managers to constantly improve their risk-detection and mitigation processess.[39]

Extensive elaboration on data protection compliance by multinationals is unnecessary, as all elements that are indicative for applying the "learning-oriented approach" are present. The technical developments in the digital era proceed at such a fast pace and are so varied and unpredictable that their impact on data protection is impossible to predict, as a result of which any attempt of regulators (even if assisted by the organisations themselves) to issue prescriptive regulation is doomed to failure. Similar uncertainty exists as to the most appropriate means to enhance data protection compliance. As discussed, there is widespread and pervasive non-compliance of multinationals with, especially, the EU data transfer rules.[40] The relevance of the learning-oriented approach to BCR is evaluated in Paragraph 13.3.2. In

---

Based on the review of the evidence provided, the FSA subsequently issued over the years informal guidance to the industry, gradually developing analytic frameworks to guide firms' self-evaluation process and provided firms with "good" and "bad" examples.

36 Gilad (Chapter 10, n 53), at 493, under refererence to J. Black, Forms and Paradoxes of Principles-based Regulation, Capital Markets Law Review [2008] 3, 425-457 and Ford (n 31).

37 Gilad (Chapter 10, n 53), at 485.

38 Gilad (Chapter 10, n 53), at 502. Empirical research has shown that there are many other relevant factors to drive transformative change to the practices of an organisation, such as the hurdle that "the regulatory goals need to be embraced by senior managers", and further that the "managers' commitment to regulatory goals and the internal compliance program has to be communicated and internalized beyond the upper echelons of [the] organizations- all the way down to front-level employees across the organization.", see Gilad (Chapter 10, n 53), at 500.

39 Gilad (Chapter 10, n 53), at 498 and 502, referring to R.A. Kagan and J.T. Scholz, The Criminology of the Corporation and Regulatory Enforcement Strategies, in: *Enforcing Regulation* (ed K. Hawkins and John Thomas), 1984, Kluwer-Nijhoff, Boston, MA, at 67 – 97.

40 See Chapter 6, n 26 and 27.

that context, the findings of existing research on this type of meta-regulation are taken into account.

The learning-oriented approach calls for a combination of regulators with a high capacity for data collection and analysis, a stable regulatory agenda and sufficient funding[41] so as to provide the latitude for the regulator to pass through the various learning cycles of a long-term incremental learning process.[42]
To engage companies in the incremental learning process, regulators will further have to establish a relationship of trust with the regulated companies. To inspire trust, for instance, that regulators will not use the information gained about such companies during the incremental learning process and then later formally prosecute such company.[43]

As indicated, part and parcel of this form of meta-regulation is the regulatory dissemination of good practice examples. This may have as a consequence that for "high performers" in the industry there is "less potential for competitive advantage from innovation", as regulatory innovations are shared by the regulators with other companies.[44] Advantage for high performers however may come in intangible forms, such as being recognised as an industry leader, good relations with regulators, and market recognition.[45] For those lagging behind, the dissemination of good practice obviously reduces costs of devising compliance tools which may lower the threshold for entry into the self-regulatory system. Despite such "recycling"

---

41 From the regulators' perspective, regulatory assessment costs are likely to be high as regulators are required to engage with the regulatees in discussions about organisation-specific risks and the merits of possibly novel solutions and controls, see Gilad (Chapter 10, n 53), at 496.

42 Gilad (Chapter 10, n 53), at 498: this requires "high regulatory capacity for data collection and analysis and a stable regulatory agenda that would enable regulators and regulatees to engage in incremental learning. The latter, in turn, requires that regulators and regulatees enjoy mutual trust and external political and public support, which would provide them with latitude for short term experimentation in pursuit of long-term improvements".

43 Gilad (Chapter 10, n 53), at 497: "This may mean that in the early stages regulators should not involve formal assessments of regulatees' performance as long as they are seen to cooperate with the self-improvement process." See further at 497, referring to Black (n 36): "for regulatees to engage in experimentation, regulators will need to establish a relationship of trust with the industry so that organisations feel confident that regulators are not simply trying to shift to them the blame for future failure."

44 Gilad (Chapter 10, n 53), at 499 however notes that "high performers may value the status of industry leaders and the credit they could gain from that in their interaction with regulators, colleagues, and the public".

45 Gilad (Chapter 10, n 53), at 499.

of regulatory innovations, the overall implementation cost of this form of meta-regulation is more expensive for all companies than compliance with prescriptive regulation, "as it demands constant improvement rather than one-off planning and implementation".[46]

The main risks identified in respect of the learning-oriented approach is that the incremental learning process (i) will result in a deadlock, where the companies await regulatory guidance and assurance that the proposed systems and controls are acceptable, whereas regulators will feel unable to make a judgement;[47] (ii) will lead to the systems and controls of the companies not meeting regulatory goals due to the fact that regulators are not able to identify flaws in companies' programs; and (iii) will lead to regulators pursuing a "tick-box" approach to assessing organisations' compliance. This drives companies to treat non-binding advice as if it were compulsory, which may lead companies to implement extensive and expensive, albeit ineffective, internal compliance programs.[48]

13.2.3 Sticks and carrots

Further, a common denominator in the literature on the accountability principle in other fields of law is that introduction of this principle should be accompanied by clear incentives for companies to implement robust compliance programmes, and in particular that sanctions will be mitigated if a proper compliance programme was in place.[49] As one author put it: "the sanctioning practice in relation to risk-based regulation should also be risk-based."[50] Other authors are more pragmatic and note that the move to a risk-based sanctioning practice is often driven by concerns of regulators to

46 Gilad (Chapter 10, n 53), at 499. Gilad however, also notes that empirical research shows that companies cognitively experience the efforts and cost involved with the incremental improvement of their own compliance systems and controls as less onerous than the efforts and cost involved with the implementation of ex-ante devised regulatory systems and controls, as these often result in organisations having to implement "extensive and expensive, albeit ineffective, internal compliance programs". See Gilad (Chapter 10, n 53), at 497, referring to K.D. Krawiec, Cosmetic Compliance and the Failure of Negotiated Governance, Washington University Law Review [2003] 81, at 487 – 544.

47 Gilad (Chapter 10, n 53), at 496.

48 Gilad (Chapter 10, n 53), at 496-497.

49 McBarnet (Chapter 8, n 23) at 36-37, Parker (Chapter 9, n 43), at 218-223 and Ottow (n 18) at para. 3.2, and in particular at 31.

50 Ottow (n 18), at 31; see further McBarnet (Chapter 8, n 23) at 36.

reduce regulatory burdens through the adoption of proportionality in enforcement.[51]

Regulatory practice shows that legislators in other fields of law have found many ways to incentivise companies to implement compliance programs. Especially regulators of financial institutions (like the SEC, NASDAQ and the NYSE) have shown great creativity in this respect by:[52]

- requiring a code of business conduct and ethics and evidence of effective implementation procedures;[53]
- requiring whistleblower policies (protecting whistleblowers) be put in place,[54] which fosters a culture of compliance with the internal codes;
- introducing "comply or explain" requirements: disclosure requirements as to how companies have complied with certain principles of good governance and when they choose not to, explain why they did so;[55]

---

51 Scott (Chapter 8, n 25), at 2 noting that the enforcement practice in consumer protection cases, which "might lead the observer to think that [this] would be shaped by ideas that work in regulatory enforcement generally", is in fact "in many jurisdictions, qualified by recent concerns to reduce regulatory burdens through the adoption of proportionality in enforcement". See Scott (Chapter 8, n 25), at 16, giving as an example the UK, where an analysis was issued of how regulatory goals might be pursued with the least burdensome necessary measures, referring to: Better Regulation Taskforce, Alternatives to State Regulation, London 2002, Cabinet Office; and Philip Hampton, Reducing Administrative Burdens: Effective Inspection and Enforcement, London 2005, HM Treasury.

52 This draws on examples listed in: McBarnet (Chapter 8, n 23) at 36-37, Parker (Chapter 9, n 43), at 218-223 and Ottow (n 18) at para. 3.2.

53 See para. 406(c) Sarbanes-Oxley Act which contains a comply or explain requirement for a Company Code of Ethics, to be found at <http://www.sec.gov/rules/final/33-8177.htm> and (since 4 November 2003) the NASD Rule 4350(n), which requires a Code of Business Conduct and the New York Stock Exchange Corporate Governance Rules, para. 303A of the NYSE Listed Company Manual, requiring Corporate Governance Guidelines and a Code of Business Conduct and Etics, both to be found at <http://www.sec.gov/rules/sro/34-48745.htm>.

54 As required by the Sarbanes-Oxley Act (2002), Pub.L.No. 107-204, and also by many corporate governance codes in Europe. See for an overview of the corporate governance codes in the EU: <http://www.ecgi.org/codes/index.php>.

55 By requiring a company to publish its compliance efforts, an incentive is provided to actually implement those measures. As the well known IT consultancy firm Gartner puts it, "you get what you inspect." France was the first country to make reporting on the "social consequences of a company's activities" (both at a group level and internationally) mandatory for publicly listed companies in their annual reports. See Aurora Voiculescu, "Green paper to new uses of human rights instruments," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability,*

- considering a compliance program as an important aspect in determining liability or penalties;[56]
- considering the robustness of a company's internal systems for managing operational risk as a factor in deciding their capital adequacy ratios;[57]
- using discretionary powers to make informal settlements requiring implementation of compliance systems or considering an effective compliance system a factor in deciding whether to prosecute or not; [58]
- treating companies that have a proper compliance program with more trust and subjecting them to less regulatory inspection;[59]
- making the existence of a compliance program a condition of license or permits required before a company can engage in a certain business; examples are the license requirements for financial services firms that include broad-ranging internal systems for ensuring integrity of funds;[60]

Corporate Social Responsibility and the Law (Cambridge University Press 2007), at 376. This 'comply or explain' principle has been introduced in many corporate governance codes in and outside Europe. For an overview of all such codes, see http://www.ecgi.org/codes/index.php. For an explanatory memorandum of the EU Corporate Governance Forum on the 'comply or explain' principle, a statement dated 6 March 2006, can be found at: <http://ec.europa.eu/internal_market/company/ecgforum/index_en.htm>. On the effect of disclosure requirements (especially if they are in a comparable format), see Campbell and Vick (n 26) at 241-278.

56 Examples are the US Federal Sentencing Guidelines for Organisations, which state that the existence of an effective compliance system will provide companies or individuals with a reduction of penalty, and the sanction guidelines of the Dutch supervisory authority on telecom operators (OPTA), Stcrt, 11 March 2008, no. 50, at 27.

57 See the Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework* (June 2004), available at <www.bis.org>, which is a voluntary agreement between G10 nations to harmonise standards for national banking regulation,

58 This is common practice of regulators both in the UK and the Commonwealth countries (see Parker (Chapter 9, n 43), at 219), as well as for instance in the Netherlands. See Ottow (n 18), at 29-31.

59 See McBarnet (Chapter 8, n 23), at 36: "A similar use of enforcement policies has been mooted in the United Kingdom, where companies that demonstrated themselves to be "responsible", would be treated with more trust and less regulatory inspection," (referring to the "Hampton Review", P. Hampton, Reducing Administrative Burdens, Effective Implementation and Enforcement (HM Treasury, 2004).

60 See for examples Parker (Chapter 9, n 43), at 220.

- fast-tracking the granting of licenses or permits; scheduling inspections less frequently; and
- making government procurement decisions conditional on implementation of proper compliance systems.

13.2.4 The "right" regulatory response

Empirical research in respect of enforcement of consumer protection laws suggests that the "right" regulatory response to violations also depends on the type of business involved and should be tailored to (a) businesses which fundamentally seek to be compliant as one of their operating values; (b) amoral calculators which operate on a cost-benefit basis and who will comply where it makes sense from a cost-benefit perspective; and (c) incompetents who, whatever their intent, lack the capacity to organise themselves to comply with regulatory requirements.[61] With the compliant organisations, it is suggested that low level enforcement approaches based on education and advice and a more cooperative (rather than adversarial) regulatory style is indicated, where the regulator and company negotiate over responses to violations rather than go to court over them.[62] With the amoral calculators it is suggested that a pyramid of sanctions should be available for regulators ranging between education and advice, through warnings and penalties, to prosecution and ultimately licence revocation. Incompetents are beyond help and their licences should be revoked.[63]

13.3 Review of the BCR regime against accountability requirements in the general literature

13.3.1 Good fit with data protection

My first observation is that on all accounts the 'accountability principle' does seem to be a good fit with EU data protection law.

As indicated, 'accountability' is part of risk-based regulation, where companies themselves prioritise and tailor their compliance efforts dependent on the level of risk involved. This fits well with many provisions in the Data Protection Directive, requiring for instance "appropriate"

---

61 Scott (Chapter 8, n 25), at 15, referring to Robert Kagan and John Scholz. 1984. The 'Criminology of the Corporation' and Regulatory Enforcement Strategies", in: *Enforcing Regulation*, ed. Keith Hawkins and John Thomas, Boston: Kluwer-Nijhoff.

62 See on the different styles of enforcement: Scott (Chapter 8, n 25), at para. 3.3. This process is also labelled "bargaining in the shadow of the law".

63 Scott (Chapter 8, n 25), at 15, referring to Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*. Oxford 1992.

security measures, "adequate" data protection safeguards, etc. As to these concepts, the Working Party 29 from the start has applied a risk-based approach, indicating as the first (of three) objectives of the Data Protection Directive "to deliver a good level of compliance", acknowledging that a 100% compliance is not achievable in practice.[64] The Working Party 29 further has applied from the start a risk-based approach to the content of data protection obligations (i.e. requiring stricter security measures in the case of a transfer of sensitive data, etc) as well as identifying priorities in enforcement for the DPAs.[65] This risk-based approach is also how multinationals manage their data protection in practice.[66] In the digital society, data flows in networks, whether within multinationals, between multinationals, or between multinationals and individual customers (i.e. internet users). The participants in such networks manage risks: they accept them, try to limit or minimise them, or transfer them to co-contractors or

---

64 WP 12 (Chapter 7, n 22), at 7: "The objectives of a data protection system are essentially threefold: 1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them."

65 WP 12 (Chapter 7, n 22), at 28 where the Working Party instructs DPAs to take a risk-based approach as to data transfers:
"It would constitute guidance regarding which cases of data transfer should be considered as 'priority cases' for examination or even investigation, and thereby allow the resources available to be directed towards those transfers which raise the greatest concerns in terms of the protection of data subjects.
The Working Party considers that among those categories of transfer which pose particular risks to privacy and therefore merit particular attention are the following:
- those transfers involving certain sensitive categories of data as defined by Article 8 of the directive;
- transfers which carry the risk of financial loss (e.g. credit card payments over the Internet);
- transfers carrying a risk to personal safety;
- transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- repetitive transfers involving massive volumes of data (such as transactional data processed over telecommunications networks, the Internet etc.);
- transfers involving the collection of data using new technologies, which, for instance could be undertaken in a particularly covert or clandestine manner (e.g. Internet cookies)."

66 See para. 9.4, especially footnote 41.

other partners whether through supply chain management or otherwise (see Paragraph 11.4 above).[67] In practice therefore, data protection is regulated through risk management. Because in the data protection context so many partners and actors are involved,[68] it seems impossible for regulators to regulate the data streams in any meaningful way without indeed "latching onto companies' inherent capacity to manage their risks". As already indicated in Paragraph 11.5.3, this is not a new insight, but a fact well known in other areas of law and a reason for states to resort to TPR since the contracting parties have more power to enforce compliance in transnational situations than does the threat of traditional judicial means.[69]

Further, the general nature of the material data processing principles in the Data Protection Directive requires that these principles are "translated" into practical instructions for employees on how to process personal data. Employees will have to receive training, compliance has to be monitored etc. This has led multinationals to introduce corporate privacy policies and compliance programs long before the introduction of the accountability principle was considered (see Paragraph 9.4).

Multinationals introducing BCR can further be categorised as type (a) businesses (see Paragraph 13.2.4), which concern companies that fundamentally seek to be compliant as one of their operating values. For type (a) companies, the right regulatory response is "a cooperative regulatory style, based on education and advice and where the regulator and multinational negotiate over responses to violations rather than go to court over them. "[70] For type (a) companies, introduction of a self-regulatory regime such as BCR therefore seems the indicated regulatory approach.

13.3.2 Learning-oriented approach

Based on the general policy research and literature, meta-regulation based on the "learning-oriented approach" seems to be indicated for data protection compliance by multinationals (see Paragraph 13.2.2). In fact this has very much been the manner in which the BCR requirements came into existence. The multinationals approached the DPAs to discuss their BCR (see Paragraph 1.1). The information obtained by the relevant DPAs in these initial discussions with the multinationals, and the documents developed

---

67 In particular n 38. As to risk-management of the supply chain, see McBarnet and Kurkchiyan (Chapter 9, n 41), at 63.

68 See Chapter 11, n 38.

69 Cafaggi (Chapter 11, n 31), at 9.

70 See Paragraph 13.2.4.

between the multinationals and these DPAs in that context (such as Privacy Impact Assessments) were subsequently fed back to the Working Party 29 and found their way into the WP Opinions (achieving intitial "triple loop learning"). Reviewing the BCR regime against the findings of the research into the learning-oriented approach, the "second loop learning" (whereby companies evaluate their own systems and controls and incrementally improve these) is missing. This is relevant as it is safe to say that data protection compliance programs are still in development[71], where further innovations are possible and best practices have therefore not yet crystallised. My conclusion is that the chances of effectiveness of the BCR regime will be improved if companies would have to not only identify data protection risks and devise internal control systems, but also achieve double loop learning by evaluating the efficacy of their internal systems and incrementally improve them in light of this evaluation. Such incremental learning will also foster the self-regulatory capacity within the multinational and overcome (remaining) regulatory resistance. This element can be addressed by introducing as a BCR requirement that multinationals "are to periodically review the totality of their BCR accountability program to determine whether modification is necessary". This requirement is also one of the "common fundamentals" of the accountability requirements as defined by the Centre for Information Policy Leadership[72] and will be part of the recommendations to be made in Paragraph 13.5.

Another element that is missing in the present regime is how the European Commission and the Working Party 29 may become engaged in this ongoing learning process of multinationals and the problems they are trying to manage in order for them to be able to improve their regulatory strategies accordingly (achieve triple-loop learning). Part of this learning process can be achieved by the European Commission organising working groups which can be tasked with defining, for instance, the accountability requirements for data transfers by multinationals to third parties outside their group of companies. I discuss this further in Paragraph 13.5.3. Another matter entirely is whether it is useful to include in the BCR regime a more structural feedback by multinationals of the evaluation of their BCR compliance programs to, for instance, the Lead DPA. For a number of reasons I do not think this is advisable. The Lead DPA is already entitled to receive such evaluation reports upon its request (see for an overview of the **passive** information requirements of the multinational towards the Lead DPA

---

71 As evidenced by the recent efforts to identify data protection accountability requirements by the Working Party 29, the Centre for Information Policy Leadership and the worldwide data protection supervisors in the Draft Madrid International Standards, see Paragraph 13.5.

72 See Paragraph 13.5.3.

Paragraph 14.7.6). In light of the strong **passive** information requirements towards the Lead DPA, introduction of additional **active** information obligations of the multinational towards the Lead DPA does not seem effective. This will just increase administrative burdens on multinationals, while leading to an information overload with the Lead DPA. This may lead to expectations of review of such information by the Lead DPA, which seems unrealistic[73] and will therefore just work counterproductively. And if the Lead DPAs were indeed to review some of the evaluations, chances are that due to time pressure this would result in a "tick-boxing" of requirements, which often leads to a semi-prescriptive regime which has a freezing effect on innovations (see Paragraph 13.2.2). My recommendation is that other manners should be found to engage EU legislators in the learning process of the multinationals as to data protection compliance. This is further discussed in Paragraph 13.7.4.

13.3.3 External disclosure requirement

Review of the BCR regime against the accountability requirements in the general literature as to other fields of law shows a nearly complete overlap. The exception, so far, is the requirement of transparency: the requirement of a company to report on (in this case) data protection compliance in a comparable format. Given the fact that reputation is a key driver for data protection compliance (see Paragraph 9.3) and further for reasons to be discussed as part of the evaluation of BCR as a form of TPR and CSR, I recommend including this publication requirement in the BCR criteria. This is also the recommendation of the Rand Report and the Working Party 29 and this recommendation will be included in the recommendations to be made in Paragraph 13.5.[74]

13.3.4 Sticks and carrots

The general literature further makes abundantly clear that the introduction of the accountability principle should be accompanied by both sticks and carrots (i.e. should provide for clear incentives for companies to implement robust compliance programs and disincentives if they don't). This is also the

---

73 See for the workload of the Lead DPAs Paragraph 10.6.1 in particular n 49.

74 The Rand Report (Chapter 6, n 27),at 53 and WP Contribution on the Future of Privacy (n 33), at 20: "The effectiveness of the provisions of Directive 95/46/EC is dependent on data controllers' effort towards achieving these objectives. This requires the following proactive measures (…) Transparency of these adopted measures vis-à-vis the data subjects and the public in general. Transparency requirements contribute to the accountability of data controllers (e.g. publication of privacy policies on the internet, transparency in regard to internal complaints procedures, and publication in annual reports)."

recommendation of the Rand Report[75], the Working Party 29[76] and (implicitly) of the Centre for Information Policy Leadership[77] and the EDPS.[78] The question is what the above means in the BCR setting. It is clear that the present "carrot" for introducing BCR (i.e. authorisation of intra-company data transfers) apparently doesn't provide a strong enough incentive as evidenced by the very low pick up of BCR (see Paragraph 10.5 above). Other incentives will have to be thought of.[79] Obvious other incentives for introduction of BCR could be to:

---

75 Rand Report (Chapter 6, n 27) at 42: "Ensure that BCR can be more easily used to ensure the legitimacy of personal data transfers to third countries, rather than relying on determining the adequacy of entire countries. This could be achieved by formalising the measures currently being developed by certain supervisory bodies, with associated guidance as to their common understanding, and should be designed so as to maximise common acceptability across Member States. Care should be taken to maintain incentives for the private sector."

76 WP Contribution on the Future of Privacy (Chapter 6, n 33), at para. 81 at 20: "A built-in reward structure could be foreseen in law to induce organisations to implement them [i.e. the accountability measures]."

77 The Centre for Information Policy Leadership has proposed to replace the BCR by "Binding Global Codes": "A multinational organisation which adopts and implements an acceptable Binding Global Code would accept responsibility for its fulfilment and for ensuring delivery of fundamental rights. In return – and for as long that remains true – it would be treated as satisfying EU and other requirements for international data transfers." See the Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 13 and the Centre for Information Policy Leadership New Proposal to International Transfers, (Chapter 10, n 49), at 7: the main "carrot" presented by the Centre is that the multinational introducing a Binding Global Code, may "self-certify their own Code without the need for prior DPA approval, which is simply not practicable with the scale of the challenge" or "if self-certification is considered too radical, there are other options for the initial adoption or approval of a Binding Global Code to ensure that minimum requirements are in fact met. These include certification by an independent Third Party (Accountability Agent) appointed by a DPA at the expense of the business or certification by a Third Party approved by the DPA."

78 EDPS Opinion on the revision of the Directive (Chapter 6, n 42), at para. 177 at 22.

79 Rubinstein (Chapter 7, n 67), at 47, proposes for the US a co-regulatory approach for regulating privacy there which is very similar to the BCR regime whereby companies create a privacy safe harbour and enjoy considerable scope in shaping self-regulatory guidelines, while government retains general oversight authority to approve and enforce these guidelines. The basic idea underlying his proposal is that such a co-regulatory approach could more effectively use 'both sticks and carrots as incentives.'

As 'sticks' are suggested

- that privacy legislation would allow civil actions and liquidated damages awards against firms that do not participate in an approved safe harbour programme;

- introduce risk-based sanctions for companies that have introduced BCR, where implementation of a compliance programme is a substantial mitigating factor.
- provide that if a multinational adopts BCR, the BCR apply instead of the national data protection laws of the Member States (as per *Recommendation 10*) or, as next best alternative, introduce the possibility that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA, releasing a multinational of the burden of complying with other possible applicable EU data protection laws (as per *Recommendation 9*).
- abolish the notification requirements for multinationals with BCR or, as next best alternative, provide for the possibility of central notification of all data processing operations of a multinational to the Lead DPA. [80]

- broader opt-in requirements;
- external and independent audits of regulatory compliance and mandatory reporting to the FTC
- stricter requirements in respect of behavioural marketing (i.e. ban on use of sensitive information and data retention limit of one month).

As 'carrots' are suggested:

- exemption from civil actions and liquidated damages;
- cost savings such as compliance reviews based on self-assessment, rather than external audits by an independent third party;
- government recognition of better performing firms (FTC 'seal of approval');
- government procurement preferences for products or services of participating firms;
- regulatory flexibility for specific business models such as online behavioural marketing.

[80] See also the Rand Report (Chapter 6, n 27) at 42, recommending to "reduce the burden of the notification obligation, by making non-notification the general rule rather than the exception," whereby "notification should be required only in cases of notable risk or harm, or when transparency cannot be adequately ensured via other means." The Centre for Information Policy Leadership Opinion on the Communication of the Commission on the revision of the Directive (Chapter 6, n 27), at 9, suggest abolishing the notification requirements and replacing them by a registration of controllers of their "basic details of corporate identity." The EDPS in its Opinion on the revision of the Directive (Chapter 6, n 35), at para. 172, recommends simplifying and/or reducing the scope of the notification requirements by: (i) limiting the obligation to notify to specific kinds of processing operations entailing specific risks; (ii) introducing a registration requirement of controllers; (iii) introducing a pan-European notification form. See further EC Communication on revision of the Directive (Chapter 6, n 34), at 2.2.2, at 10.

Recommendation 11
Introduce incentives for multinationals to adopt BCR, such as:

- risk-based sanctions for a violation of data protection by multinationals that have implemented BCR (where the implementation of a proper compliance programme is a mitigating factor);
- providing that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States (as per *Recommendation 10*), or as next best alternative, providing that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA (see *Recommendation 9*);
- abolishing the notification requirements, or, as next best alternative, providing for the possibility of central notification of all data processing of a multinational to the Lead DPA.

13.4 The accountability principle according to the Working Party 29

As a follow up to its WP Contribution on The Future of Privacy, recommending the introduction of the accountability principle in the revised Data Protection Directive, the Working Party 29 issued an Opinion on the accountability principle,[81] elaborating the implications of the accountability principle in practice.
The Working Party 29 proposed the following concrete provision:

> "Article X – Implementation of data protection principles
> 1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.
> 2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request. "

In its Opinion, the Working Party 29 stressed that introduction of this provision in the Data Protection Directive does **not** constitute additional requirements,[82] as "most of the requirements set out in this provision actually already exist, albeit less explicitly, under existing laws" and that to

[81] WP Opinion on the principle of accountability (Chapter 1, n 15), at 10.

[82] The Working Party 29 also tries to substantiate that elements of the accountability principle are already introduced in European data protection law. The examples which the Working Party 29 give are, however, very limited and cannot veil the fact that introduction of the accountability principle would be a *novum* in European data protection law.

comply with these existing legal requirements, it is already "intrinsically necessary to set up, and possibly verify, data protection related procedures." In summary, the new provision does not aim at subjecting data controllers to new principles but rather at ensuring *de facto*, effective compliance with existing ones." [83] As to the consequences of compliance with the accountability principle, the Working Party 29:

> "highlights that fulfilling the accountability principle does not necessarily mean that a controller is in compliance with the substantive principles [...], i.e., it does not offer a legal presumption of compliance nor does it replace any of those principles. [...] In practice however, companies with a robust compliance program are according to the Working Party 29 more likely to be in compliance with the law". [84] (*Sic*)

More important is the remark of the Working Party 29 that compliance with the accountability principle may play a role in assessing sanctions by the DPAs related to violation of the substantive principles.[85] This is also in line with the Rand Report that recommends a risk-based approach to sanctions, where also the compliance measures that were in place are a factor for the sanction to be imposed.[86]

Another important observation of the Working Party is that introduction of the accountability principle justifies that the role of the DPAs can be more "ex post" rather than "ex ante", justifying that certain administrative requirements (like prior notification requirements) be replaced or diminished.[87] This is also the recommendation of the Rand Report encouraging a risk-based approach, "making non-notification the general

---

[83] The EDPS is more realistic in its view that the Data Protection Directive contains elements of accountability, but that these have limited scope only. See the EDPS Opinion on the revision of the Directive (n 35), at para. 102: "This type of provision is not entirely new. Article 6 (2) of the Directive 95/46 refers to the principles relating to data quality and mentions that "It shall be for the controller to ensure that para. 1 is complied with." Equally, Article 17 (1) requires data controllers to implement measures, of both a technical and organisational nature. However, these provisions have a limited scope. Inserting a general provision on accountability would stimulate controllers to put into place proactive measures in order to be able to comply with all the elements of data protection law."

[84] WP Opinion on the principle of accountability (Chapter 1, n 15), at 11.

[85] WP Opinion on the principle of accountability (Chapter 1, n 15), at 11.

[86] Where criteria are such as the: (i) egregiousness of the conduct (was the breach the result of carelessness; what were the measures in place to protect personal data, etc); (ii) the number of data subjects affected; (iii) monetary loss; etc. See Rand Report (Chapter 6, n 27), at 57.

[87] WP Opinion on the principle of accountability (n 15), paras. 54 and 63.

rule rather than the exception"[88] and further that in respect of BCR "care should be taken to ensure incentives for the private sector".[89] A similar comment is made by the Working Party in its Opinion on the Future of Privacy[90]: "A built-in reward structure could be foreseen in law to induce organizations to implement them [i.e. the accountability measures]." The above recommendations are in line with the general literature on the principle of accountability (see *Recommendation 11* above).

The Working Party 29 subsequently gave a non-exhaustive list of common accountability measures[91]:

(i) establishing internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc).
(ii) setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects.
(iii) mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations.
(iv) appointing a data protection officer and other individuals with responsibility for data protection.
(v) offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.
(vi) setting up procedures to manage access, correction and deletion requests which should be transparent to data subjects.
(vii) establishing an internal complaints handling mechanism.
(viii) setting up internal procedures for the effective management and reporting of security breaches.
(ix) performing privacy impact assessments in specific circumstances.

---

88 The Rand Report (Chapter 6, n 27), at x and 42.

89 The Rand Report (n Chapter 6, n 27), at 42.

90 WP Opinion on the principle of accountability (Chapter 1, n 15), at 20.

91 As a complementary approach, the Working Party 29 suggests including not only the general accountability principle as cited above, but also the measures cited above as an illustrative list of measures that could be encouraged at a national level (see WP Opinion on the principle of accountability (Chapter 1, n 15), at 12).

(x) implementing and supervising verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc).

The Working Party 29 further notes that "transparency is an integral part of the accountability measures, both vis-à-vis the data subjects and the public in general". Examples of transparency measures that increase accountability include

(xi) publishing privacy policies on the internet, by providing transparency in regard to internal complaints procedures and through publication in annual reports.[92]

13.5 Review of the BCR regime against data protection accountability requirements

Below, I will compare the BCR requirements with the Working Party 29 accountability requirements listed above. There are two other sources for accountability requirements as to data protection: those as defined by the Madrid draft International Standard and those defined by the Centre for Information Policy Leadership. A comparison with those requirements will be made below. I will then discuss whether it is to be recommended that the different or additional requirements identified in these comparisons also be made part of the BCR regime.

13.5.1 Comparison with Working Party 29 accountability requirements

Review of the Working Party 29 requirements for accountability shows a nearly complete overlap with the requirements the Working Party 29 set for BCR (see Paragraph 10 above). In its Opinion on the accountability principle, the Working Party 29 also explicitly notes that the BCR regime already reflects the accountability principle: "Indeed BCR are codes of practice, which multinational organisations draw up and follow, containing internal measures designed to put data protection principles into effect (such as audit, training programmes, network of privacy officers, handling compliant system).[93] Reviewing the WP Opinion on accountability, it seems to have been rather the other way around, the work on BCR by the Working Party 29 seems to have been the basis for the listing of the accountability measures in its Opinion on accountability. Compared to the BCR

[92] WP Opinion on the principle of accountability (Chapter 1, n 15), para. 48.

[93] WP Opinion on the principle of accountability (Chapter 1, n 15), at. 7, 10, 15 and 16, and Wugmeister, Retzer, Rich (n 61), at 450.

requirements, the WP Opinion on accountability provides for five additional (or in any event more explicit) requirements. Requirements (i), (iii) and (ix) are more explicit; requirements (xi), (viii) are additional. I discuss these requirements below.

More explicit requirements identified by the Working Party 29 are:

(i) establishing internal procedures prior to the creation of new personal data processing operations;

(iii) mapping procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations; and

(ix) performing privacy impact assessments in specific circumstances.

There is little discussion that the elements above should indeed be present for a multinational to be able to be "in control" of its data processing operations. Although till now not explicitly included as such in the BCR requirements, in practice multinationals indeed comply with these requirements.

At present the BCR regime requires a "detailed description of the data processed and the data flows". For large multinationals this is not doable in the BCR itself, due to the number of data processing operations in such multinationals (easily over 10,000) and the pace of changes, replacements and additions. For multinationals to be able to be "in control" of their data processing operations (in the sense that they are able to know which systems they operate and whether these are data protection compliant), multinationals perform "privacy impact assessments" (PIA) at the time of implementation of a new data processing system (or material changes to existing systems). The PIAs are a questionnaire filled out by the manager(s) responsible for the relevant data processing system, listing all relevant details (such as the system owner, the data processed, purposes of processing, level of data security, recipients of the data, etc). This PIA is subsequently verified for data protection and security compliance by the responsible privacy officer. If the privacy officer detects a violation of the BCR, the data processing system will be adapted, the PIA adapted accordingly and resubmitted for approval to the relevant privacy officer. To ensure continued compliance, changes to a data processing system may only be made after the PIA has been adapted accordingly and resubmitted for approval by the responsible privacy officer. The multinational has oversight over its collective data processing operations by including either of the individual PIAs together in an inventory.

I do not dispute that these three requirements listed by the Working Party 29 should be part of a data protection compliance program, but I do not

recommend including these requirements in their present form in the BCR regime. The main reason for this is that the requirements are too specific and have as an inherent danger working as a "tick box" list for compliance measures regardless of their actual impact on compliance.[94] Rather, accountability rules should be formulated as overall framework rules to "latch onto the inherent capacity of the multinational to organise itself" in order to achieve that multinationals take responsibility for the **outcome** of their compliance efforts. An example is provided as an illustration.

As indicated, the first WP Opinion on BCR requires that the BCR provide for a "detailed description of the data processed and the data flows". This was practically not viable, not least because by the time such description was given by the multinational it would already be outdated. In the first discussions about BCR with for instance the Dutch DPA, the DPA acknowledged this impossibility and instead requested a "blue print" of two cross-border IT systems of the multinational to verify whether the multinational had indeed brought these systems into compliance with the BCR requirements. As the system documentation of a large cross-border IT system of a multinational may well entail many binders of technical information, the multinational proposed to instead provide an overview of the information relevant to verify data protection compliance of those IT systems (which we called "privacy impact assessments"). At the time these were paper questionnaires filled out to include the relevant information. Now we see that the Opinion on accountability prescribes that in certain cases PIAs have to be performed and that an inventory is kept of the data processing operations. However, many multinationals have now moved on and PIAs are no longer performed by means of hardcopy questionnaires but as integrated steps of an automated "gateway system" which manages the implementation of new IT systems. This not only concerns data protection compliance, but also requirements under other laws, like export controls, financial regulations, etc. This may further entail that the PIA is not performed in one step, but in stages, and that parts that the DPA would consider part of the PIA are performed as part of other mandatory checks (for instance, as part of system security rather than in relation to just data security). The information on data protection may therefore not be available in a dedicated PIA in a central inventory but rather part of a compliance dashboard combining all information on data protection, IT security, export controls, financial regulations, etc.

94 J.W. Winter, "Geen regels maar best practices," in: *Willems' wegen, Opstellen aangeboden aan prof.mr. J.H.M. Willems*, [2010], at 464.

The example above illustrates how descriptions of the **means** by which multinationals should achieve data protection compliance are outdated the moment they are issued and stifle innovation as regards the most effective means to achieve data protection compliance in practice.[95] Rather than specifying the means, the three accountability requirements listed by the Working Party 29 should be translated in a general framework requirement which imposes accountability on the multinational in achieving proper **outcomes**. In this case, for instance, the three requirements may be rephrased as a general obligation for multinationals "to have readily available information on the compliance of their data processing operations and to have ongoing risk assessment and mitigation in place."

Additional requirements identified by the Working Party 29 are:

(xi) being transparent on the internal complaints procedure (assuming such transparency concerns the number and nature of the complaints filed rather than only the existence of the complaints procedure itself) and on its data protection compliance also in its annual report (see already *Recommendation 17*).

(viii) setting up an internal procedures for the effective management and reporting of security breaches.

Concerning the transparency requirement (xi), I indeed recommend that this be included in the BCR regime. As already indicated, the driving force for data protection compliance by multinationals is reputation and transparency requirements are therefore a key factor to capitalise on this driving force. This recommendation is also based on the evaluation of BCR as a form of TPR and CSR and applicable legitimacy requirements, which will be discussed in Chapters 14 and 15.

Concerning requirement (viii) on setting up internal procedures for the effective management and reporting of security breaches, the same comment applies that it concerns a specific element of compliance only and thereby misses the more overall obligation to ensure proper compliance procedures, which should be part of accountability of a multinational. Security breaches are only one of the causes that may lead to a data protection violation; other events may occur, data protection laws may change and require changes, an audit may be performed and disclose data protection violations that require correction or violations may be reported by means of a complaint by an individual. In all cases an effective management of the "event" is indicated. Further, within a multinational a security breach of its IT systems may have far more implications than a breach of data protection. In case of a cyber

95 See on the phenomenon of prescriptive requirements stifling legal innovation, para. 11.3.2.

crime attack, the financial systems of a company may be compromised, which may trigger disclosure obligations under laws regulating listed companies.[96] If health information is involved, this may lead to specific notification obligations under laws regulating medical and health information.[97] If confidential intellectual property or know how of the multinational is stolen, this may lead to violation of export control laws.[98] Security breaches may further have consequences under labour law and telecommunications law.[99] Procedures relating to security breaches are therefore in most cases not specific to data protection breaches. If I include these obligations in an overall framework obligation for a multinational, this would be that the multinational has to have in place "event management and complaint handling, i.e. procedures for responding to inquiries, complaints and data protection breaches."

It is to be expected (and also advisable), that these additional requirements also be added to the BCR requirements. To be in control of its data processing operations, a multinational will have to have an inventory of its data processing operations as well as an ongoing risk assessment of data protection compliance. As to the requirement to have internal security breach management and notification procedures, most multinationals have such policies already in place in order to be able to comply with security breach notification laws.[100]

---

96 For instance, disclosure obligations under U.S. federal securities laws (including Sarbanes-Oxley and Security Exchange Act 1933 and 1934) are triggered if: the validity of financial statement information has been compromised; a material financial impact is to be expected; or the company has a disclosure obligation under foreign law. Separate disclosure obligations may be triggered depending whether a company is listed at the NYSE or Nasdaq. See for instance the disclosure requirements under Section 2 of the NYSE Listing Manual. Specific data breach notification requirements apply to financial institutions: see the breach notification requirements issued by the federal banking agencies under the US federal Gramm-Leach-Bliley Act (see n 13).

97 Such as the data breach notification requirements under the US HIPPA and HITECH Act (see n 12).

98 For instance, US export control laws require that a company obtains an export licence before certain technology is exported to specific countries. The US also imposes trade sanctions and export embargoes against certain countries (currently Cuba, Iran, Syria and Sudan) which are administered by the Office of Foreign Assets Controls (OFAC) of the US Treasury Department.

99 For instance, requiring that the works council be informed, or triggering security breach notification duties for telecommunication operators. See for the latter Article 2(4)(c) of the e-Privacy Directive, (Chapter 7, n 5). See also Kuner (Chapter 6, n 8), at 12.

100 As discussed in para. 9.2.

13.5.2 Comparison of the BCR regime with Madrid accountability requirements

Besides the general accountability provision, the Madrid draft proposal for an International Standard[101] also contains a list of compliance measures the application of which should be encouraged by the states. Compared to the BCR requirements, the Madrid draft for an International Standard has two additional measures, of which the requirement to implement a security breach management procedure is equivalent to additional requirement (viii)

[101] See Article 22 Madrid draft proposal (Chapter 8, n 14) for an International Standard: "States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others:

a) The implementation of procedures to prevent and detect breaches, which may be based on standardized models of information security governance and/or management.

b) The appointment of one or more data protection or privacy officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

c) The periodic implementation of training, education and awareness programs among the members of the organization aimed at better understanding of the applicable laws on the protection of privacy with regard to the processing of personal data, as well as the procedures established by the organization for that purpose.

d) The periodic conduct of transparent audits by qualified and preferably independent parties to verify compliance with the applicable laws on the protection of privacy with regard to the processing of personal data, as well as with the procedures established by the organization for that purpose.

e) The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the development and implementation thereof.

f) The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing.

g) The adoption of codes of practice the observance of which are binding and that include elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in case of non-compliance.

h) The implementation of a response plan that establishes guidelines for action in case of verifying a breach of applicable laws on the protection of privacy with regard to the processing of personal data, including at least the obligation to determine the cause and extent of the breach, to describe its harmful effects and to take the appropriate measures to avoid future breaches."

of the Working Party 29 in its Opinion on accountability. [102] There is one additional requirement not listed by the Working Party 29: "the implementation of a response plan that establishes guidelines for action in case of verifying a breach of applicable laws on the protection of privacy with regard to the processing of personal data, including at least the obligation to determine the cause and extent of the breach, to describe its harmful effects and to take the appropriate measures to avoid future breaches."[103]
Though not listed by the Working Party 29 in its Opinion on accountability, the Working Party 29 does require in its WP Opinions that the BCR audit program covers "methods of ensuring that corrective actions have taken place".[104] In respect of this Madrid requirement, the same comment applies as to the requirement to implement "internal procedures for the effective management and reporting of security breaches". A response plan as prescribed by the Madrid requirements is part of the follow up of an "event" (whether due to a security breach or other data protection violation discovered), and is covered by the overall framework obligation for a multinational as defined above to have in place "event management and complaint handling, i.e. procedures for responding to inquiries, complaints and data protection breaches."

13.5.3 Comparison with the accountability requirements of the Centre for Information Policy Leadership

In October 2010, the Centre for Information Policy Leadership[105] issued a discussion document "Demonstrating and Measuring Accountability"[106] (**Accountability Discussion Document**), which identifies 9 common

---

[102] The BCR requirements are also largely equivalent to the measures listed in the Madrid draft for an International Standard (Chapter 8, n 14). Additional requirements in the Madrid International Standard requirements are: (a) implementation of security breach management and notification procedure; and (h) implementation of a response plan for data protection law breaches.

[103] See requirement sub (h).

[104] See WP 108 (Chapter 10, n 7), para. 6, at 7, requiring that the BCR audit programme covers "methods of ensuring that corrective actions have taken place."

[105] The Centre for Information Policy Leadership acted as secretariat to a working group facilitated by various DPAs, which included 60 representatives of business, civil society, government, data protection and privacy enforcement agencies, and the European Data Protection Supervisor.

[106] The Centre for Information Policy Leadership, "Demonstrating and Measuring Accountability, A Discussion Document, Accountability Phase II – The Paris Project," October 2010, to be found at www.information policy centre.com (**Accountability Discussion Document**). It is to be expected that the Accountability Discussion Document will prove a significant indicator of what privacy accountability will have to encompass.

fundamentals that an accountable organisation should be prepared to implement and demonstrate to regulators.[107] As the Working Party 29 and Madrid requirements for accountability were already available at the time of drafting the Accountability Discussion Document, it is not surprising that the 9 "common fundamentals" identified by the Centre for Information Policy Leadership show a near complete overlap therewith. The added value of the Accountability Discussion Document is that it sets out the collection of requirements (i) in a more logical grouping of requirements; (ii) as more general obligations, while still describing in the explanatory notes to the requirements what is understood under the relevant general heading; and this all (iii) in a terminology which is (more) familiar to companies. The 9 common fundamentals identified by the Centre for Information Policy Leadership are:

1. **Policies**: Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.
2. **Executive Oversight**: Internal executive oversight and responsibility for data privacy and protection.
3. **Staffing and Delegation**: Allocation of resources to ensure that the organisation's privacy program is appropriately staffed by adequately trained personnel.
4. **Education and awareness**: Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations.
5. **Ongoing risk assessment and mitigation**: Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks.
6. **Program risk assessment oversight and validation**: Periodic review of the totality of the accountability program to determine whether modification is necessary.
7. **Event management and complaint handling**: Procedures for responding to inquiries, complaints and data protection breaches.
8. **Internal enforcement**: Internal enforcement of the organisation's policies and discipline for non-compliance.
9. **Redress**: The method by which an organisation provides remedies for those whose privacy has been put at risk.

Comparing for instance the fifth fundamental "Ongoing risk assessment and mitigation" with the Working Party 29 and the Madrid accountability

[107] See Accountability Discussion Document (n 106), at 6.

requirements, this fundamental seems to rightfully group the Working Party accountability requirements (i), (iii) and (ix) and the Madrid accountability requirement (h) under one heading. The explanatory notes to this fundamental explain this criterion by indicating that an organisation should:

> "be able to demonstrate the nature of their risk analysis. The organisation must show the rigor of the criteria against which analyses are carried out, and the suitability of those criteria to the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are made and steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective".

This seems indeed a proper summary of how multinationals achieve compliance in practice. Most multinationals will have a data security policy setting the security requirements (both operational and technical) based on the privacy and other risks of different categories of data (for instance, the highest security classification will include not only sensitive data, but also critical financial data of a company and confidential IP of company). The PIAs will subsequently show whether the data processed in a certain data processing system are properly classified in accordance with the classifications of this data security protocol. In case of data security or other data protection breaches there will be a security breach response procedure which sets out the procedures to be followed and the decisions to be made. A proper response procedure will require that, if an actual data security or other data protection breach occurs, the various decisions and steps taken will be documented along the way (in meeting notes etc), in order to be able to assess the adequacy of the response made and avoid future breaches. This practice corresponds with the explanatory notes to the fifth fundamental (ongoing risk assessment and mitigation):

> "To be accountable for its risk assessment and mitigation practices, organisations also should be able to demonstrate the nature of their risk analysis. The organisation must show the rigour of the criteria against which analyses are carried out, and the suitability of those criteria and the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are being made and steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective."

This fundamental encompasses a learning element, i.e. experiences in the past are translated into actions both to avoid future breaches as well as improve the related response. The fundamentals as identified by the Centre for Information Policy Leadership also provide a more overall learning

element by requiring as the seventh fundamental that organisations provide for: program risk assessment oversight and validation, where the totality of the accountability program is periodically reviewed to determine whether modification is necessary. The fundamentals as defined by the Centre for Information Policy Leadership therefore provide adequate "double loop learning" and are further an example par excellence of the required "triple loop learning" since the fundamentals have been drafted in a working group facilitated by various DPAs, which included 60 representatives of business, civil society, government, data protection and privacy enforcement agencies, and the European Data Protection Supervisor.[108]

My conclusion and recommendation is that EU legislators, when setting the main requirements for the BCR regime, should not add the additional accountability requirements as listed by the Working Party 29 and in the Madrid draft Standard, as these are too specific and may prove even counterproductive to achieving optimal compliance. But instead set these requirements in more general obligations based on the common fundamentals as defined by the Centre for Information Policy Leadership. An overall transparency requirement is missing from the common fundamentals. Again, also for reasons to be discussed as part of the evaluation of BCR as a form of TPR and CSR, my recommendation is to indeed make these transparency requirements part of the BCR regime. A final observation in respect of the common fundamentals identified in the Accountability Discussion Document is that these seem to be limited to accountability of a company in respect of **its own data processing operations**. Part of the business activities of any multinational is, however, that data are transferred to third parties outside the group of companies (which also constitutes processing of data). The Accountability Discussion Document does not identify common fundamentals in respect of accountability of companies in respect of such data transfers. This element is further discussed in Paragraph 13.6.

[108] See n 105.

Recommendation 12
To add as requirements for BCR:
- prescribe the reporting on BCR in the annual reports of company in a comparable format;
- the multinational should be transparent vis-à-vis the third-party beneficiaries as to the number of complaints received and the nature of these complaints under the internal complaints procedure;
- define the BCR requirements as to accountability in general obligations of the multinational on the basis of the common fundamentals defined by the Centre for Information Policy Leadership.

13.6 Proposal of the Working Party 29 to introduce accountability for data transfers

The Working Party 29 proposed in its Contribution to The Future of Privacy, to include a general provision in the revised Data Protection Directive "that controllers remain accountable and responsible for the protection of data for which they are controllers, even if the data have been transferred to other controllers".[109] This proposal is made by the Working Party 29 in the context of the section on BCR. According to the Working Party 29, the provision would fit in with introduction of the "accountability principle" in the revised Directive (subsequently discussed by the Working Party 29 in Chapter 6). This is mistaken. The accountability principle as envisaged by the Working Party 29 and discussed above entails that an independent obligation be included in the revised Data Protection Directive that the controller has to have adequate measures in place to ensure compliance with the material data protection principles. This is also in line with the accountability principle as included in the OECD Privacy Guidelines, [110] the APEC Privacy Framework,[111] the PIPED Act,[112] and in the Madrid draft proposal for

[109] WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 39.

[110] See at 14: "A data controller should be accountable for complying with measures which give effect to the principles stated above.' The principles stated above concern the material processing principles"

[111] APEC Privacy Framework (Chapter 6, n 38), Principle 26: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above."

[112] See PIPED Act (Chapter 7, n 78) Section 5, 4.1.3 first sentence: "An organization is responsible for personal information in its possession or custody, including information that has been

International Standards.[113] The additional provision, as proposed by the Working Party 29, that controllers remain accountable and responsible for the protection of data for which they are controller also after transfer, merely provides for external liability of the original controller for anything that happens with the data after the data have been transferred by him, this while these data are then outside his control.

The proposal by the Working Party seems to be leading to an accumulation of the requirements of two different systems to regulate cross-border transfers. As seen in Paragraph 6.2, there are systems which are based on a territorial approach for data transfers (based on "adequacy" of protection in **countries**) and systems which have chosen the organisational approach (based on accountability of organisations). Accountability does not specifically restrict cross-border data flows, but imposes compliance obligations on parties that transfer personal data on a transborder basis. One example is the APEC Privacy Framework.[114] Some APEC Member Economies have already implemented the accountability principle (also for data transfers), such as the Canadian PIPED Act.[115] Accountability may

---

transferred to a third party for processing."; and Section 5, 4.1.3, second sentence: "The organization shall use contractual or other means to provide a comparable level of protection while the information is processed by a third party."

113 See Madrid draft proposal for International Standards (Chapter 8, n 14), Article 11: "the responsible person shall: a. take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in paragraph 23."

114 See Principle 26: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

115 Personal Information Protection and Electronic Documents Act, 200, C.5, to be found at <www.laws.justice.gc.ca>. See Schedule I, para. 4.1.3: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." Or, as the Guidelines for processing personal Data across Borders (January 2009), at 3 state: "In contrast to this state-to-state approach, Canada has, through PIPEDA, chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an

require organisations to take steps such as implementing appropriate privacy policies, training employees, implementing monitoring and auditing of compliance and adopting mechanisms to enforce compliance.[116]

As an exception to the territory-based system of the EU, the EU introduced the BCR regime that reflects the organisational (i.e. the accountability) approach to regulate **inter-company data transfers**. As soon as the multinational with BCR transfers data outside the company group to a third party in a non-adequate country, however, the regular EU data transfer rules have to be complied with (i.e. the EC Model Clauses, consent of data subjects, etc). It is doubling requirements if companies with BCR have to comply both with the EU transfer rules (thus have to enter into the EC Model Clauses with a third-party supplier) and on top of that be accountable for any data protection breach by such third party. This is not to say that I would prefer the EU data transfer rules above the accountability approach to data transfers. The accountability approach in fact seems to be the better alternative.[117] The main reason for this is that even if data are transferred to

---

organization in another jurisdiction for processing. However, under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement."

116 Galway project and Centre for Information Policy leadership, "Data Protection Accountability: The essential Elements, A document for Discussion" (2009), to be found at <www.hunton.com>.

117 Kuner (Chapter 6, n 52), Chapter 16 at 271, is also in favour of replacing the present adequacy system of the EU by the accountability approach, since "use of the accountability approach need not in practice result in a lessening of the level of data protection for international data transfers." However, see Kuner (Chapter 6, n 8), at 41, where he concludes that "neither of the two default systems seems inherently better than the other, each one has inherent advantages and disadvantages (…)." Kuner further concludes that "what is needed is for the two approaches to co-exist, whereby the solution selected by a country should be accompanied by measures to avoid its inherent disadvantages, as otherwise the first approach will tend to be excessively bureaucratic and the second too reactive." The position of the Rand Report (Chapter 6, n 27), is not completely clear. Nowhere in the report is a clear choice made for the one or the other system. At 43, however, the Rand Report recommends that as the adequacy approach to data transfers at present proves ineffective, "[t]he promotion of alternatives – such as SCCs and BCR – should become a greater priority." This seems to be an indication that it assumes the present adequacy system is continued. At 49, however, the Rand Report seems to (implicitly) recommend the accountability approach for data transfers, where it recommends recasting the Directive "as an articulation of General Principles and Outcomes." The Rand Report subsequently lists 6 General Principles (Legitimacy, Purpose restriction, Security and confidentiality, Transparency, Data subject participation and **Accountability**). These Principles do not include data transfer requirements, but instead the 6th General Principle

an 'adequate country', enforcement of data protection violations may prove problematic even in such 'adequate countries' (see for examples Paragraph 8.3). Further, in practice the EU approach requires a full adequacy assessment of the data protection laws of each country and proves insufficiently productive in achieving global data protection coverage.[118] Key trade partners of the EU like China, Japan, Brazil, India and the US are not covered, which inevitably leads to non-compliance in practice.[119] The

---

provides that those processing data are held accountable for the outcomes (of the first 5 principles). The Centre for Information Policy Leadership New Approach to International Transfers (Chapter 10, n 49), at 2, also proposes taking the accountability approach to data transfers: "We believe that a new framework for international data transfers, built on the experience with BCR and explicitly grounded on the Accountability principle, could be achieved with "Binding Global Codes"(BGC) (…) The BGC proposal allows an organisation to develop and implement its own bespoke Code with a set of binding rules for demonstrating and ensuring compliance with the Data Protection Principles and their practical implementation on a worldwide basis. The Code must be published and the organisation be held accountable for fulfilling its terms."

[118] See also the findings of the Rand Report (Chapter 6, n 27), at 43: "The study shows that the Directive's focus on adequacy assessments and the strategies to achieve this are inefficient and insufficiently productive in an increasingly globalised data market. Key economic trading partners are not covered by adequacy findings, which means that alternatives should play a crucial role in practice. When these are not easily available, non-compliance is de facto encouraged. The promotion of alternatives – such as SCCs and BCR – should become a greater priority. The use of these alternatives should be facilitated for data controllers in any Member State, as was already noted above. In addition, it was noted by several interviewees that current adequacy assessments were not sufficiently effective, focusing mostly on a review of regulations and declared policy, rather than on the effectiveness of data protection. If the credibility of the adequacy assessment system is to be maintained, assessments should consider whether the principles put forward by the Directive are achieved in practice, which includes issues such as the actual independence of DPAs and court rulings on data protection issues, the availability of sufficient means to allow DPAs to operate in practice, and the existence of actual enforcement actions." See also Kuner (Chapter 6, n 52), at 263.

[119] See quote from the Rand Report in (Chapter 6, n 27), and Kuner (n 8), at 29: "The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries." See also Kuner (Chapter 6, n 52), at 263, stating that "an examination of the current adequacy system shows that it is cumbersome, expensive, slow, and sends the wrong message to third countries." He further calculates that with the present pace of approval of adequacy decisions, it will take 130 years to achieve some sort of global coverage. Taking into account that there are 192 member states of the United Nations only in total about 48 countries are considered adequate (27 Member States, 3 EFTA countries, 8 countries with an adequacy ruling (see Chapter 6, n 18) and 10 countries that have

accountability approach to data transfers seems to be more flexible in tailoring to the transfers at hand and even facilitates some form of central enforcement against the data exporter who is often in the country where the data subject is domiciled (see Paragraph 8.4.4). This being said, accumulation of the requirements of both systems is not advisable.

In any event the provision proposed by the Working Party seems more stringent than the accountability provision in respect of data transfers as included, for instance, in the APEC Privacy Framework. Principle 26 APEC Privacy Framework requires that "When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." This provision therefore does not provide that the exporting organisation is generally accountable for the data also after transfer. Similarly, under the Canadian PIPED Act, companies are not accountable per se for any breach after data transfer, but are accountable only for the measures that could be required of such company to provide a comparable level of protection taking, for instance, into account the adequacy level of the country of destiny.[120]

Finally, the provision proposed by the Working Party 29 is in such general terms ("controllers remain accountable and responsible for the protection of data for which they are controllers, even if the data have been transferred to other controllers"), that liability of the multinational may extend beyond its responsibilities under its BCR. The provision as proposed by the Working Party 29 does not refer to the BCR regime and could therefore include any breach by the relevant third party of his respective national data protection laws (such as a breach of national notification obligations of such third

---

ratified Convention 108 and the Addendum to Convention 108 (and are not already included in the aforegoing countries (see Chapter 8, n 11). This leaves about 144 possible candidates. Kuner (Chapter 6, n 52), at 264 notes that "half of these would never be found adequate for various reasons, such as they do not have a democratic system of government, a functioning legal system, or other basic requirements for adequacy." It is clear that the adequacy solution will not lead to a global coverage (at least at any time in the foreseeable future).

120 See Chapter 6, n 51. The proposal put forward by the Centre for Information Policy Leadership New Approach to International Transfers (Chapter 10, n 49), at 9, is not clear on what the extent of accountability of the multinational is. The Centre proposes that the revised Directive will authorise data transfers by a multinational to non-adequate countries if such a multinational has adopted a Binding Global Code providing that "the data is processed, and continues to be processed, in accordance with the Code."

party). I therefore recommend that EU legislators not follow the proposal of the Working Party 29.

Recommendation 13
Not to follow the recommendation by the Working Party 29 to include a provision in the revised Data Protection Directive that controllers remain accountable and responsible for the protection of data for which they are controllers, even if the data have been transferred to other controllers.

13.7 The way forward: accountability for onward transfers in BCR

13.7.1 Which system to take as a starting point?

The question left is: then what? Should I recommend European legislators abolishing the adequacy system and adopting the accountability approach for data transfers? Strangely enough it does not matter which system is chosen by EU legislators as both systems can serve **as a starting point only**. Both systems in unadapted form are not attractive. As one author puts it: "otherwise the first approach [the adequacy approach] will tend to be excessively bureaucratic and the second too reactive".[121] For any of the two systems to be acceptable, additional measures are indicated. From the EC Communication on revision of the Directive,[122] I derive that the European Commission intends to stick with the adequacy approach, where it intends to "clarify the Commission's adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organisation", but also intends to mitigate negative aspects of the adequacy system where it intends to "improve and streamline the current procedures for international data transfers, including legally binding instruments and 'Binding Corporate Rules' in order to ensure a more uniform and coherent EU approach vis-à-vis third countries and international organisations". This approach seems to provide ample room to keep the benefits of an adequacy approach (which stimulates third countries to adopt adequate data protection laws) while also providing for more flexible organisational measures which may mitigate the downsides of the adequacy system. For the organisational measures to indeed be able to mitigate the downsides of the adequacy approach, EU legislators will need to adopt a far more flexible approach than has until now been the case in respect of the organisational measures. The present inflexible approach

[121] See citation Kuner in Chapter 6, n 53.

[122] EC Communication on revision of the Directive, (Chapter 6, n 34), at 12.

taken vis-à-vis for instance the EU Standard Contractual Clauses, is certainly not the way forward. One example hopefully clarifies this.

The EC Standard Contractual Clauses for Processors have been recently updated to cater for the situation where the controller involves a main processor, who in its turn involves sub-processors. This is by now a very common feature in large outsourcing arrangements.[123] Before the update of the Clauses, the controller had to enter into EC Standard Model Clauses with each of the non-EU entities of the supplier involved in the services. The aim of the updated Clauses was to simplify this situation where the multinational would have to enter into EC Standard Contractual Clauses with the main supplier only. The updated Clauses, however, now appear to apply only if the main processor is established outside the EU,[124] even though in most large outsourcing arrangements multinationals enter into the main outsourcing contract with the group company of a supplier in their own jurisdiction. This supplier entity will subsequently sub-contract with its group companies outside the EU. For those cases the EC Standard Contractual Clauses do not apply, which leaves these parties with the situation as before the updated Clauses were issued, requiring the multinational to enter into multiple EC Standard Contractual Clauses with each of the non-EU entities of the supplier involved in the services.[125] The same applies when the multinational has more entities in the EU. The new EC Standard Contractual Clauses do not facilitate that these will be jointly signed by all EU group companies of the multinational.[126] Here again each of the EU group companies of the multinational has to enter into the EC Standard Contractual Clauses with each of the non-EU entities of the supplier involved in the services. If ever an unnecessary administrative burden is created, this is the example. Multinationals and their multinational suppliers entering into an outsourcing arrangement on a global basis each have convincing reasons to

---

123 Recitals 16 and 17 to the EC Standard Contractual Clauses for Processors (Chapter 7, n 42). See also Kuner (Chapter 7, n 42), at 5.

124 Recital 23 EC Standard Contractual Clauses for Processors (Chapter 7, n 42); Kuner (Chapter 7, n 42), at 5 and 7; Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (data controller to data processor) (WP 161), 5 March 2009 (**WP Opinion on Standard Contractual Clauses for Processors**), at 3; and FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, dated 12 July 2010 (WP 176) (**WP FAQs on Standard Contractual Clauses for Processors**), at 3.

125 WP Opinion on Standard Contractual Clauses for Processors (n 124), at 3.

126 WP FAQs on Standard Contractual Clauses for Processors(n 124), at 7 (FAQ 5).

ensure that their respective group companies are indeed bound by this arrangement. Why on earth the data protection obligations would not be able to follow that contractual structure but would require separate individual contracts is truly beyond me. What is relevant is that the multinational imposes binding obligations on the supplier and all its group companies involved. By setting as a requirement that for that purpose separate contracts have to be concluded, unnecessary administrative burdens are created without any added value as to material data protection, which is a recipe for non-compliance which in turn undermines the legitimacy of the material data processing principles which these norms aim to protect.[127] Such requirements should be avoided at all cost.

13.7.2 Define the core principles only

I propose that EU legislators opt for an accountability approach, by limiting themselves to setting the core material data protection requirements that need to be put in place between multinationals and their external suppliers, without prescribing the **means and form** by which these requirements have to be achieved. Again, multinationals are well able to decide on the most optimal legal instrument to achieve the prescribed protection. My proposal deviates from the proposal made by the Centre for Information Policy. The Centre proposes that the revised Directive will authorise data transfers by a multinational to non-adequate countries that has adopted a Binding Global Code that provides that "the data is processed, and continues

[127] That an overly strict approach undermines the credibility of the Data protection Directive is acknowledged in the First Report on the Data Protection Directive (Chapter 6, n 26), at 19: "An overly lax attitude in Some Member States [as to data transfers] (…) risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export. An overly strict approach, on the other hand, would fail to respect the legitimate needs of international trade and the reality of global telecommunications networks and risks creating a gap between law and practice which is damaging for the credibility of the Directive and for Community law in general." A similar observation is made by Christopher Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2) (October 1, 2010), International Journal of Law and Information Technology, Vol. 18, 2010. Available at SSRN: http://ssrn.com/abstract=1689495, at 13, noting that "when the jurisdictional scope of the law is much broader than the chance that the law will be enforced, there is a risk that respect for the law will be diminished", and at 15: "a low chance of enforcement may cause controllers to regard data protection rules as a kind of bureaucratic nuisance rather than as 'law' in the same category as tax laws, employment laws, etc."

to be processed, in accordance with the Code."[128] This presupposes that the multinational transferring data to its external suppliers imposes the terms of its Global Code on its external suppliers. This will not always be necessary. It is possible that the external supplier has its own Global Code (maybe even a BCR for Processors). In that case the data may be transferred to such supplier without the multinational having to impose the terms of its Global Code on the external supplier. Suppliers processing data on behalf of many multinationals may be unable to apply a Global Code from each of those multinationals. What is relevant is that the data obtain an adequate level of protection, not that the original Global Code remains applicable to all other parties subsequently processing that data in the chain. The same may apply if the data processing by the external supplier is subject to the data protection law of a country that obtained an adequacy ruling.[129] My conclusion is that the accountability requirements of multinationals under the BCR regime for data transfers to third parties should not be to impose the BCR on such third parties, but should require a more thoughtful defining of the core data protection elements that have to be safeguarded.

13.7.3 Focus on alternative means of redress

EU legislators in setting these core requirements should focus not on traditional judicial legal rights and remedies of individuals covered by BCR, but concentrate on means of redress that actually achieve compliance in practice.[130] One example is provided as an illustration.

In Paragraph 11.5, I explained that the EC Standard Contractual Clauses contain a third-party beneficiary clause, granting individuals rights against the data importer. The individuals obtain the right to address the data importer in case of a data protection breach by such data importer and, if this data importer goes bankrupt, the individual may address the data exporter instead. Given the practical obstacles for individuals bringing a claim against a data importer in for instance India, these rights may look good on paper, but have in practice no added value for individuals. Worse, as the rights are prescribed in detail in the EC Standard Contractual Clauses which may not be amended, multinationals contracting with the data

---

[128] See the Centre for Information Policy Leadership New Approach on International Transfers (Chapter 10, n 49), at 9.

[129] See, for instance, the draft Australian data protection law, which combines the adequacy approach and the accountability approach by providing that the multinational transferring data will remains accountable for the data also after transfer unless the data are transferred to an adequate country. See Chapter 31 of the Australian Law Reform Commission report at 1087-1113

[130] Kuner (Chapter 6, n 52), at 271,

importer have no interest in improving on these rights, even though they certainly would have the bargaining power to do so. Why not include in the "core principles" for legally binding instruments that the instrument should provide for "proper means of redress by individuals in case of onward transfers of their data" (as the BCR regime already requires in respect of data processing by the multinational itself). My expectation is that within a short period of time, outsourcing contracts will for instance provide that the data importer has to accept that individuals may file complaints via the complaints procedure of the multinational also against the data importer, that the data importer is required to respond to such complaints within certain time limits and to reimburse the multinational for any costs incurred in respect of facilitating the whole process. Alternatively, the parties to the outsourcing agreement may provide that complaints will be processed by the outsourcing supplier, being the party responsible for the factual processing and best placed to respond to complaints about security breaches. The outsourcing contract may subsequently provide that the multinational has to cooperate and respond to complaints relating to the data processed itself, etc. In other words, the requirement should be that appropriate redress is organised; the means how to achieve such redress should be left to the parties involved.

13.7.4 Conclusion and starting points for core principles

My conclusion is that the BCR requirements should provide for core principles as to what can be expected of a multinational when involving third parties in the processing of its personal data (whether within or outside the EU). As with the "binding legal instruments" discussed above, these should be set in general accountability requirements and not be specified as mandatory contractual provisions to be included in each of the contracts between a multinational and third parties in the context of which data are transferred. It is beyond the scope of this dissertation to list exhaustively the main core accountability requirements when controllers transfer data to third parties (whether a controller or a processor). I recommend that an inventory of these core requirements be made similar to the inventory made by the Centre for Information Policy Leadership of the accountability requirements for **internal compliance** by the multinational. My recommendation to EU legislators is to delegate this task in the revised Directive to the European Commission in order to ensure that these requirements remain adaptable to changing circumstances.[131] The Commission can then preferably organise a project similar to that

[131] On the possibility of delegation to the Commission, see para. 10.6.

undertaken by the Centre for Information Policy Leadership, in order to ensure triple-loop learning (see Paragraph 13.2.2).

For this inventory some general starting points can be formulated.
One of these requirements should be that individuals will have "proper means of redress". I already identified this as a requirement as part of the evaluation of proper supply chain management (see Paragraph 11.5).

Mandatory monitoring and auditing of all data processing operations of the data processor should not be one of the requirements (see Paragraph 11.5). It is sufficient that the multinational has a right to do so only. Whether it is indicated that a multinational exercises such rights will depend on the risk assessment of the relevant data processing.

A more general guideline for drafting the inventory is the realisation that data processing is performed in networks rather than in neat one-to-one relationships. [132] Research in other areas of law shows an inherent weakness of a chain of contracts along the supply chain, replicating the required contractual clauses where regulatory obligations are passed on in the chain. [133] A straightforward requirement for multinationals to impose certain contractual obligations on its contract party may therefore not do the trick. The main objective of supply chain management is to minimise risks of non-compliance and to improve effectiveness and efficiency of control **at the source of such risk**.[134] Rather than imposing requirements on all parties in the network, a more productive exercise may be to first identify the risks, the source of these risks and then allocate responsibilities accordingly. A factor in allocating responsibilities may also be which of the parties has the best contracting power to enforce compliance. Below is an illustrative example.

The Data Protection Directive imposes obligations on the controller of data. At the time the first outsourcing transactions were concluded it was indeed the controller who was in the driving seat as to imposing all terms relating to the outsourcing, including security requirements and whether data were transferred to non-EU countries or not. Today, with more commoditised

---

[132] See Trudel (Chapter 11, n 67), Chapter 19, at 332-334; and Raab and Koops (Chapter 8, n 23), at 220, who have attempted to map the landscape of privacy actors in the online data protection arena "showing a remarkable range of diverse and versatile actors with many potential interconnections and interrelationships."

[133] Cafaggi (Chapter 11, n 31), at 9.

[134] In similar terms as to the management of risks in relation to food safety, see Cafaggi (Chapter 11, n 31), at 18.

outsourcing services (like straightforward "server management"), contractual terms on security and whether data transfers are taking place or not are (as much) dictated by the outsourcing supplier.[135] Looking at the relationship from a risk perspective, security breaches may occur at the data processing operations of the outsourcing supplier (especially when in transit to offshore group companies) rather than at the premises of the controller. Imposing an obligation on the controller to have proper security breach incident procedures in place and an obligation to impose a similar obligation on the outsourcing supplier may therefore not do the trick. The two security incident procedures will have to coincide, resulting in a joint handling of the relevant incident, each to the extent they have control over the relevant IT. The security incident issues will multiply the more sub-processors are involved. In this case, solutions will not be forthcoming by a contractual chain, but by allocating responsibilities where they are best placed. To reflect this, the BCR requirements should therefore not require a mandatory contractual provision that the processor should have data security procedures in place (as all will have these in standard form), but should require the multinational to allocate the relevant responsibilities as to data security breaches to the party in the network that is best placed and this in such a manner that accountability for the whole is achieved. The risk that by one-to-one contracting data protection obligations may be diluted and even prevent effective control is also recognised by the Working Party 29 in its Opinion on controller and processor[136]:

> "The strategic issue here is that - with a plurality of actors involved in the process – the obligations and responsibilities stemming from data protection

[135] Teme (Chapter 6, n 27): "An additional dichotomy in need of review is that between controllers and processors. Data protection law allocates responsibility and delineates duties according to a categorization of an organization as a "controller" or "processor." A controller, defined in the EU DPD as the party that "determines the purposes and means of the processing of personal data," is traditionally viewed as the owner of the database, the one who has a direct relationship with the individual and therefore locus of liability. The processor (or "mere processor") is traditionally perceived as a service provider, a servant to the master-controller, whose sole responsibility is keeping the data secure. Yet how far this description is from market reality today, where layer upon layer of service providers (processors?) undertake an increasing role in the clients' (controllers?) business processes, including providing consulting services, driving innovation, and managing change. Moreover, with the advent of cloud computing and its architecture as a stack of infrastructure, platform and software layers, the neat distinction between controllers and processors has muddled. This is a critical matter, since in the absence of a clearly identified controller the framework remains teetering without a focal point for responsibility/accountability."

[136] WP Opinion on controller and processor (Chapter 7, n 7), at 27.

> legislation should be clearly allocated and not dispersed along the chain of outsourcing/subcontracting. In other words, one should avoid a chain of (sub-)-processors that would dilute or even prevent effective control and clear responsibility for processing activities, unless the responsibilities of the various parties in the chain are clearly established."

Taking it one step further, even if the responsibilities of the parties may be clearly established in the network, rather than fragmented liability of the different parties accumulating to full liability, liability of each should be for the outcome of the network as a whole. In its Opinion on controller and processor, the Working Party 29 also seems to recognise the risk of fragmentation and to consider solving this by joint and several liability for all parties involved:[137]

> "the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing. (…) Against this background, it can be argued that joint and several liability for all parties involved should be considered as a means of eliminating uncertainties, and therefore assumed only in so far as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances."

Thought should be given to the question whether the present set-up of the Data Protection Directive where the controller is the sole bearer of all data protection obligations is indeed the best **incentive** to achieve compliance in case of complex data processing operations. In light of the diminishing contracting power of multinationals vis-à-vis their multinational outsourcing suppliers, an obligation on **all parties** involved in a data processing (whether controller or data processor) to achieve accountability as to the end result, may ultimately prove the better stick. This may work as an incentive for all parties to come to a proper allocation of obligations in relation to the network. By separating the contractual form from the liability regime, it is left to the parties to allocate responsibilities where they are best placed.[138]

---

[137] WP Opinion on controller and processor (Chapter 7, n 7), at 24.

[138] Cafaggi (Chapter 11, n 31), at 25 – 26.

Recommendation 14
Define the core accountability principles for the situation when a multinational transfers personal data to third parties, taking into account the guidelines identified in this Paragraph.

13.8 Solution of Working Party 29 to achieve joint responsibility of controller and processor

As a side issue, I note that the Working Party 29 in its Opinion on controller and processor[139] has taken a first step in the direction of achieving joint responsibility of controllers and processors in respect of a joint processing. Rather than a clear classification of a party as either a controller or a processor, it seems that in case of complex joint processing operations, the Working Party 29 has a preference to qualify all parties involved as to the different aspects of the processing as a (joint) controller rather than some as data processor only, to achieve maximum responsibility for the processing as a whole of all parties in order to avoid pointing fingers or gaps in liability:[140]

> "The bottom line should be ensuring that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties."

The Working Party 29 achieves this by (insofar as relevant here) three instructions on the concept of controller. The first is that the concept of controller should be considered as a **functional** one, in the sense that it is intended to allocate responsibilities where there is **factual** influence, and thus based on a factual rather than a formal analysis.[141] A telling example given by the Working Party 29 itself is the SWIFT example:[142]

> "The fact itself that somebody determines how personal data are processed may entail the qualification of data controller, even though this qualification arises

139 See (Chapter 7, n 7).
140 WP Opinion on controller and processor (Chapter 7, n 7), at 22.
141 WP Opinion on controller and processor (Chapter 7, n 7), at 9
142 WP Opinion on controller and processor (Chapter 7, n 7), at 11.

> outside the scope of a contractual relation or is explicitly excluded by a contract. A clear example of this was the SWIFT case, whereby this company took the decision to make available certain personal data - which were originally processed for commercial purposes on behalf of financial institutions - also for the purpose of the fight against terrorism financing, as requested by subpoenas issued by the U.S. Treasury."

The Working Party 29 further introduces the concept of **pluralistic control**. According to the Data Protection Directive it is possible that multiple parties may be responsible for a certain processing activity (and qualify as co-controllers). In its Opinion the Working Party 29 makes clear that this concept of pluralistic control refers not only to cases where the controllers **equally** determine purposes and means and are **equally** responsible for a single processing operation (i.e. the co-controllership as implied in the definition of controller).[143] According to the Working Party many other forms and combinations of "pluralistic control" are possible, where one party is controller for certain parts, aspects or stages of the processing and another controller for other parts, aspects or stages. [144]

The third instruction of the Working Party 29 concerns the elements of the definition of controller: "purpose and means".[145] According to the Working Party 29 the determination of the "purpose" of a processing activity is reserved to the controller. Whoever makes this decision is (de facto) controller. The determination of the "means" of processing can be delegated by the controller, as far as **technical or organisational questions** are concerned. Means however, does – according to the WP 29 - not only refer to the technical ways of processing personal data but also to the "how" of processing, which includes questions like "which data will be processed", "which third parties will have access to these data", "when will data be deleted", etc. Determination of the "means" therefore includes both technical and organisational questions where the decision can be delegated to processors (e.g. "which hardware or software will be used?") but also essential elements which are traditionally and inherently reserved to the determination of the controller, such as "which data will be processed?", "how long will they be processed?", "who will have access to the data?".[146] Delegation of these decisions to a processor may well have consequences for the qualification of the processor as a controller.

---

143 WP Opinion on controller and processor (Chapter 7, n 7), at 19.

144 WP Opinion on controller and processor (Chapter 7, n 7), at 18.

145 For the full definition of controller, see Article 2 (d) Data Protection Directive (Chapter 6, n 2).

146 WP Opinion on controller and processor (Chapter 7, n 7), at 14.

In line with the above, one would expect that security measures would fall under "technical and organisational means", which traditionally can be delegated by the controller to the processor (without changing its qualification as a processor). The Working Party 29 confirms this but also highlights that in **some legal systems** decisions taken on security measures "are particularly important, since security measures are explicitly considered as an essential characteristic to be defined by the controller".[147] The Working Party 29 itself indicates that this raises the issue of which decisions on security may entail the qualification of controller for a company to which processing has been outsourced, but does not answer this question.

The Working Party 29 gives a number of examples to illustrate how the instructions above work out in practice. The example that best illustrates how the Working Party 29 achieves joint controllership for the security measures is the example of an e-government portal, where certain public administration units outsource the servicing of requests of citizens for copies of public documents to a third-party service provider that will host such e-governmental portal. There is no question that the public administration units are the controllers in respect of the respective documents they issue. The party operating the e-governmental portal is instructed to perform the issue of the copies on behalf of the relevant public administration units and is prohibited to use the documents for any other purposes. The fact pattern seems to indicate that the portal provider qualifies as a data processor as to the servicing of the requests of citizens on behalf of the public administration units. Based on the above instructions, the Working Party 29 however concludes that the portal provider qualifies as a controller and is therefore responsible for the security of the transfer of the data from the user to the administration's system as this transfer is an essential part of the services provided for by the portal.[148]

> "Example No. 11: E-Government portals
>
> E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the

147 WP Opinion on controller and processor (Chapter 7, n 7), at 15.

148 WP Opinion on controller and processor (Chapter 7, n 7), at 21.

> citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit. These controllers, among other obligations, will have to ensure that the system to transfer personal data from the user to the public administration's system is secure, since at a macro-level this transfer is an essential part of the set of processing operations carried out through the portal."

For a number of reasons I do not agree with this interpretation of the concept of controller. In the first place the interpretation is not in accordance with the legislative history of the Data Protection Directive. It may be derived from the history that at the time it was contemplated that two parties could jointly decide on the purposes and means of the processing as a whole and as such be co-controllers[149] and further that different parties could be responsible for different **parts** of a data processing operation, each deciding for its part **the means and purposes of the processing** and as such being co-controllers.[150] What was not contemplated at the time was that a party could qualify as a controller based on the single fact that he would be tasked with one **aspect** of the processing (like decisions on security), without (also) determining the purpose and means of (part of) the processing itself. The history makes clear that a controller qualifies as the person who in last instance is **responsible** for the decisions on the

[149] See the opinion of the European Commission on the amendments of the European Parliament to the draft Data Protection Directive, accepting the amendment to Article 2(d) based on the possibility that in the context of one processing operation, "a number of parties may *jointly determine the purpose and means of the processing* to be carried out." The Commission subsequently states: "It follows from this that, in such case, each of the co-controllers must be constrained by the obligations imposed by the directive so as to persons about whom the data are processed". See the Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (95) 375 final, amending the Proposal of the Commission, at 3.

[150] See the leading commentary on the Data Protection by Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997), at 112 -113. Simitris was one of the drafters of the Directive and is generally considered to have "grandfathered" it. As this book is no longer generally available, here follows an unauthorised translation into English: "The definition in the Directive is on purpose functional, so that when there are separate parts of a data processing complex, different parties determine the purposes and means of this data processing complex, and these are jointly responsible for the data processing. The Directive does not specify which controller obligation (e.g. information obligations, the obligation to keep data up to date, the obligation to secure the data), should be allocated to which party and this will have to be decided based on the meaning and purpose of the relevant provision of the Directive."

purposes and means, rather than the person who performs (parts of) the processing. [151]

In the example of the Working Party 29 on e-government portals, the third-party provider has no decision-making power as to the purposes of the processing of the data, who has access to the data, how long the data will be stored, etc. The public units remain (and should remain) in control. If the services had not been outsourced, the government would probably have set up its own portal for e-governmental services (as already done by numerous public units in many countries). The fact that the third-party provider probably decides on the security measures for the portal (and is probably best positioned to do so), does not change the fact that he does not have decision-making power as to the purposes and means of the processing. Though I agree with the Working Party 29 that it may be advisable to make data processors (in addition to controllers) responsible for data security, this should be achieved by making (also) the data processor directly responsible for the security of the processing in the revised Directive, rather than through a creative interpretation of the concept of controller.

Making the processor a controller has many consequences under the Data Protection Directive that have unpredictable and undesired results. Many obligations are tied in with the qualification of a party as the controller, such as the provisions on applicable law as well as an obligation to comply with requests of individuals to access or correct their data. By making the processor a controller, the original controller no longer has decision-making power whether to comply with such request to access or correct data. This may seem a minor point, but by now there are court cases in Member States where abuse is made of access rights by individuals (by making repeated and

[151] See the Explanatory Memorandum of the European Commission to the Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final – SYN 287, 15 October 1992, at 11: "The controller is the person ultimately responsible for the choices governing the design and operation of the processing carried out (usually a chief executive of the company), rather than anyone who carries out processing in accordance with the controller's instructions. That is why the definition stipulates that the controller decides the objective of the processing. This is in line with Parliament's Amendment No. 17. The controller may process data himself, or have them processed by members of his staff or by an outside processor, a legally separate person acting on his behalf." This Explanatory Memorandum is no longer available on the site of the European Commission. It can be retrieved from Archive of European Integration of the University of Pittsburg, at: <http://aei.pitt.edu/10375>.

unbridled requests or obtaining information for other purposes than to assess data protection compliance).[152]

Further, the instruction of the Working Party 29 that delegation of security measures may entail that a processor becomes a controller, this "dependent on how important national law finds such security measures", is not workable in practice and is further contrary to EU law. Community concepts like controller have their own autonomous meaning independent of the national laws of the Member States.[153]

Finally, situations such as the SWIFT case where processors change colour over time depending on incidental decisions of processors are unfit to base data compliance on. As indicated, issues of applicable law depend on the qualification of a party as a controller which should be a predictable concept. Again, the attempt of the Working Party 29 to impose joint obligations on data controllers and processors in joint processing situations is understandable and even commendable, but should not be achieved by an extensive interpretation of the concept of controller. Legal certainty requires that clarity is given by EU legislators on whether the distinction between controller and processors is still viable given the present network economy where joint processing operations are the rule rather than the exception and if so, whether this should lead to changes in imposing certain data protection obligations also on processors (or jointly on controllers and processors).

13.9 Conclusion as to accountability

The conclusion is that the present requirements for BCR will not require substantive updating to be aligned with the accountability principle as envisaged by the Working Party 29, the Madrid Draft Proposal for International Standards and the general literature on the accountability principle in other fields of law. Indeed, the conclusion seems to be justified

---

[152] See for example the case law in the Netherlands in respect of the refusal by a number of banks to to (fully) comply with the mass requests by disappointed investors to access their personal data processed by these banks for use in their court cases against these banks. See on these court cases (from the perspective of the banks) W.A.K. Rank and A.J. Haasjes, "'Misbruik van de Wbp in civiele procedures tegen financiële instellingen", Tijdschrift voor Financieel Recht 2005-12, at 370-379 and (from the perspective of the investors) A.J.E. van den Bergen, 'De Wet bescherming persoonsgegevens in de financiële procespraktijk', Tijdschrift voor Financieel Recht 2005-10, at 296- 306.

[153] This also according to the Working Party itself, see the WP Opinion on controller and processor (Chapter 7, n 7), at 8.

that the BCR regime has served as a template for a model data compliance program for all companies (also in case the relevant company does not transfer data across borders).[154] This is quite a step from the initial position by the Working Party 29 where BCR were grudgingly accepted as an alternative tool for data transfer compliance.[155] This being said, EU legislators are well advised to (i) introduce incentives for multinationals to implement BCR; (ii) introduce transparency requirements; (iii) update the BCR requirements in line with the generic accountability principles as defined by the Centre for Information Policy Leadership; and (iv) list the core accountability requirements when multinationals transfer data to third parties outside their group of companies (whether a controller or a processor). An inventory of these last requirements should be made similar to the inventory made by the Centre for Information Policy leadership in respect of **internal compliance** by the multinational.

Recommendation 11
Introduce incentives for multinationals to adopt BCR, such as:

- risk-based sanctions for a violation of data protection by multinationals that have implemented BCR (whereby the implementation of a proper compliance programme is a mitigating factor);
- providing that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States (as per *Recommendation 10*), or as next best alternative, providing that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA (see *Recommendation 9*);
- abolishing the notification requirements, or, as next best alternative, providing for the possibility of central notification of all data processing of a multinational to the Lead DPA.

154 See WP Opinion on the principle of accountability (Chapter 1, n 15), at 15. Obviously, the BCR requirements will have to be 'scaled' (i.e. depending on the size and nature of the data processing operations of a company. On scaling see the WP Opinion on the principle of accountability (Chapter 1, n 15),paras. 43 – 48 and 51.

155 WP 74 (Chapter 10, n 2), at 6.

Recommendation 12
Add as requirements for BCR:

- prescribing the reporting on BCR in the annual reports of company in a comparable format;
- the multinational should be transparent vis-à-vis the third party beneficiaries as to the number of complaints received and the nature of these complaints under the internal complaints procedure;
- defining the BCR requirements as to accountability in general obligations of the multinational on the basis of the common fundamentals defined by the Centre for Information Policy Leadership.

Recommendation 13
Not to follow the recommendation by the Working Party 29 to include a provision in the revised Data Protection Directive that controllers remain accountable and responsible for the protection of data for which they are controllers, even if the data have been transferred to other controllers.

Recommendation 14
Define the core accountability principles for the situation when a multinational transfers personal data to third parties, taking into account the guidelines identified in this dissertation.

14 Evaluation of BCR as a form of TPR

14.1 Rules for rule-making

In Paragraph 13.1 on the principle of accountability, I mentioned that the regulatory initiatives to achieve accountability of organisations are often called "meta-regulation", i.e. the regulation of internal self-regulation.[1] In Paragraph 13.2, I discussed one aspect of meta-regulation, i.e. how regulators can provide companies with incentives and tools to use their own inherent 'regulatory capacities'. Another aspect of meta-regulation relates to the **optimal form** of meta-regulation to choose.[2] As Julia Black has put it, "[t]he 'how' of regulation, or more particularly 'how to do it better', is a burgeoning policy area and deserves separate consideration in its own right".[3] The discipline of how to best regulate (the rules for rule-making, the search for meta-norms) has in the EU become known under the label "Better Regulation" (**BR**).[4] I note that the two aspects of meta-regulation cannot be clearly divided in separate categories as these aspects to a certain extent overlap (i.e. some of the tools provided to companies to regulate have also to comply with the normative requirements for proper-self regulation).

The "official" starting point for the rules of BR is the 2003 Inter-Institutional Agreement on Better Lawmaking, entered into between the European Parliament, the EU Council of Ministers and the European Commission. This Inter-Institutional Agreement (together with other EU documents issued as part of the BR agenda) (i) sets out the basic requirements for EU law making, for instance as to requirements of consultation and transparency and (ii) promotes co- and self-regulation

---

1 Many other terms are used in this context. One is the term 'horizontal supervision' (whereby actions are adjusted by the supervisory authority and the supervised entity in cooperation), as opposed to vertical supervision, which is the traditional *command and control* model whereby any actions of the supervised entity are corrected top down by the supervisory authority. See Ottow (Chapter 13, n 18), in particular para. 2.1. On the expansion of regulation from government to governance, see Wessel and Wouters(Chapter 13, n 18), at 22 -47.

2 This paragraph draws on Bomhoff and Meuwese (Chapter 6, n 75).

3 J. Black, Legitimacy and the Competition for Regulatory Share, LSE Working Paper 14/2009 (2009) at 15 and Bomhoff and Meuwese (Chapter 6, n 75), at 169 also citing Black.

4 This term originated in the European Commission as a brand name for a strategy to improve EU lawmaking without making any explicit constitutional changes. See the 2003 Inter-Institutional Agreement on Better Lawmaking, Chapter 6, n 72). Recently, the Commission has made an effort to change the label into "Smart Regulation": European Commission, Communication on `Smart Regulation in the European Union' (COM/2010, 8 October 2010) 543.

when possible.[5] In accordance with requirements of BR, alternatives to legislation have to be considered. The Inter-Institutional Agreement marks the shift in European governance (with turning point in 2001) "ready to recognise, at times even promoting, non-state actors' activism (…), "generating new informal alliances between European institutions (the Commission in particular) and private actors, both at European and the national level".[6] The binding effects of the Inter-Institutional agreement on the EU institutions are undisputed.[7] Looking at the definitions of self-regulation and co-regulation in the Inter-Institutional Agreement, the dividing line between the two seems to be that co-regulation implies legal measures while self-regulation does not.[8] The two aspects of the Inter-

5 Inter-Institutional Agreement on Better Lawmaking (Chapter 6, n 72), in particular Article 16 and the White Paper on European Governance (Chapter 6, n 72), at 20, promoting especially co-regulation.

6 See Fabrizio Cafaggi (Chapter 8, n 61), Chapter 10, at 203. The movement to BR was accelerated by the recommendations made by the Mandelkern Report and the following Communication by the European Commission. See Cafaggi (Chapter 8, n 61), at 211 and the Mandelkern Group on Better Regulation: Final Report (13 November 2001), available at http://ec.europa.eu/governance/better_regulation/documents/mandelkern_report.pdf; and "Action Plan on Simplifying and Improving the Regulatory Environment," COM (2002) 278 final. See further Colin Scott, "Regulatory Governance and the Challenge of Constitutionalism," EUI Working Paper RSCAS 2010/07, at 7.

7 Cafaggi (Chapter 8, n 61), at 211, and literature therein referred to.

8 Suzanne Nikoltchev, A European Perspective of Self-Regulation in the Media, in: Reframing Self-Regulation in European Private Law, ed. Fabrizio Cafaggi, at 277. The definitions of self-regulation and co-regulations provided for in the 2003 Inter-Institutional Agreement are generally not followed in the literature. The Inter-Institutional Agreement takes a top-down approach of the concept of self-regulation, where the assumption seems to be that 'self-regulation' is an alternative to legislation and is something that can be put in place, see Article 22: "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements." Many authors do not consider self-regulation as an alternative to regulation, but rather define self-regulation in substantive terms and not by reference to any legally authoritative source. See for instance the definition provided by Zayènne D. Van Heesen-Laclé and Anne C.M. Meuwese, "The legal framework for self-regulation in the Netherlands", Utrecht Law Review, Volume 3, Issue 2 (December) 2007, to be found at http://ssrn.com/abstract=1083677 (citing: B. Morgan & K. Yeung, An Introduction to Law and Regulation: Text and Materials, 2007, at. 92 - 93): "We speak of self-regulation when an issue of public interest is addressed by standard-setting monitoring and/or enforcement carried out by private bodies vis-à-vis their members or affiliates who voluntarily subject themselves to this regulation. Self-regulatory arrangements may derive their authority from formal legal structures such as contract law, but they may also

Institutional Agreement referred to above may be of relevance to BCR. The first (the basic requirements as to EU law making) may apply also to the norm-setting for BCR. The Inter-Institutional Agreement grandfathers the current European practice where private actors today directly participate together with public officials in European policy-making in a formalised way, "the question has thus become: which combination of private and public actors is desirable in European policy design and implementation?".[9] And as there is a growing number of autonomous legal orders: both public, private and hybrid forms, the issue is not "which system will prevail, but rather how these systems can be coordinated so that they can "co-exist and co-evolve".[10] In this new setting there is a call for "one set of rules, common to public and private-law-making, including principles of delegation (degree and limits of delegatibility of law-making power) and more general coordination between public and private law-making".[11] This is especially relevant for BCR as BCR norm-setting is presently not undertaken by European legislators, but *de facto* by the Working Party 29.[12] The second element (promotion of co-regulation and self-regulation), is relevant as the Inter-Institute Agreement also provides that it does not consider co- and

---

be primarily grounded in social consensus within a community." A similar definition is given by Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 119 – 120. See further, Linda Senden, Soft Law, Self-Regulation and Co-Regulation in European Law: Where do they meet, Electronic Journal of Comparative Law, vol. 9.1 (January 2005) at para. 3.1, to be found at www.ejcl.org; and Fabrizio Cafaggi, preface New Modes of Regulation in Europe: Critical Rethinking of the Recent European Paths, in: Reframing Self-Regulation in European Private Law, ed. Fabrizio Cafaggi, at xxiii. The same applies to the definition of co-regulation provided for in the Inter-Institutional Agreement. Article 18 defines co-regulation as: "[T]he mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)." In the literature a more informal definition of co-regulation is followed, qualifying co-regulation as any regulation that involves some form of engagement of government in stimulating, overseeing or adopting what would otherwise by private or self-regulatory regimes. See Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 122 who simply qualify as co-regulation any "kind of regulation that is characterised by the cooperation between government and the private sector". See extensively on co-regulation: Fabrizio Cafaggi, "Rethinking Private Regulation," in: Fabrizio Cafaggi (ed.), *Reframing Self-Regulation in European Private Law* (Kluwer Law International 2006), Chapter 1, at 27 -34.

9 Cafaggi (Chapter 8, n 61), at 202.

10 Cafaggi (Chapter 8, n 61), at 204.

11 Cafaggi (Chapter 8, n 61), at 205.

12 As provided for under Article 29 of the Data Protection Directive, among other things to promote a clear interpretation of the Data Protection Directive.

self-regulation to be appropriate instruments to regulate human rights.[13] Data protection qualifying as a human right, the question is whether this caveat applies to BCR.

As indicated in the introduction to this dissertation, for BCR to be acceptable at the national and global level, they will have to "build on the assumption of common reference points".[14] The body of research and literature as to BR is potentially one of the sources for such common reference points or meta-norms.

14.2 Criteria for evaluating public law

Before discussing potential meta-norms that can be distilled from BR, I note that a preliminary survey of prior research and literature concerning BR of TPR[15] (as opposed to public law making) shows many different opinions as to the legitimacy and effectiveness of TPR to regulate corporate behaviour in a globalised society. Some conclude that TPR is not the answer to close the gap in the regulatory capacity of national states. Yet others suggest that, in comparison to public regulation, the new forms of TPR generate better behaviour of their actors in transnational settings, generate a higher degree of adherence, are more efficient and effective, are of higher quality, the norm-creating process is more transparent and democratic and thus more legitimate and enforcement is less problematic.[16] Despite all these differences in opinion, there seems to be more or less consensus among all authors that **public** law making should be evaluated based on four key

---

13 The European Commission is also of that opinion. See White Paper on European Governance (Chapter 6, n 72), at 21; and the Inter-Institutional Agreement on Better Lawmaking (Chapter 6, n 72), para. 22.

14 Bomhoff and Meuwese (Chapter 6, n 75), at 165.

15 For an inventory of prior research the 'Survey of Research Programmes,' see Annex 2 to "The added value of private regulation in an international world? Towards a model of the legitimacy, effectiveness, enforcement and quality of private regulation," HiiL 2007 – 2008, p.1 – 21, to be found at <www.hiil.org>.

16 Yesim Yilmaz, "Private Regulation: a Real Alternative for Regulatory Reform," Cato policy Analysis No. 303 April 20, 1998, available at <www.cato.org>. For a more nuanced view, whereby public regulation and TPR are complementary rather than substitutes, see Cafaggi (Chapter 6, n 67) at 16: "The conventional view that associates legitimacy to the public sphere and effectiveness to the private sphere is deeply unsatisfactory. It is the nature of complementarily between the spheres and the relationship between legitimacy and effectiveness which varies at the transnational level."

criteria, which (adapted to the particulars of TPR) should be taken as a starting point for evaluating TPR also:[17]

- **Quality**. Quality of law tends to be measured in terms of traditional criteria applied to formal legislation. Qualitatively, sound norms are inter alia: certain, predictable, unambiguous, while at the same time flexible, effective and malleable. In most legal systems there is a formal quality control institutionalised through advisory bodies that also ensure alignment with existing regulatory regimes.
- **Legitimacy**. Legitimacy requirements concern the baseline demands placed on any form of decision-making. Are all those affected by a norm included in the process of its formulation? If so, how much weight is attached to their interests? If the process of norm creation has been fair and inclusive, also dispute settlement can systematically privilege certain interests over others, which undermines the legitimacy of the norms.
- **Effectiveness**. This concept refers to the degree to which norms succeed in regulating the conduct of a specific group of actors, whether by trust mechanisms, in realising enforcements or otherwise.
- **Enforcement.** Norms which cannot compel compliance or enforcement cannot be effective, legitimate nor of sufficient quality.

It is clear that these evaluation criteria for public legislation at the national level (i) cannot be simply transposed from the national to the international level; and (ii) cannot be simply applied one-to-one to TPR. These criteria first need to be "transposed" (or as some label it "privatised")[18] into criteria to apply to TPR. The initial results of the HiiL Program show that despite the many difficulties in transposing these requirements to the TPR context, "it does not seem impossible to turn public accountability of TPR into a

[17] See HiiL 2008, "The added value of private regulation in an international world? Towards a model of the legitimacy, effectiveness, enforcement and quality of private regulation," at. 5 – 7, to be found at <www.hiil.org>.

[18] See Bomhoff and Meuwese (Chapter 6, n 75), at 163. Or, as Cafaggi (Chapter 6, n 67) at 1, formulates it: "[TPR] still lacks a comprehensive and integrated set of common principles. The toolbox of regulatory instruments differs significantly form that developed in the domain of public international law." Scott (n 6), at 7, addresses the issue form the other end, by labelling the phenomenon whereby private law is evaluated against public law criteria: the "publicization of private law," which "involves the development of mechanisms and norms through which private actors are enrolled in the delivery of public functions."

reality".[19] Before discussing these "transposed" criteria, I will discuss some general guidelines or rules of thumbs as to how to "privatise" the evaluation criteria of public law making to TPR (Paragraph 14.4). To understand the issues in privatising the evaluation criteria, it is essential to realise that other than with public law, the norm-setting often takes place at various levels as a result of which more actors often play a role than in public law-making. The criteria for evaluation of public law may therefore have to be divided over the various levels of norm-setting and this according to the involvement of the relevant actor in the overall norm-setting process. For convenience sake I first summarise below the different levels of norm-setting for BCR and the actors involved (or not involved).

14.3 Different levels of norm-setting for BCR

The following **actors** are involved in the BCR norm-setting process:

European legislators. European legislators enacted the Data Protection Directive which sets the general framework for data protection in the EU. The Data Protection Directive facilitates that Member States approve of data transfers if the controller "adduces adequate safeguards with respect to the protection of personal data", which is the legal basis for approval of BCR.[20] The Data Protection Directive does not provide for the material criteria for such adequate safeguards (i.e. BCR), nor does any Commission decision. At present EU legislators are therefore not part of the norm-setting process for BCR, which is at present *de facto* undertaken by the Working Party 29. This may change if European legislators decide to include rules on BCR in the revised Directive (as per *Recommendation 1*). In that case also European legislators will qualify as one of the actors in the BCR norm-setting process.

Working Party 29. At present the general norm-setting process is undertaken by the Working Party 29 by issuing of opinions setting out the requirements of the BCR regime.

Lead DPA. The Lead DPAs are subsequently responsible for the approval procedure of individual BCR in the MRP. The DPAs therefore verify whether the BCR submitted by a multinational for approval meets the criteria set by the Working Party 29 in the WP Opinions.

---

[19] See conclusions of Curtin and Senden (Chapter 6, n 67), at 18 – 19 and literature there referred to.

[20] Article 26(2) Data Protection Directive.

Multinational applying BCR. At the time the first BCR applications to Lead DPAs were made, norm-setting was to a certain extent performed also by the multinational when it drafted its BCR in consultation with the Lead DPA. After the WP Opinions were issued, the norm-setting for BCR became more and more a top-down process by the Working Party 29 and the room to manoeuvre for the multinational became correspondingly smaller. At present the conclusion is that the multinational is no longer an actor in the BCR norm-setting process.

The following **stakeholders** can be indentified in the BCR norm-setting process:

Multinationals. The multinationals are the addressees of the Data Protection Directive and the WP Opinions.

Beneficiaries. The beneficiaries of the Data Protection Directive and BCR are also stakeholders. In the case of BCR for Employee Data, these concern (former) employees and job applicants of the multinational. In the case of BCR for Customer Data, these concern the individual customers of the multinational (i.e. consumers) and all contact persons of its corporate customers, suppliers and business partners.

Suppliers and business partners. As supply chain management is part of the BCR regime, the third parties to which the multinational outsources data processing operations or otherwise transfers data are also stakeholders of the BCR. They have an interest in how the data transfer regime in the BCR norm-setting is set as this will also have an effect on their business model.

This dissertation focuses on the present manner in which BCR norm-setting takes place. I will here concentrate on the norm-setting by the Working Party 29 and Lead DPAs rather than possible future norm-setting by European legislators. The public accountability of European legislators for their legislative acts in general is outside the scope of this dissertation.

14.4 General starting points for "privatisation" of criteria for evaluating public law

14.4.1 Enhanced accountability

In general many commentators[21] indicate that if norm-setting is done by "*de facto* regulators", the four factors set out above in respect of public law making should be applied in an enhanced manner (also labelled "extended" accountability or "aggregate" accountability). [22] The fact is that more and more non-governmental organisations are involved in the setting of norms in certain business sectors or areas of law. Some of the main features of such *de facto* regulators are: (i) they are governed by networks of state agencies acting not on behalf of the state but as independent actors; (ii) they lay down standards and general regulatory principles rather than strict rules; and (iii) they frequently contribute to the emergence of a system of decentralised enforcement or the regulation of self-regulation.[23] An example of a de facto regulator is the "Basel Committee", in which the central bank directors of a limited number of countries harmonise their policies in such a way as to result in *de facto* regulation of the capital market.[24]

---

[21] This paragraph draws on Wessel and Wouters (Chapter 13, n 18), para. 2.3 and Bärbel R. Dorbeck-Jung, "Challenges to the Legitimacy of International Regulation: The Case of Pharmaceuticals Standardisation," in: Andreas Follesdal, Ramses A. Wessel and Jan Wouters (eds.) *Multilevel regulation and the EU, The interplay between global, European and national normative processes* (Martinus Neijhof Publishers 2008), para. 2.2, which gives a good summary of the literature available on this topic.

[22] Curtin and Senden (Chapter 6, n 67), at 6, in particular footnote 35. Cafaggi (n 61), at 221. I note that the assumption that TPR is inherently less legitimate than public law may be valid for "legitimate" states. However, the reality is that many states are not legitimate and in those cases TPR (for instance CSR codes regulating human rights) will be more legitimate than state laws violating those rights. Here I focus on the situation when state legislation does meet the four evaluation criteria for public law.

[23] See Wessel and Wouters (Chapter 13, n 18) at 28, under citation of K. Jayasuriya, "Globalization, Law, and the Transformation of Sovereignty: the Emergence of Global Regulatory Governance," Indiana Journal of Global Legal Studies, Vol. 2 1999, p. 453. Büthe and Mattli (Chapter 7, n 62), at Chapter 2, use a a broader definition of de facto regulators and categorise 4 different types of de facto private regulators, of which the one described by Wessel and Wouters is one category only (though the first and the one with the longest history and most prominence). As the findings of Büthe and Mattli in respect of this category is of relevance for BCR, I will refrain form discussion the other types distinguished by Büthe and Mattli.

[24] See Wessel and Wouters (Chapter 13, n 18), at 28 and 55-56. Another example provided there of a de facto regulator is the International Organisation of Securities Commissions (IOSCO), which deals with the transnationalisation of securities markets and attempts to provide a regulatory framework for them.

In anticipation of the evaluation of the BCR norm-setting procedure, I note that it is clear that the Working Party 29 qualifies as such a *de facto* regulator. The Working Party 29 (i) has been set up as the institutional body for cooperation among the DPAs[25]; (ii) has advisory status only[26] and issues opinions to "contribute to the uniform application of the Data Protection Directive and advises on proposals for Community legislation having an impact of data protection rather than the issuing of strict rules[27] and (iii) contributes to the emergence of self-regulation as promoted by the Data Protection Directive. See on the norm-setting by the Working Party 29 in more detail Paragraph 14.7.2 below.

Most commentators agree that if the norm-setting for TPR is done by a *de facto* regulator, the approach to the evaluation criterion legitimacy cannot merely reproduce the model of the public regulation process. Legitimacy must then be provided through a "surrogate" legislative process that requires additional measures**,** such as stronger participation of the stakeholders in the regulation process, increased transparency of regulation, as well as increased accountability and control of regulators.[28] Further, in the literature the question is raised whether TPR that regulate human rights should raise the bar as to legitimacy, and whether this depends also on the type of right that is at stake.[29] The present findings of the HiiL Program indicate that further research is necessary in order to come to identify context / area / sector specific elements which may contribute to enhancing legitimacy.[30]

A bit of a side step, but nevertheless highly interesting in this context, is that the requirements of "stronger stakeholder participation" and "increased

---

25 Pursuant to Article 29 Data Protection Directive.

26 See Article 29(1) Data Protection Directive.

27 See article 30 Data Protection Directive and the Document "Tasks of the Working Party 29," as published at <www.ec.europa.eu>. See further WP Contribution on the Future of Privacy (Chapter 6, n 33), para. 7b about the functioning of the Working Party 29 and proposals of the Working Party 29 itself for improvement.

28 Wessel and Wouters (Chapter 13, n 18), at para. 2.2 and the literature cited therein; Cafaggi (n 8), at 38.

29 Curtin and Senden (Chapter 6, n 67), at 6. Cafaggi (Chapter 6, n 67), at 15: "The search for legitimacy for these various regulatory forms requires different answers depending on the origins and effects of the rule-making power. Regimes based on freedom of contract and association need different legitimacy responses from those based on the protection of fundamental rights or the environment."

30 As presently part of the HiiL Program, (n **13**). See especially Curtin and Senden (Chapter 6, n 67), at 6.

transparency" are indicated also from the perspective of political science theory. Research reported in 2011 involved extensive empirical research into the norm-setting process by a number of global private regulators, by asking "Who gets to write the rules in these private bodies? What is the process of rule-writing? Who are the winners and losers in this process, and why?"[31] The research shows that transnational norm-setting by de facto regulators is a highly political process, where stakes for multinationals are high and which results in winners and losers.[32] Particularly relevant is that the transnational rule-setting is rarely about reaching a compromise between the different regulatory models, but mostly involves making a choice for one model or approach over another.[33] Multinationals benefit from the transnational norms by increasing their export opportunities (previously foreclosed by cross-national differences in national rules).[34] Potential costs for multinationals are caused by having to redesign products and services to comply with transnational norms if these differentiate from their initial national norms.[35] Multinationals therefore have a strong incentive to seek to influence the process of transnational rule-making.[36] For those who succeed

31 Büthe and Mattli (Chapter 7, n 62), at 214.

32 Büthe and Mattli (Chapter 7, n 62), at 12.

33 As Büthe and Mattli (Chapter 7, n 62), at 11 put it: "standards do not embody some objective truth or undisputed scientific wisdom professed by experts (…) expertise is not a single correct set of beliefs about what works or what does not. A German accountant (…) who underwent eight years of studies, training, and examinations, is every bit an expert as an American Certified Public Accountant (CPA). Nevertheless, these experts are likely to vigorously disagree on how to best approach a wide range of financial reporting challenges, because any accounting tradition or school is deeply rooted in the business and legal cultures of a given country. As an official of the accounting Standards Board of Japan (ASBJ) puts it: "there is no right or wrong answer.… It's like religion – Christianity or Buddhism". Global standardization is rarely about reaching a compromise among different regulatory models and approaches (a fusion between Christianity and Buddhism would be impossible to engineer) but instead about battles for pre-eminence of one approach or solution over another.".

34 Büthe and Mattli (Chapter 7, n 62), at 6: "The shift from domestic regulation to global private rule-making substantial gains, particularly to multinational and internationally competitive firms, for which it opens up commercial opportunities previously foreclosed by cross-national differences in standards ans related measures."

35 Büthe and Mattli (Chapter 7, n 62), at 8: "At the same time the shift (…) also entails cost. To comply with international product standards, for example, firms may have to redesign their products, retool their production methods, or pay licensing fees to other firms whose proprietary technology may be needed to implement the international standard efficiently. These cost can be so massive, to the point where some feel forced to discontinue production of certain goods or even go out of business."

36 Büthe and Mattli (Chapter 7, n 62), at 12.

in pushing their domestic standards for adoption as international standards, switching cost will be minimal; for those who do not succeed, switching cost can be massive.[37] As a result, transnational rule making involves what game theorist call "a co-ordination game with distributional conflict"[38]: "standardization implies the harmonisation of different prior practices and therefore adjustment costs, at least for some. Consequently, it involves conflicts of interest over the distribution of those adjustment costs - even when the benefits of convergence on a single international standard clearly exceed the adjustment costs for each country or even each affected user."[39] The research shows that the following factors determine which actors are likely to succeed in shaping the global norms: (i) technical expertise; (ii) financial means; (iii) timely information; and (iv) effective mechanisms of interest representation.[40] It is clear that multinationals are far more likely than employees, consumers or civil society interest groups to have the required expertise and financial resources to participate in the transnational norm-setting. "As a consequence representatives from industry in most cases vastly outnumber other stakeholders in international standard-setting, even when formal procedures, such as public notice-and-comment periods, create a nominally even playing field."[41]

14.4.2 Empirical research

The only valid manner in which a full assessment may be made of BCR against the "privatised" or "transposed" criteria of evaluating public law is to perform empirical research. All of the evaluation criteria contain a perception element (i.e. are the norms in BCR **perceived** as predictable and legitimate, to lead to compliance in practice, to be enforced in practice, etc). At the time this dissertation was written, the empirical research was undertaken as part of the HiiL Program, where BCR are one of the forms of TPR which was evaluated against the transposed criteria.[42] The expectation was that based on these findings an informed assessment could be made as to (i) the extent to which the BCR norms, the creation process of BCR, the validation and implementation of BCR and the enforcement regime meet the "transposed" criteria of Quality, Legitimacy, Effectiveness and Enforcement and (ii) the relative merits of BCR as compared with the data protection

---

37 See citation in n 35.

38 Büthe and Mattli (Chapter 7, n 62), at 5 (in particular footnote 10) and at 42 (in particular footnote 1).

39 Büthe and Mattli (Chapter 7, n 62), at 42.

40 Büthe and Mattli (Chapter 7, n 62), at 44-45.

41 Büthe and Mattli (Chapter 7, n 62), at 47-48, reffering to earlier research by the authors.

42 The final report of the HiiL Program is expected in December 2012.

compliance of multinationals prior to implementation of their BCR. Proposals for improvement of the BCR regime will subsequently be made based on these assessments.

14.4.3 Normative criteria

This being said, there are some **normative elements** in the evaluation criteria of which it is known that these influence how norms are ultimately perceived and responded to in practice.[43] The pivotal factor for TPR in this respect is the question of legitimacy. The general assumption in the literature is that TPR provide a trade off between a higher effectiveness and lower legitimacy (in particular the sub-component accountability).[44] To remedy possible gaps in terms of legitimacy, TPRs could introduce legitimacy-enhancing mechanisms, such as judicial control over the rule-making process. The existence of judicial review is one of the normative elements that do play a role in how legitimacy of TPR is perceived. Systems that limit or exclude judicial review of TPR decrease the chances that the relevant TPR are perceived as legitimate.[45]

14.4.4 Relative lack of legitimacy

An initial finding of the HiiL Program[46] is that "today's global governance arena is not considered to be defined by unaccountable organisations, but rather by organisations that are either accountable to the wrong set of stakeholders or focus accountability on one set of stakeholders at the expense of others."[47] An example of the latter is if a certain business community such as the cigarette industry (under the threat of public regulation) sets up a self-regulatory agency that issues a self-regulatory

---

43 Linda Senden, *The OMC and its Patch in the European regulatory and constitutional landscape*, RSCAS 2010/61.

44 See Cafaggi (Chapter 11, n 31), at 10.

45 Aileen McHarg, "The Constitutional Dimension of Self-Regulation," in: Fabrizio Cafaggi (ed.), *Reframing Self-Regulation in European Private Law* (Kluwer Law International 2006), at 93; Cafaggi (n 8), at xix.

46 See Curtin and Senden's conclusions (Chapter 6, n 67), at 18 – 20 on which the following paragraphs draws.

47 Curtin and Senden (Chapter 6, n 67), at 19 and Wessel and Wouters (n 18), at 55-56. See also Communication from the Commission, "Towards a reinforced culture of consultation and dialogue - General principles and minimum standards for consultation of interested parties," 11 December 2002, COM(2002) 704 final, at 5: "The Commission has underlined, in particular, *its intention to "reduce the risk of the policy-makers just listening to one side of the argument or of particular groups getting privileged access[…].*" (citation from the White paper on European Governance (Chapter 6, n 72), at 17).

advertising code. The self-regulatory agency holds a consultation on the code and invites the government and all companies belonging to such business community (as addressees of the self-regulatory code), to submit comments, but overlooks to also consult other stakeholders of the code, such as consumer organisations, the anti-smoking association, child advocacy groups, etc.

Below I first discuss whether, and if so which form of, TPR is suitable to regulate human rights (Paragraph 14.5). I then elaborate on the concept of legitimacy from a normative perspective (Paragraph 14.6) and evaluate the current BCR norm-setting regime against these normative criteria (Paragraph 14.7).

14.5 TPR regulating human rights

14.5.1 Introduction

Many consider TPR not to be suitable for regulating human rights. For instance the European Commission in its White Paper on European Governance provided that co-regulation is "only suited to cases where fundamental rights (...) are not called into question".[48] Also the 2003 Inter-Institutional Agreement on Better Lawmaking which promotes co- and self-regulation when possible,[49] provides that "these mechanisms are not available if fundamental rights or important political options are at stake."[50] In the literature it is remarked that as to data protection "this exception is questionable as the Data Protection Directive itself explicitly asserts that codes of conduct must be promoted and it is quite clear that self-regulatory mechanisms including technological solutions will ensure the needed data protection more efficiently than certain legislative texts".[51] Other authors just assume that the self-regulation promoted by the Data Protection Directive fits in with the 2003 Inter-Institute Agreement on Better Lawmaking and promote the co-regulatory approach for inter alia BCR as the right approach in accordance with the Agreement on Better Lawmaking. They give no consideration to the fact that data protection qualifies as a human right for which according to the Agreement on Better Lawmaking

48 See the White Paper on European Governance (Chapter 6, n 72), at 21.

49 Inter-Institutional Agreement on Better Lawmaking (Chapter 6, n 72), in particular Article 16.

50 White Paper on European Governance (Chapter 6, n 72) at 21. See Inter-Institutional Agreement on Better Lawmaking, Chapter 6, n 72), Article 17. The Dutch government is also of this opinion, see Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 117, referring to Kamerstukken II, 1997 – 1998, 25 880, at 180 – 181.

51 Poullet (Chapter 8, n 61), at 253.

self- and co-regulation should not be available.[52] I fully agree with the conclusion (or the position) that as to data protection, self- and co-regulation as promoted and facilitated by the Data Protection Directive[53] should be possible. This is however not because the Data Protection Directive itself provides so, in the sense that the Data Protection Directive would thereby overrule the exception formulated in the 2003 Inter-Institutional Agreement on Better Lawmaking. The reason is more fundamental, in the sense that the form of self-regulation promoted by the Data Protection Directive is adequately embedded within public legislation as a result of which there are no valid arguments why this form of "framework" legislation should not be appropriate. To the contrary, (as amplified hereafter) this form of framework regulation is considered in literature to be the appropriate form of TPR to choose if human rights are involved.

14.5.2 Rationale

The White Paper on Corporate Governance and the 2003 Inter-Institutional Agreement on Better Lawmaking do not clarify why they consider the caveat for human rights to be necessary. The first question is whether this caveat is still valid. The Inter-Institutional Agreement dates from 2003, at which time the rules of BR were starting to be developed. In January 2009, the European Commission updated its "Impact Assessment Guidelines,"[54] that provide instructions for Commission staff when preparing Commission policy proposals. Part of the impact assessment that has to be performed is that the policy options have to be identified (non-EU policy action, regulation, directive, recommendation, communication, self-regulation, or co-regulation, or any combination of the foregoing).[55] Though the Impact Assessment Guidelines in the paragraphs where it discusses the various policy options contain many references to the 2003 Inter-Institutional

---

52 See, for instance, the Rand Report (Chapter 6, n 27), at 8 and 48. See further: Nikoltchev (n 8), Chapter 11, at 279, where the requirements for co-regulation are listed, including the negative requirement that co-regulation is not suitable if "it involves human rights." Further down, at 276 and at 282-283, various forms of self- and co-regulation of data protection in the online environment are discussed without also discussing whether data protection being a human right is suitable for self- and co-regulation at all.

53 See Article 27 Data Protection Directive and para. 7.1.6.

54 European Commission Impact Assessment Guidelines of 15 January 2005, SEC(2009) 92, replacing the Commission Guidelines adopted in June 2005 and updated in March 2006, to be found at http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf.

55 Impact Assessment Guidelines (n 54), at para 7 and Annex 7.

Agreement,[56] the caveat is nowhere repeated. Instead of respecting all policy options (including if these include self-regulation and co-regulation), staff is expected to make an assessment of the social impact of the policy options (which includes making an assessment of the impact on human rights).[57] I take this as an indication that by now the thinking about BCR of the EU institutions (or in any event the Commission) has been evaluated and that it is questionable whether the caveat (in its absolute form) is still valid.

The second question is whether the caveat (if still valid) is justified. One may infer that at the time the 2003 Inter-Institutional Agreement was entered into, the caveat reflected an implicit belief "that fundamental rights should be only abridged through legislative acts of democratically elected bodies which are politically accountable and subject to constitutional review".[58] The underlying assumption here seems to be that the fundamental rights expressed in the Constitution, being the expression of the state, only confer rights against the state (i.e. against public authority). In this view human rights do not have a horizontal effect, i.e. do not confer obligations on private parties.[59] The consequence would be that if private parties issue self-regulation these could tread on human rights without these human rights being enforceable against such private parties. In such cases the state has to

---

56 Impact Assessment Guidelines (n 54), at Annex 7 at para. 7.1 at 24. The Annex extensively discusses the different policy options and guidelines when which option is to be considered. These guidelines do not contain any reference to the caveat.

57 Impact Assessment Guidelines (n 54), at paras. 8 at 31 and Annex 8.1.

58 See Fabrizio Cafaggi, (n 8) at xviii, who assumes that this is the underlying rational for the caveat. The view that fundamental rights should be only abridged through legislative acts of democratically elected bodies which are politically accountable and subject to constitutional review, is part of a broader constitutional discourse, which represents the idea that "public power is or should be limited and subject to some higher form of control by reference to law." See Scott (n 6), at 1. The "constitutionalists" critique has been voiced against any form of delegation of governmental power to regulatory agencies, as "[s]uch delegations may be quite extensive and arguably undermine the effectiveness of the limitations placed on legislative and executive power" (Scott (n 6), at 1). Scott, at 15, rejects this idea as "orthodox constitutionalism, while it might once have been the most appropriate way to think about legitimating a governance centred on the nation state, is not capable of legitimating the diffuse governance patterns associated with contemporary regulation. An alternative narrative offered here seeks to match the variety of governance forms with varied forms of institutionalization which link processes and values of hierarchy, competition and community to appropriate governance forms."

59 On the horizontal effect of human rights, see (Chapter 10, n 71), Chapter 5 at para. 2.2; and Cafaggi (Chapter 6, n 67), at 28.

intervene.[60] Hence, the requirement that any abridging of human rights should be through a legislative act, where a proper balancing of rights can be ensured.

The question is whether this is still a valid assumption. This view of human rights finds its basis in the origin of human rights, which were traditionally[61] crafted to protect individuals from abuse of power by the state, which at the time were the biggest aggregations of power in society.[62] Companies are in that tradition treated on the notion that they are private, not public, entities, i.e. are more like individuals than states. Accordingly, they are traditionally treated as **rights holders** of human rights, rather than duty holders.[63] The

---

60 Ziller (Chapter 10, n 71), at 154.

61 Human rights arose out of the Enlightenment, see Amy Sinden, 'Addressing Corporate Environmental Wrongs', in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 504 and 506.

62 Sinden (n 61), at 505.

63 The US Supreme Court has held that corporations are 'persons' entitled to assert certain constitutional rights. For an overview of evolution of the doctrine of legal personhood and constitutional rights of corporations in the US see, e.g. Pollman, Elizabeth, Reconceiving Corporate Personhood (December 31, 2010), available at SSRN: http://ssrn.com/abstract=1732910. At 16, Pollman explains that the origins of the doctrine of legal personhood of corporations are found in *Santa Clara Co. v. Southern Pacific Railroad*, 118 U.S. 394 (1886). See, however, a recent decision of the US Supreme Court in *Federal Communications Commission v. AT&T Inc.*, 562 U.S.(2011), that corporations do not enjoy the "personal privacy" exemption under the Freedom of Information Act. It is noteworthy that in the context of the US legal system one cannot make general statements on whether or not corporations do or do not enjoy a certain right regardless of a particular context. For instance, the right to privacy stems from the system of privacy law that does not have a single, hierarchical order of rules. Instead it consists of common law torts, constitutional, and statutory law, with various subjects of regulation and applicability. The complexity is further increased given that the US is a federation where regulatory competence is divided between the federation and the states. See Paul M. Schwartz, Reidenberg, Joel R., *Data Privacy Law: A Study of United States Data Protection* (Charlottesville, Virginia: MICHIE Law Publishers, 1996), at 102, as cited in Purtova (Chapter 12, n 33), at 90. As a result, the decision not to grant a statutory privacy right to a corporate entity in *Federal Communications Commission v. AT&T Inc*, is made for the purposes of application of the Freedom of Information Act and has no bearing for the scope of any constitutional privacy rights. The Court affirms that the Constitution's Fourth Amendment does protect a corporation against search and seizure, a recognised privacy interest (at 8). Simultaneously, the Restatement (Second) of Torts §6521, Comment c (1976) reads that a corporation has no privacy claim under the law of torts (cited in *Federal Communications Commission v. AT&T Inc.* at 8).

fact is, however, that many multinationals now wield as much or even more power than many states, and the conditions of individuals' lives are shaped as much by multinationals as by states, especially in the area of workers rights (e.g. equal pay, working hours, etc).[64] Hence there now seems to be a broad consensus in the literature that multinationals as to certain human rights[65] should be (in addition to states) also **duty holders**.[66] In this view

---

In the EU, corporations possess (to a certain extend) rights to free speech and privacy. Article 1 of the First Protocol to the ECHR makes clear that both natural and legal persons have the right to the peaceful enjoyment of their possessions. Under the ECHR, corporations have been held to possess rights to free speech under Article 10 (for case law, see Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights*, (Sweet&Maxwell, 2007), at 344). Corporations further have a right to privacy under Article 8. In *Niemietz v. Germany,* 72/1991/324/396, Council of Europe: European Court of Human Rights, 16 December 1992, the European Court of Human Rights (**ECHR**) has ruled that the words "private life" and "home" as mentioned in Article 8 ECHR, extend to professional or business activities or premises. See e.g. *Niemietz v. Germany*, at 31: "More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8." The ECJ, notably in competition cases, followed the ECHR case-law and also recognised that to business activities (to a certain extent) fall within the protection of the "home" as provided for by Article 8. See e.g. Case C-94/00 *Roquette Frères SA v. Directeur général de la concurrence, de la consommation et de la répression des frauds* (Commission of the European Communities, third party): 2002 E.C.R. I-9039: "For the purposes of determining the scope of that principle in relation to the protection of business premises, regard must be had to the case-law of the European Court of Human Rights (...). According to that case-law, (...) first, the protection of the home provided for in Article 8 of the ECHR may in certain circumstances be extended to cover such premises (see, in particular, the judgment of 16 April 2002 in *Colas Est and Others v. France*, not yet published in the Reports of Judgments and Decisions, § 41) (...) and, second, the right of interference established by Article 8(2) of the ECHR 'might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case' (*Niemietz v. Germany*, cited above, § 31)." See also Case C-238/99 *Limburgse Vinyl Maatschappij (LVM) v Commission and Others,*, para. 245 et seq., etc.) and Sinden (n 61), at 514.

64 See John Ruggie, Protect, Respect and Remedy: a Framework for Business and Human Rights, 7 April 2008, A/HRC/8/5, to be found at <www.ohchr.org> (the "Ruggie Report"), Addendum 2, which reports the results of research on the actual impact of multinationals on the various fundamental rights.

65 Some human rights have clearly no relevance for multinationals. For instance, a multinational will not act as prosecutor and the criminal procedure rights of individuals are therefore of no relevance vis-à-vis multinationals. Other rights will require some creative adaption to apply in the context of multinationals. See for examples para. 15.2.1 below and in particular n 17 below.

66 See McBarnet (Chapter 8, n 23, at 56; McBarnet and Schmidt (Chapter 11, n 12), at 148 – 176; Andrew Clapham, *Human Rights Obligations of Non-State Actors* (Oxford University Press

human rights do have "horizontal effect". The assumption that human rights have no horizontal effect is not only challenged in the literature, it is also challenged in positive law. Many national and international courts have applied human rights in private disputes.[67] In some countries the fundamental rights in the Constitution also equally apply to private and public relationships.[68] This being said, the caveat in the 2003 Inter-

---

2006), at Chapter 6; and Damian Chalmers, "The Government and Citizenship of Self-Regulation," in: *Reframing Self-Regulation in European Private Law* (Kluwer Law International 2006), Chapter 6, at 187 – 188. Willem van Genugten, "Handhaving van Wereldrecht, een kritische inspectie van valkuilen en dilemma's," [2010] Nederlands Juristenblad-1 at 12, who more generally observes that the international legal order is transforming from being directed at the protection of state interests into the interests of the people (which he labels the 'humanitisation' of the international legal order). He notes that this is visible in the effect of human rights on the key concepts of international law. In more detail, see Willem van Genugten, Kees Homan, Nico Schrijver and Paul de Waart, *The United Nations of the Future; Globalization with a Human Face* (Amsterdam: KIT Publishers 2006). See also Cafaggi (Chapter 6, n 67), at 28: "The limited direct applicability of soft law to private parties derives from the more general principle of public international law which, conventionally, imposes primary responsibility on States. This view has been criticized and increasingly international law obligations are also applied directly to private parties."

67 Like in the US and France, see Ziller (Chapter 10, n 71), at 155. See for other examples: Cafaggi (Chapter 6, n 67), at 28 especially fn 156, which includes Case 36/74, *Walrave v. Association Union Cycliste Internationale*, 1974 E.C.R. 1405, where the ECJ held that anti-discriminatory provisions of the Treaty of Rome also apply to private entities (employment discrimination).

68 Like the Irish Constitution of 1937, see Ziller (Chapter 10, n 71), at 155. The issues discussed here are relating to national constitutional law. There is also the question of whether human rights in the framework of the ECHR have horizontal effect. Here the fundamental rights are part of a treaty between sovereign states, and this justifies the question whether, and if so, to which extent, these are intended to confer obligations upon private parties against other private parties. In literature such *direct* horizontal effect of the ECHR provisions is generally rejected. See Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights,* D.J. Harris et al. eds. (Oxford University Press, 2 ed.: 2009) at 20 in particular footnote 177. However, in literature there is also general agreement that "the human rights laid down in the Convention do (...) exercise (...) influence on the relationships between private parties." See Arthur S. Hartkamp, "Fundamental Rights, Fundamental Freedoms, and Contract Law" in *Constitutional values and European contract law,* Stefan Grundmann ed. (Wolters Kluwer, 2008) at 98; and Purtova (Chapter 12, n 33), at 224 as to horizontal effect of Article 8 ECHR. Hartkamp (this n) at 98, refers to the ECHR as *indirect* horizontal effect of human rights. Other authors are hesitant to use horizontal effect terminology with regard to the "obligations of the kind that exist under the Convention," see *Harris, O'Boyle & Warbrick* fn 175 at 20. Leaving terminological disagreements aside, established case law under the ECHR recognises that, if an article of the ECHR is found to impose positive state obligations, "these obligations may involve

Institutional Agreement may remain relevant in case in a certain country human rights are not considered to have horizontal effect.[69]

The question is whether the above does necessarily mean that the EU institutions are right in their caveat that self- and co-regulation are not fit to regulate human rights. While the concerns of the Commission and EU institutions are understandable, a wholesale rejection of the possibility of using self- and co-regulation is considered contrary to current traditions and further without theoretical foundation.[70] There are many instances where fundamental rights are traditionally regulated by self-regulation.[71] Notable examples are the field of freedom of the press and the church, where self-regulation is often Constitutionally preferred to forms of public regulation and, to some extent, public regulation is even prohibited.[72] Based on the broad history of self-regulation in the area of human rights, one author concludes:

> "it is, perhaps unsurprisingly, much easier to find constitutional supports for self-regulation than constitutional prohibitions. (…) thus as the attempts to find constitutional limits to privatisation has demonstrated, it is extremely difficult to identify a set of 'core' public functions which are irreducibly the state's responsibility. (…) This is not to say that some things are not more effectively done through public rather than private means. But the conclusion is

---

the adoption of measures designed to secure respect for private life *even in the sphere of the relations of individuals between themselves*." See e.g. ECHR 26 March 1985, *X. and Y. v. The Netherlands*, Application no. 8978/80 para. 23. This doctrine was upheld in further case law. See e.g. ECHR 17 July 2008, *I v. Finland*, Application no. 20511/03, and more recently, *Von Hannover v Germany* [2004] ECHR 294 (Application no. 59320/00).

69 Cafaggi (n 8) at xviii and Ziller (Chapter 10, n 71), at 153. The current trend in the EU is that horizontal effect of fundamental rights is rapidly emerging in doctrine. See B.J. De Vos, Horizontale werking van grondrechten. Een kritiek, for a discussion of the doctrine under the main jurisdictions in Western Europe and case law thereon and (as the title promises) clear criticism as to the diffuseness of the concept and the (lack of sufficient) foundation of the concept itself. For the English summary see at 293 et seq.

70 See Cafaggi (n 8) at xviii.

71 McHarg (n 45), at 82 even observes that "all constitutional systems are self-regulating to some degree: all rely to some extent on self-enforcing conventions and all face problems of balancing accountability and independence."

72 Cafaggi (n 8) at xviii; Cafaggi (Chapter 8, n 61), at 213; and McHarg (n 45), at 80. McHarg lists examples and arguments why in certain cases self-regulation is not only permitted but actually required, in the sense that state regulation is prohibited in certain areas. Examples mentioned are self-regulation of the press and the church, which both should operate separately and independently from government.

> inescapable that the lines drawn between public and private action are the result of political choices, conditioned by history, circumstance and tradition"[73]

Based on the foregoing it is difficult to maintain a blanket condemnation of the use of self- or co-regulation as a policy instrument for regulating human rights.[74] The key issue is more how concerns regarding human rights should influence the regulatory design for self-regulation and co-regulation, for instance by ensuring that the relevant rights and especially the outcome of any balancing of those rights against any other fundamental rights, are safeguarded by public framework legislation.[75] Indeed, this form of general framework legislation for TPR is in the literature considered to be the appropriate form to apply if fundamental rights are at stake.[76] As another author summarises it:[77]

> "In the context of the discussion regarding fundamental rights, the key issue with co-regulation arises from the spectre of *conflicting* fundamental rights

---

73 McHarg (n 45), at 81, referring to T. Daintith and M. Sah, "Privatisation and the Economic neutrality of the Constitution," [1993] PL 465 and D. Feldman and F. Campbell, "Constitutional Limitations on Privatisation," in: J.W. Bridge (ed.), Comparative Law facing the 21st century (UKNCCL, London, 2001).

74 McHarg, (n 45), at 93.

75 McHarg (n 45), at 93, Cafaggi (Chapter 8, n 61), at xix. Scott (n 6), comes to a similar conclusion when discussing private law making from the perspective of "constitutionalism." See Scott at 1: "Constitutionalism is a term which seeks to capture the idea that public power is or should be limited and subject to some higher form of control by reference to law." The 'constitutionalists' critique has been voiced against delegation of governmental power to regulatory agencies, as "[s]uch delegations may be quite extensive and arguably undermine the effectiveness of the limitations placed on legislative and executive power." Scott at 1 -2, notes that "[o]ne response to the diffusion of regulatory power is to seek the application of traditional modes of control and accountability, seeking their extension beyond state actors to those who were found to wield power." Scott, at 2 (and at 15), however suggests adopting a more comprehensive solution and to "recognise diffusion not only in actors but also in modes of regulatory governance (…) by seeking to institutionalise broader modes of control and accountability which are best to match the governance powers which are targeted."

76 See Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 143 and Cafaggi (Chapter 8, n 61), at 204: "Common rules, often of constitutional relevance, should ensure that the private-law-making power is not exercised at the expense of other private groups."

77 Cafaggi (n 8), at xviii. See also Cafaggi (Chapter 8, n 61), at 214 – 215: "Freedom of speech may also conflict with rights to privacy and data protection. Balancing different constitutional principles granting law-making-power to different private actors may translate into limitations and constraints for the exercise of PLM [Private Law Making]. These constraints can be considered organising principles of normative pluralism."

> within the regulatory process, and the legitimacy of co-regulatory bodies and striking an appropriate balance between these rights. (…) For example, in the context of media regulation or press regulation there is a well-recognised conflict between the freedom of speech and the right to privacy. A biased selection favouring journalists or media firms over private organisations which represent the right to privacy may translate into an unacceptable balancing of those conflicting rights which may be constitutionally illegitimate. An initial response to this objection is to point out that the legislative act which defines the co-regulatory model is capable of identifying principles that ensure the right balance between competing rights and binds the private bodies to adhere to those enumerated principles".

Using framework legislation (and consultation of all relevant stakeholders) is not the sole device which can be used to encourage protection of fundamental rights in self- or co-regulation. Other elements can be used to enhance protection of fundamental rights, like judicial review.[78]

14.5.3 TPR of data protection

How does all the above apply to data protection? Different from most other human rights, data protection rights have from the outset been also directed at companies. Although the Data Protection Directive applied from the outset also to data processing by the governments of the Member States, important areas of data processing by governments were initially excluded from the scope of the Directive (like processing for public safety, defence, state security, and for criminal law purposes). [79] These exceptions to the scope of the Data Protection Directive have recently been 'remedied' by TFEU, that made Article 16 TFEU regulating data protection of general application (i.e. also applicable to all areas of data processing by governments). The Data Protection Directive (when implemented into national legislation) does therefore already impose direct data protection duties on multinational (and thus have per definition horizontal effect). To the extent that the Data Protection Directive promotes self-regulation[80], this

---

[78] See n 45 and Cafaggi (n 8), at 38, listing as mitigation measures for interest representation: "(a) by applying to private regulators' activities the participatory rules generally deployed by public regulators; (b) by designing a governance structure able to represent sufficiently diversified interests; and/or finally (c) by guaranteeing a system of liability able to protect those interests whose voice finds no representation within the organisation or which do not translate into participatory rights."

[79] See Article 16 TFEU. See for details Chapter 7, n 3.

[80] Article 27 Data Protection Directive reads as follows:

is always under the umbrella of the Data Protection Directive. This form of self-regulation is also labelled "stipulated self-regulation", which is self-regulation accomplished within an existing general legal framework.[81] The general legal framework provides for minimum standards and conditions and is established by means of legislation and the framework promotes that further (technical) detailing is left to the relevant sector through a code of conduct.[82] Under the Data Protection Directive, the organisation that drafted an EU self-regulatory code can request the Working Party to declare that the rules contained in its code properly implement the provisions of the Data Protection Directive.[83] These "conformity declarations" by the Working Party 29 are not binding. National courts having to decide on data protection violations will (have to) decide whether a certain data processing is legitimate based on applicable data protection law rather than based on the relevant self-regulatory code.[84] Conformity declarations can also be

---

"1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party."

81 Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 121.

82 Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 121 and 142; Poullet (Chapter 8, n 61), at 254.

83 See Article 27(3) Data Protection Directive.

84 Although Article 27(3) of the Directive prescribes that "Draft Community codes (...) may be submitted to the Working Party [and] this Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive," the opinions that the Working Party may adopt on these matters do not go beyond the competences given to the Working Party pursuant to Article 30 of the Directive, and as such do not have binding effect. The publication by the European Commission

requested at a national level from the DPAs. Whether such decisions by the DPAs are binding or non-binding will depend on applicable national law. If the decision of the DPA is non-binding, the courts of the DPA will have to decide based on their national data protection law rather than based on the rules of the relevant self-regulatory code. If the decision of the DPA is binding, data protection violations will have to be decided based on the relevant code. However, also in such case the conformity decision by the DPA will then be subject to review by the courts.[85]

Based on the foregoing the conclusion is that self-regulation of data protection is regulated by the national laws of the Member States (i.e. is regulated by government legislation) and only when a self-regulatory code has obtained a conformity declaration by a DPA which is binding, data protection is regulated by the relevant self-regulatory code. However in that case, the decision of the DPA to issue the conformity declaration is subject to judicial review. By this procedure, it is ensured that self-regulation of data

---

of the relevant opinion does not change this (see for publication by the Commission the last sentence of Art. 27(3): "The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party."). Kuner (Chapter 6, n 8) at 48 points out that also the practice of the Working Party when approving codes of conduct shows that the Working Party itself is of the opinion that its approvals are not meant to have a binding effect: "The 'uncertain legal status' of the codes approved by the Working Party is evident in the fact that while the Working Party has competence to determine whether 'drafts submitted (...) are in accordance with the national provisions adopted pursuant to this Directive,' (...) the Working Party has so far refused to approve or endorse any instrument that does not contain extensive disclaimers making it clear that application of the instrument is without prejudice to the provisions of national data protection law. This means that, notwithstanding approval of the Community code by the Working Party, its use is still subject to all the details of data protection law in the different Member States where it is used." The consequence of the non-binding nature of Working Party opinions is that they are not subject to review by the ECJ. The ECJ only reviews acts of the EU institutions and agencies "which are intended to have legal effects," see case 22/70 *Commission v Council* [1971] ECR 263 at para. 42.

85 As required by Article 28(3) Data Protection Directive. For instance, Article 25 (4) of the Dutch Data Protection Act provides that conformity declarations are "equivalent to a decision ('*besluit*') within the meaning of the Dutch General Administrative Regulations Act (*Algemene wet bestuursrecht*)" and are therewith subject to administrative and judicial review. Article 25(4) further provides that the consultation procedure under the General Adminstrative Regulations Act applies to such decisions. This entails that the DPA has to make the request for a conformity declaration and the draft self-regulatory code available for consultation to the public for a period of 4 weeks, during which time interested parties may submit their comments. The possibility for consultation must be publicly announced. See the publication of the Dutch DPA Gedragscodes, bescherming van persoonsgegevens door zelf-regulering, qt 15, available at <www.cbp.web.nl>.

protection remains within the framework requirements of the Data Protection Directive which is the appropriate form considered in literature to apply if fundamental rights are at stake.[86]

14.5.4 BCR

The next question is whether the Data Protection Directive also provides a "sufficient general legal framework" for BCR. This question is justified as BCR are a different form of self-regulation than the self-regulatory codes promoted by the Data Protection Directive. BCR are not submitted by multinationals for review to the Lead DPAs as to whether they comply with the **level of protection provided for by the Data Protection Directive**, but are submitted for review to the DPAs whether they provide for an **adequate** level of protection as required for the transfer of data to non-adequate countries pursuant to Article 26(2) Data Protection Directive. An adequate level is not necessarily the same level of protection as provided for by the Data Protection Directive, which is generally assumed to be of a higher level. In Paragraph 10.6, I noted that the Data Protection Directive does not (yet) explicitly recognise that BCR are an appropriate tool to provide adequate safeguards for the transfer of data and in any event does not define the main substantive requirements for the required adequate level to be provided by BCR. The Working Party 29 in the WP Opinions has recognised BCR as a valid tool for data transfers and defined these criteria, but these WP Opinions are not binding (i.e. do not qualify as government regulation). As a consequence at present no proper formal legal framework exists for DPAs to review and authorise individual BCR, or for the national courts (and ultimately the ECJ) to be able to review BCR authorisation decisions of the DPAs.[87] To ensure that BCR also have a formal legal basis as required for TPR regulating human rights, I therefore recommend that the revised Data Protection Directive also provide a proper legal framework to recognise BCR as an appropriate tool to provide adequate safeguards for the transfer of data and to define the main substantive requirements for BCRs to be set an adequate level.

This is in line with the recommendation of the Working Party 29 itself, which recommendation the European Commission intends to follow.[88] This

---

86 See Koops, Lips, Nouwt, Prins and Schellekens (Chapter 6, n 67), at 143. For the sake of completeness, I note that some Member States "within implementation have delegated rule-making power to private bodies." See Cafaggi (Chapter 8, n 61), at 209. I will not further discuss the legitimacy of this form of delegation by Member States here.

87 As required by Article 28(3) Data Protection Directive.

88 See Chapter 10, n 47.

is further in line with *Recommendation 2* (made in Paragraph 10.7), and will therefore not lead to a separate recommendation here.

As a note of interest, I add that in Paragraph 6.1, I indicated that the introduction of corporate privacy policies by multinational companies has created a bottom-up pressure on national legal orders, which we saw reflected in the pressure on the DPAs to recognise these corporate privacy policies as a data transfer instrument. In respect of the regulation of self-regulation, in the literature a distinction is made between 'a bottom-up approach' and a top-down approach. Though at the start the discussions about acceptance of BCR with the various individual DPAs were very much bottom up, the approach subsequently taken by the WP Opinions as to BCR (which to all probability will also be adopted in the revised Directive) is, however, very much the top-down approach. This is in conformity with the European approach to co-regulation which is fundamentally top-down.[89]

14.6 The concept of legitimacy- The normative perspective

14.6.1 General introduction

In regulation theory "legitimacy"[90] constitutes "the acceptance that a person or organisation has a right to govern given by those it seeks to govern and those on whose behalf it purports to govern".[91] For a regulatory norm to be

---

89 Yves Poullet, "Selected comments on themes developed in this volume," in: Bert-Jaap Koops et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (TCM Asser Press 2006), at 254. Senden (n 8), at para. 3.1.

90 This Paragraph draws on the papers presented at the HiiL Annual Conference on Transnational Private Regulation, June 2010, Dublin, to be found at <www.privateregulation.eu>.

91 For a discussion of the concept of legitimacy for example, see Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 1999), Chapter 6 and Julia Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes," in: [2008] 2 Regulation & Governance, at 137-164. For a discussion of legitimacy from an organisations theory perspective, see Marc Suchman, Managing Legitimacy: Strategic and Institutional Approaches, Academy of Management Review 1995, Vol. 20, No. 3, at 571- 610. Suchman notes at 573, that "Within contempary organisations theory, legitimacy is more often invoked than described, and is more often described than defined". Though Suchman adopts a very broad definition (legitimacy is a generalised perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions), his insights are of (surprising) relevance for legitimacy from a legal perspective as well. In the footnotes I make some references to Suchman if a parallel with organisations theory may be made.

legitimate, it must be accepted by those to whom it is addressed.[92] Rule-makers may claim legitimacy and may even engage in various strategies to enhance legitimacy. The extent to which they succeed, however, depends on the extent to which the rules are accepted by others. In that sense legitimacy is *de facto* more an objective empirical phenomenon rather than a normative abstraction.[93] There is no single answer to the question which regulatory norms ultimately become legitimate ("crystallise") and which do not. Factors which are known to play a role in the crystallisation process are:

- **Distribution of the norm.** This concerns the extent to which the norms are known, accepted and applied; training and education for those involved in applying the norm and information campaigns and notices may play a role;
- **Enforcement**. This concerns the rewards (and punishments) associated with (not) following the norm, the mechanisms and extent of enforcement.
- **Transmission.** This concerns the extent to which the norm is transferred onto others which in its turn reinforces the legitimacy of the norm for the original actor (e.g. adoption of the norm may raise consumer expectations, which in its turn may legitimise the norm).[94]

14.6.2 Normative criteria

In this legitimisation or crystallisation process certain normative criteria, however, do play a role in the way in which actors initially react to new regulatory norms (i.e. is this new rule a norm which is perceived as potentially "legitimate").[95] Such perceived legitimacy will create a sense of obligation to act in accordance with such norms and even foster active support for such norms, which will ultimately lead to legitimacy.[96] In that sense the concept of legitimacy is not insulated from normative concerns of those actors to whom the norms are addressed, both as to how the norms are created and the substantive content.[97] The main normative sub-component

92 Black (n 91), at 144.

93 Donal K. Casey and Colin David Scott, "The Crystallization of Regulatory Norms," (February 22, 2011), Journal of Law and Society, Vol. 38, Issue 1, at 76-95. Available at SSRN: http://ssrn.com/abstract=1772396 or doi:10.1111/j.1467-6478.2011.00535.x, at 87.

94 Casey and Scott (n 93), at 78 and 82.

95 Casey and Scott (n 93), at 88.

96 Casey and Scott (n 93), at 88.and 89.

97 Casey and Scott (n 93), at 89.

of legitimacy is "accountability".[98] Accountability here is a different concept than the "accountability principle" discussed in Chapter 8. In Chapter 8 "accountability" concerned the compliance measures that multinationals can take to achieve desired regulatory outcomes and to make these compliance measures verifiable to the regulators. These compliance measures often include the adoption by an organisation of corporate self-regulatory codes. In this chapter "accountability" concerns the question whether the norm-setting process as to, for instance, such corporate self-regulatory code meets the requirements of proper self-regulation (i.e. meets the requirements of BCR). As I indicated in the beginning, the concepts may to a certain extent overlap, for instance if a meta-regulator prescribes that companies have to introduce corporate self-regulation and further provides for procedural requirements how this self-regulation has to be established.

As a sub-component of legitimacy, two conceptions of accountability can be distinguished:

- **Accountability as a virtue**, as a positive quality of organisations or officials (Paragraph 9.6.3).
- **Accountability as a social mechanism**, as an institutional arrangement in which an actor can be held to account by a forum (Paragraph 9.6.4).

14.6.3 Accountability as a virtue

The concept of accountability as a virtue is essentially seen as a normative concept, as a set of standards for the evaluation of the behaviour of actors. Accountability, or "being accountable", is thus seen as a virtue, as a positive quality of organisations.[99] Studies into accountability as a virtue therefore

[98] Alongside with authorisation and representation, see Curtin and Senden (Chapter 6, n 67), at 2, and references therein. Accountability is however the main sub-component, and will be concentrated upon here.

[99] Curtin and Senden (Chapter 6, n 67), at 2. See Suchman (n 91), at 579 for a discussion of the concept of "moral legitimacy" from an organisations theory which shows remarkable similarities with the concept of accountability as a virtue discussed in this paragraph. According to Sachman, moral legitimacy "reflects a positive normative evaluation of the organization and its activities." He discusses that moral legitimacy takes one of three forms: evaluations of outputs and consequences (consequential legitimacy), evaluation of techniques and procedures (procedural legitimacy) and evaluations of categories and structures (structural legitimacy). Suchman himself notes at 579 in footnote 2 that "consequential legitimacy and procedural legitimacy both reflect legal-rational authority".

often focus on the actual behaviour of organisations.[100] As there is no general consensus about standards that constitute accountable behaviour, the concept is contested.[101] However, some normative components have been identified which make an organisation more accountable to its stakeholders. The Global Accountability Framework (GAF)[102] provides useful criteria for accountability as a virtue and identifies four core dimensions that make an organisation more accountable to its stakeholders: (i) transparency; (ii) participation; (iii) evaluation; and (iv) complaints and response mechanisms.

(i) **Participation**. This describes the process through which an organisation enables key stakeholders to play an active role in the decision-making processes and activities which affect them.[103]

(ii) **Transparency**. This concerns the provision of accessible and timely information to stakeholders and the opening up of organisational procedures, structures and processes for their assessment.[104]

(iii) **Evaluation.** This encompasses the processes through which an organisation, with involvement from key stakeholders, monitors and reviews its progress and results against goals and objectives; feeds

---

[100] Curtin and Senden (Chapter 6, n 67), at 2.

[101] Curtin and Senden (Chapter 6, n 67), at 2.

[102] As developed by One World Trust, a charity that conducts research on practical ways to make global organisations more responsive to the people they affect, and how the rule of law can be applied equally to all, see Monica Blagescu, Lucy de Las Casas and Robert Lloyd, Pathways to Accountability: The GAP Framework (One World Trust 2005), to be found at <www.oneworldtrust.org>.

[103] Blasgescu, De Las Casas and Lloyd (n 102), at 32 -34. Suchman (n 91), discusses different types of legitimacy from an organisations policy perspective and indicates that granting participatory rights to constituents may enhance legitimacy. See at 578, where he discusses the type "influence legitimacy" which "arises when the organization incorporates constituents into its policy-making structures or adopts constituents' standards of performance as its own. In a world of ambiguous causality, the surest indicator of ongoing commitment to constituent well-being is the organization's willingness to relinquish some measure of authority to the affected audience (to be co-opted so to speak)." See further Suchman at 587-9 discussing strategies for gaining legitimacy) "To achieve pragmatic legitimacy through conformity, an organization must either meet the substantive needs of various audiences or offer decision-making access, or both." See finally Suchman at 580, where he discusses "procedural legitimacy" (as one of the three forms of moral legitimacy, see n 99) and indicates that moral legitimacy can be enhanced "by embracing socially accepted techniques and procedures".

[104] Blasgescu, De Las Casas and Lloyd (n 102), at 30 -32.

learning from this back into the organisation on an ongoing basis; and reports on the results of the process".[105]

(iv) **Complaints and response mechanisms.** These concern the mechanisms through which an organisation enables stakeholders to address complaints against its decisions and actions, and through which it ensures that these complaints are properly reviewed and acted upon.[106]

There are three phases of the regulatory process (a) norm-setting, (b) evaluation and monitoring and (c) enforcement.[107] The requirements (i) transparency and (ii) participation concern phase (a) the norm-setting phase and are relevant to ensure **accountability ex-ante** during the process of rule-making.[108] Requirement (iii) evaluation concerns phase (b) monitoring and evaluation. Requirement (iv) complaints and response procedure concerns phase (c) enforcement. These requirements are relevant when the process of rule-making is completed and seek to ensure **accountability ex-post**.

The four normative criteria are not absolute; different legitimacy demands may be made by the different addressees of the regulatory norms. In the BCR context different stakeholders are addressees of the data protection rules: the data protection rules are addressed to the multinationals and the third-party beneficiaries of these rules are the data subjects. In the case of BCR, different legitimacy demands may be made by the multinationals to which the rules are addressed and the beneficiaries of BCR, in this case the employees and customers of the multinational. Such different legitimacy demands may lead to a "legitimacy dilemma" for a regulatory regime. [109] A solution suggested in the literature[110] is to enhance legitimacy in such case by resorting to public oversight, either by issuing framework legislation[111] or

---

[105] Blasgescu, De Las Casas and Lloyd (n 102), at 34 – 36.

[106] Blasgescu, De Las Casas and Lloyd (n 102), at 37.

[107] See Cafaggi (Chapter 8, n 61), at 215.

[108] Curtin and Senden (Chapter 6, 67), at 12.

[109] Cafaggi (Chapter 8, n 61), at 212.

[110] Cafaggi (Chapter 8, n 61), at 222 -223, lists in total 4 possible responses to conflict of interest situations. Two are mentioned in the text. The other two are: (i) competition (increasing the number of private law makers and the degree of competition between them whereby full transparency as to the rules will force private law makers to disclose the features of the rule-making-processe to the potential addressees); and (ii) regulatory networks (by adhesion to protocols or principles set by independent organisations).

[111] Cafaggi (Chapter 8, n 61), at 223, suggests that delegation is also possible provided that legitimacy requirements are imposed on the entity to which norm-setting is delegated at the

by judicial oversight by making the regimes subject to judicial review. Another (overlapping) solution is to separate the norm-setting, monitoring and enforcement function into different organisations with independent governance bodies. TPR often lacks the so-called "separation of powers", where the norm-setting, the implementation and enforcement are all in one hand. One measure is then to outsource compliance monitoring and dispute resolution to independent private bodies (or to the judiciary).[112] If it is simply not possible to have complete legitimacy from all aspects (i.e. the regime may not be perceived as legitimate by all stakeholders)[113], legitimacy may be enhanced by introducing greater participation and transparency as to the choices made.[114]

A separate normative legitimacy requirement identified in the literature in respect of regulators is the requirement of the independence of regulators.

(v) **Independence.** Independence of regulators is safeguarded through a prohibition on having any financial or other interest that could affect impartiality[115], and can further be fostered by job rotation.[116] This requirement will be dealt with as part of transparency.

14.6.4 Accountability as a mechanism

The concept of accountability as a mechanism concerns the question: can a regulator be held publicly[117] accountable ex post (i.e. who is accountable, to whom and for what exactly and what institutional relation or arrangement(s) have been put into place for this?).[118] These questions entail

---

same time. Cafaggi lists as legitimacy requirements: openness, transparency, representativeness, participation and independence from vested interests.

112 Cafaggi (Chapter 8, n 61), at 224.

113 Julia Black (2008), "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", LSE Law, Society and Economy Working Papers 2/2008 London School of Economics and Political Science Law Department, available at www.lse.ac.uk/collections/law/wps/wps.htmm, at 30.

114 Casey and Scott (n 93), at 14. Cafaggi (Chapter 8, n 61), at 221: "The solution of conflicts of interests increases accountability of PLM [Private Law Making]."

115 Dorbeck-Jung (n 21), at 57.

116 Dorbeck-Jung (n 21), at 57.

117 Public accountability means that the account giving process takes place in the public domain and not behind closed doors. Curtin and Senden (Chapter 6, n 67), at 7.

118 Curtin and Senden (Chapter 6, n 67), at 14. According to Curtin and Senden (n 67), at 3, there two different conceptions of accountability: accountability as a virtue, as a positive quality of

an analysis of accountability ex ante, during the process of rule-making, and also ex post, as to whether there are mechanisms or arrangements by which accountability forums can hold the actors accountable after the fact.
Accountability therefore refers to the mechanisms of oversight and control that render the exercise of the regulatory powers acceptable to those regulated and to those who will be affected positively or negatively by the conduct of the regulated parties, i.e. the beneficiaries. For a social relation to be subject to accountability, some authors require seven constituting elements: "(i) a relationship between an actor and a forum (ii) in which the actor has an obligation (iii) to explain and to justify (iv) his or her conduct (v) the forum can pose questions (vi) and pass judgement and (vii) the actor may face consequences".[119] The actors responsible for the outcome of the norm-setting can be an organisation or an individual, including a public institution, companies involved in norm setting, standardisation bodies, professional bodies, etc.[120] The accountability forum can be an institution or an individual, including public authorities, the executives of a company, international organisations, audit offices, financiers, or the stakeholders (represented by interest groups, or otherwise).[121] A key feature of TPR is that in the norm-setting process of TPR both the actors and the accountability forums involved are "plural, partial and emergent".[122] As a consequence two major complications can be identified (i) the problem of the many hands (where it is difficult to identify the actors responsible for the outcome of regulation) and (ii) the problem of the many eyes (the risk that actors are accountable to a plethora of different accountability forums).[123] While the problem of the many hands might suggest that all the stakeholder communities should be made part of the rule-making process (to increase accountability of the actor), this would only exacerbate the problem of the many eyes. The conclusion of the HiiL Program is therefore that "bringing the public back in should (…) be a balanced exercise". To avoid situations of "accountability paralysis" a prioritisation has to take place both in respect of (i) the forums that are most significantly affected by the TPR regime and (ii) the most pressing issues on which the actor should be held accountable.

---

organisations or officials; and (ii) accountability as a social mechanism, as an institutional arrangement in which an actor can be held to account by a forum. See for a justification of the choice to apply the concept of accountability as a mechanism, Curtin and Senden (n 67), at 18.

119 This is the definition introduced by M. Bovens, D. Curtin and P. Hart (eds), *The Real World of EU Accountability: What Deficit?* Oxford University Press (2010), at 37. This definition is also used by Curtin and Senden (Chapter 6, n 67), at 14.

120 Curtin and Senden (Chapter 6, n 67), at 14.

121 Curtin and Senden (Chapter 6, n 67), at 14.

122 Curtin and Senden (Chapter 6, n 67), at 14.

123 Curtin and Senden (Chapter 6, n 67), at 15.

The constituting elements of accountability as a mechanism all concern ensuring **accountability ex-post.** [124] These constituting elements can be taken together and regrouped into three requirements:

(i) **Information requirement.** The actor is obliged to inform the forum about his or her conduct, by providing various types of data about the performance of tasks, outcomes, or procedures, which may also involve providing explanations and justifications. This requirement boils down to the following questions:

- Is there a formal obligation to explain and justify conduct and what is the nature – political, legal/judicial, administrative, professional, financial, otherwise - of this obligation (e.g. by public officials to supervisory agencies, courts or audits)?
- Is there an informal – social, moral, professional, public – obligation to do so (e.g. press conferences, briefings, voluntary audits, public panels)?

(ii) **Debate.** There needs to be a possibility for the forum to interrogate the actor and to question the adequacy of the information or the legitimacy of the conduct.[125] This requirement leads to the following question.

- What are the possibilities for debate; can the forum interrogate the actor and question the adequacy of the information or the legitimacy of the conduct?

(iii) **Pass judgement.** The accountability forum may pass judgement which may take the form of approval of the annual accounts, denounce a policy, publicly condemn behaviour, pass a negative judgement, or as a result thereof the actor may face certain consequences like sanctions.[126] This requirement boils down to the following questions:

- What arrangements and policies have been put into place to enable the accountability forum to pass judgment:

---

[124] For these three criteria, see Curtin and Senden (Chapter 6, n 67), at 17. The break down of these three criteria into detailed questions derives from the questionnaire used in the HiiL Program for the empirical research.

[125] Curtin and Senden (Chapter 6, n 67), at 17.

[126] Curtin and Senden (Chapter 6, n 67), at 17.

- What evaluation process, both of regulatory outcomes and practices/policies, is provided for; what formal and informal complaint-and-response mechanisms have been put into place and how independent and credible are these?
- What consequences and/or sanctions may the actor(s) face for its conduct (e.g. (dis)approval of annual accounts, denouncement of a policy, public condemnation of behaviour)?
- What non-judicial means of dispute resolution are there and what formal judicial redress may be obtained?

Requirements (i) and (ii) apply both to phase (b) monitoring and enforcement. Requirement (iii) is only relevant for phase (c) enforcement.

14.6.5 Cumulative overview accountability requirements

Taking together the evaluation criteria of accountability as a virtue and accountability as a mechanism, I come to the following overview.

Requirements to ensure accountability ex-ante

Phase (a) norm-setting

(i) Participation
(ii) Transparency
(iii) Independence

Requirements to ensure accountability ex-post

Phase (b) monitoring and evaluation

(iv) Evaluation
(v) Information requirement
(vi) Debate

Phase (c) enforcement

(vii) Complaints and response procedures
(viii) Information requirement
(ix) Debate
(x) Pass judgement

14.7 Are BCR legitimate? – The normative perspective

14.7.1 Identifying the actors and accountability forums involved in the three phases

Phase (a) BCR norm-setting process
The accountability forums vary per actor involved in the BCR norm-setting process. To identify the main accountability relationships[127], it has to be decided:

(i) Who are the most prominent actors that bear responsibility for the norm-setting?
(ii) What are the accountability forums; who are most significantly affected by the regime, both internally and externally?
(iii) What are the most pressing issues on which the actors should be held accountable?

Below are listed the two main actors involved in the BCR norm-setting process and (listed in sequence of priority) their corresponding accountability forums.

Working Party 29. For the Working Party 29 the following accountability forums may (in any event) be identified:
- the multinationals as addressees of the BCR regime
- suppliers and business partners of the multinational to which the multinational transfers data
- potential beneficiaries of the BCR (i.e. employees, consumers, patients)
- the courts of the Member States, and ultimately the ECJ
- European legislators.

Lead DPAs. For the Lead DPAs the same accountability forums can be identified with the difference that now the specific employees and customers of the relevant multinational applying for BCR authorisation will be the accountability forum.

Phase (b) monitoring and evaluation
The main actor involved in the monitoring and evaluation of BCR is the multinational and its accountability forums are:

[127] Because of the many hands and many eyes involved in the determination of the accountability relationship, prioritization is required in this regard in order to avoid accountability paralysis. These questions are also derived from the questionnaire drafted as part of the HiiL Program, for purposes of performing the empirical research into the various forms of TPR.

- internal accountability forums: the board, the internal complaints committee
- external stakeholders (employees, consumers, patients)

Phase (c) enforcement
The main actor involved is the multinational and its accountability forums are:

- internal complaints committee
- Lead DPA
- national courts
- ECJ

Below I will focus on the accountability of the actors in respect of their **specific part** in the BCR norm-setting process. This is not to say that the Working Party 29 and the Lead DPAs are, for instance, not also **accountable ex-post** for their part in the BCR norm-setting. For instance, the Working Party 29 will be accountable ex-post to the European Commission (being its advisory body). The Lead DPA will be accountable ex-post for the proper performance of its tasks to the public at large in its Member State. This general accountability ex-post of the Working Party 29 and the Lead DPAs are outside the scope of this publication. I will review, however, to what extent decisions and opinions of the Working Party 29 and the Lead DPA are subject to **judicial review** (in which review requirements (vi), (vii) and (viii) play a role). This constitutes the accountability ex-post of the Working Party and the Lead DPAs to the courts of the Member States and the ECJ. As indicated in Paragraph 14.4.3, judicial review of norm-setting by de facto regulators may be a factor of relevance in deciding on the legitimacy of such norms.

14.7.2 Phase (a) BCR norm-setting by Working Party 29

Introduction. The Working Party 29 is a *de facto* regulator. Pursuant to Article 29 Data Protection Directive, the Working Party 29 has been set up as the institutional body for cooperation among the DPAs. The Working Party 29 has advisory status and acts independently.[128] Members are representatives of each of the DPAs, of the EDPS and of the European Commission. The tasks of the Working Party 29 are clearly formulated and are publicly available. It issues opinions to "contribute to the uniform application of the Data Protection Directive and advises on proposals for EU

[128] Article 29(2) Data Protection Directive.

legislation having an impact of data protection.[129] The opinions of the Working Party 29 are non-binding but they are followed in practice by the DPAs and *de facto* set the rules for application of the Data Protection Directive.

The Working Party 29 has issued Rules of Procedure of the Working Party[130], pursuant to which the Working Party 29 is authorised to invite experts to attend meetings of the Working Party 29[131] and further to install sub-groups to prepare the position of the Working Party 29 on specific topics.[132] Members of the Working Party 29 may be further authorised to be assisted by experts "in their confidence".[133] The Rules of Procedure of the Working Party do not include a requirement for the Working Party to hold a public consultation or public hearing before issuing its opinions.

Norm-setting as to BCR. The Working Party 29 installed a sub-group on BCR[134], which sub-group prepared the WP Opinions. The Working Party 29 held a consultation[135] and a public hearing[136] on the first of the WP Opinions, the input of which was taken into consideration into its subsequent WP Opinions. As part of the consultation a number of multinationals and industry groups were invited to submit their input, but no employee representatives or consumer interest groups.[137] At the public hearing about

---

129 See the Document "Tasks of the Working Party 29", as published at <www.ec.europa.eu>. See further WP Contribution on the Future of Privacy (n 33), para. 7b about the functioning of the Working Party 29 and proposals of the Working Party 29 itself for improvement.

130 The Rules of Procedure of the Working Party, Brussels, 15 February 2010, to be found at <www.ec.europa.eu> (**WP Rules of Procedure**).

131 See Article 9 of the WP Rules of Procedure.

132 Which the Working Party 29 is authorised to do pursuant to Article 16 of the WP Rules of Procedure (n 130).

133 Which the Working Party 29 may authorise pursuant to article 9 WP Rules of Procedure (n 130).

134 This is based on oral information of DPAs. No public information is available on the existence of this sub-group (or other sub-groups for that matter), their mandates, their members or meetings. According to the Dutch DPA, presently 15 DPAs are members of the BCR sub-group.

135 A summary of the contributions can be found at: <http://ec.europa.eu/justice/policies/privacy/workinggroup/consultations/binding-rules_en.htm>.

136 See the Official Summary of the Public Hearing on internal codes of conduct for multinationals drafted by the Dutch Data Protection Authority, to be found at http://ec.europa.eu/geninfo/query/resultaction.jsp?page=1.

137 For their contributions, see: <http://ec.europa.eu/justice/policies/privacy/workinggroup/consultations/binding-rules_en.htm>.

30 representatives of the business community were present (which included both multinationals as addressees of the BCR regime and potential suppliers and business partners of those multinationals) and one consumer organisation.[138] It is not known which members of the Working Party 29 participated in the BCR sub-group and whether any experts participated either in this sub-group or in the plenary meetings of the Working Party 29 or whether any of the members were assisted by an expert. The Working Party 29 draws up an annual report which is transmitted to the European Commission, the European Parliament and the Council and which is made public.[139]

Being a de facto regulator, any norm-setting by the Working Party 29 requires a strict (or even an enhanced) application of the legitimacy requirements.

14.7.3 Accountability ex-ante Working Party 29

Re (i) Participation

It does not require much discussion that the BCR regime as developed by the Working Party 29 in the WP Opinions has **not** been inclusive in the sense that the third-party beneficiaries (i.e. employee or consumer organisations[140] and civil society stakeholders) have been sufficiently included in the norm-setting process.[141] As business organisations (both as addressees of the BCR regime and as contracting parties) were amply represented in the norm-setting process, even the risk exists that the Working Party 29, while deciding on the WP Opinions, was subject to "regulatory capture": if not all

---

138 See n 136.

139 Article 15 WP Rules of Procedure (n 130).

140 Participation of consumers will be effective only if their representatives can rely on the relevant expertise and financial sources, see Dorbeck-Jung (n 21), at 56.

141 This is with the exception that apparently (next to 30 representatives of the business community) one consumer organisation was represented at the Public Hearing held by the Working Party 29 on the first of seven WP Opinions. See the Official Summary of the Public Hearing on internal codes of conduct for multinationals drafted by the Dutch Data Protection Authority, at 1, to be found at <www.ec.europa.eu>. The Working Party 29 may seek the views of data subjects or their representatives pursuant to Article 27(3) Data Protection Directive. Apparently the Working Party 29 (by now) also realises that a broader consultation is indicated, where it announced in a WP Opinion on the principle of accountability (Chapter 1, n 15), at para. 15, that it may develop a model data compliance program for medium and large controllers in the future (which will be similar to the compliance program of BCR) and then will consult 'all appropriate stakeholders.'

stakeholders are involved or heard, impartiality of the regulator is at risk.[142] This potential lack of legitimacy should be remedied in the future.[143] The opportune moment to remedy this shortcoming is the consultation launched by the European Commission as part of the review of the Data Protection Directive (see Paragraph 10.6 above). If *Recommendation 2* is followed and EU legislators delegate the further norm-setting in respect of BCR to the European Commission pursuant to Article 290 TFEU, a further consultation of the BCR stakeholders has to take place prior to such further norm-setting by the Commission.[144] In Paragraph 5.6.6, I discussed that as the European Commission in its turn will not be able to specify all BCR requirements in full detail, the Working Party 29 will continue to play an important role in providing guidelines in respect of these requirements (for instance, the application of the BCR norms to certain industry sectors, such as the health industry or the telecom sector). I further indicated that both the Working Party 29 and the EDPS recommended that the European Commission insist "on a strong commitment by the members of the Working Party 29 to implement the views of the Working Party 29 into national practice"[145] and "make the opinions [of the Working Party 29] more authorative" by including an obligation for the DPAs and the Commission "to take utmost account of opinions".[146] Based on these recommendations the expectation is

---

142 See para. 14.4.4 in particular n 47.

143 See also Recommendation 5 of the Rand Report (Chapter 6, n 27) at 42:
"**Recommendation 5: Achieve broader liaison with stakeholders**
The Article 29 Working Party should liaise more systematically with business representatives, third sector and NGO communities, and the perspectives of NGO representatives and citizen organisations should be more explicitly taken into account."

144 See also the Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe, Brussels, 4 November 2002 (Chapter 8, n 30), at para. 2: "Many respondents commented that where primary regulation through a Directive would still be necessary, the Directive should be restricted to setting principles and general rules, leaving the detailed rules to secondary regulation. Where recourse is made to secondary regulation, democratic legitimacy must be ensured."

145 WP Contribution on The Future of Privacy (Chapter 6, n 33), para. 99. See also Wugmeister, Retzer and Rich (Chapter 7, n 61), at 492.

146 EDPS opinion on the revision of the Directive (Chapter 6, n 35), at 146: "The EDPS recommends solutions which would make opinions of the Working Party more authoritative without modifying substantially its way of functioning." The EDPS suggests including an obligation for the DPAs and the Commission to take utmost account of opinions and common positions adopted by the Working Party, based on the model adopted for the positions of the Body of European Regulators for Electronic Communications (BEREC). Furthermore, the new legal instrument could give the Working Party the explicit task to adopt "interpretative recommendations". These alternative solutions would give the positions of the Working Party a

justified that although no formal delegation of regulatory powers will take place to the Working Party 29, the opinions of the Working Party 29 will (remain to) be more than just guidelines and will be policy rules *de facto* setting norms for DPAs and controllers. Legitimacy demands require that also in respect of such *de facto* norm-setting, proper stakeholder consultation will take place. The suggestion by the EDPS, that as long as the opinions of the Working Party 29 are not given binding force, and "safeguards such as transparency and redress" do not come into play[147], fails to recognise that legitimacy must also be ensured for de facto norm-setting.

Recommendation 15

- Hold a proper consultation of all stakeholders of BCR prior to enacting the norms for BCR in the revised Data Protection Directive (or the EU regulation);
- Instruct the European Commission to hold a consultation of all stakeholders of BCR prior to the further norm-setting on BCR by the European Commission;
- Instruct the Working Party 29 to hold a consultation of relevant stakeholders prior to the Working Party 29 issuing opinions on BCR.

Re (ii) Transparency

It also does not require much discussion that the norm-setting procedure by the Working Party 29 is not sufficiently transparent. Transparency is provided effectively only if information is "accessible, intelligible, all-embracing and objective".[148] The Rules of Procedure of the Working Party 29 are publicly available,[149] but the minutes of the meetings of the Working

stronger role, also before the Courts. For the position of the BEREC, see Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L337, 9 18.12.200, p. 1.

147 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at 151: "The EDPS would put a caveat against introducing stronger measures, such as giving binding force to WP29 positions. This would undermine the independent status of individual DPAs, which has to be guaranteed by the Member States under national law. If the Working Party decisions were to have a direct impact on third parties such as data controllers, new procedures should be foreseen including safeguards such as transparency and redress, including possibly appeal before the European Court of Justice."

148 Dorbeck-Jung (n 21), at 56.

149 To be found at <www.ec.europa.eu>.

Party 29 and any draft documents produced by the Working Party 29 are restricted, unless the Working Party 29 decides otherwise.[150] Further, though the Working Party 29 held a consultation on BCR of which the contributions are published[151] and a public hearing of which a (very) short summary of the discussions is published,[152] no information is available on:

- why the consultation was limited to certain companies and one consumer organisation only;
- whether any experts were invited by the Working Party 29 to attend the relevant meetings of the Working Party 29;
- whether any sub-group was established to prepare the position of the Working Party 29 on the WP Opinions and if so, which members of the Working Party 29 participated in such sub-group, and what the mandate of such sub-group was;
- whether any members of the Working Party 29 were assisted by experts of their confidence;
- if experts were involved, how they were selected, their competences, experiences and dependencies, how any conflicts of interest were identified and dealt with, what their expert advice was and the choices subsequently made based on this advice.[153]

---

[150] See Article 11(1) WP Rules of Procedure (n 130).

[151] For which a number of multinationals and industry groups were invited to submit their input. See for their contributions <www.ec.europa.eu>.

[152] See the Official Summary of the Public Hearing on internal codes of conduct for multinationals drafted by the Dutch Data Protection Authority, to be found at <www.ec.europa.eu>. The Public Hearing was attended by 30 representatives of the business community and one consumer organisation.

[153] In response to a commitment made in the EC White Paper on European Governance (Chapter 6, n 72), at 19, the European Commission issued guidelines on collection and use of expert advice in the Commission to provide for the accountability, plurality and integrity of the expertise used and expressed the intention that "[o]ver time these guidelines could form the basis for a common approach for all Institutions and Member States."
The guidelines were issued in 2002, see Communication from the Commission on the collection and use of expertise by the Commission: Principles and Guidelines, 11 December 2002, COM(2002) 713 final (**EC Communication on the use of experts**). The Guidelines at 9-10 provide for three core principles when seeking expert advice, the second of which is **"Openness.** The Commission should be open in seeking and acting on advice from experts. Transparency is a key precondition for more accountability for all involved. Transparency is required, particularly in relation to the way issues are framed, experts are selected, and results handled (…) Instead, the Commission must be capable of justifying and explaining the way expertise has been involved, and the choices it has made based on advice. In a similar way, accountability also extends to the experts themselves. They should, for example, be prepared to

This lack of transparency should be remedied in the future. This is also the recommendation of the First Report on the Directive[154] and the EDPS[155] and the intention of the European Commission.[156]

Recommendation 16
Instruct the Working Party 29 to amend its Rules of Procedure to remedy the lack of transparency as to its decision-making process.

Re (iii) Independency
The next question is whether the Working Party 29 is sufficiently independent.The independence of the Working Party 29 is in principle ensured in the Data Protection Directive.[157] The EDPS in its Opinion on revision of the Directive[158] rightfully notes that "the strength of the [Working Party 29] is intrinsically linked with the independence and powers of its members". The members of the Working Party 29 are representatives of the DPAs, the EDPS and the European Commission. The independence of the DPAs and the EDPS is in principle ensured in the Data Protection Directive.[159] The ECJ (Case C-518/07 *Commission v. Germany)*[160] ruled that the requirement of "independence" of DPAs entails that the DPAs:

---

justify their advice by explaining the evidence and reasoning upon which it is based." The first principle further includes the requirement of "independency" which should aim at promoting practices "to minimise the risk of vested interests distorting the advice proffered (…) by making dependencies explicit".

154 First Report on the Data Protection Directive (Chapter 6, n 26), at 23.

155 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at 144: "Finally, reinforcing the powers for DPAs also requires stronger powers for the Working Party, with a structure including better rules and safeguards and more transparency. This will be developed for the advisory role as well as for the enforcement role of the Working Party."

156 The lack of transparency of the Working Party 29 is implicitly acknowledged by the European Commission in its Communication on the revision of the Directive (Chapter 6, n 34), at para. 2, where it announces that the Working Party 29's role should be strengthened in coordinating the DPAs positions and should become a "more transparent body."

157 This is also a requirement under Article 29(1) Data Protection Directive.

158 EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 142.

159 The independence of the DPAs is ensured by Recital 62 and Article 28(1) Data Protection Directive and Article 8(3) TFEU. For the independence of the European Data Protection Supervisor, see Article 41(1) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing

> "enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect".

It is clear that in some Member States, the DPAs still lack sufficient independence, which should be remedied (see further Paragraph 14.7.5).

However, the Working Party 29 itself does not meet the test of independence as set by the ECJ. The EDPS again rightfully notes that the Working Party 29 does not enjoy the required freedom of (indirect) external influence, as the European Commission is "at the same time member, secretariat and addressee of the Working Party's opinions", and concludes that the:

> "autonomy of the Working Party should be ensured in the new legal framework, in accordance with the criteria developed for a complete independence of DPAs by the European Court of Justice in case C-518/07. The EDPS considers that the Working Party should also be provided with sufficient resources and budget and a reinforced secretariat, to support its contributions."

Further, if experts are participating in the meetings of the Working Party 29, it is not clear whether they are representing any interest and as such their independence is not guaranteed.[161] This should be remedied by a public

---

of personal data by the Community institutions and bodies and on the free movement of such data, [2000] OJ L8/1.

[160] Case C-518/07, *Commission v. Germany*, [2010] OJ C 113, at 3-4. See at para. 30: "the second subparagraph of Article 28(1) of Directive 95/46 is to be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data."

[161] Independence is safeguarded through a prohibition on having any financial or other interest that could affect impartiality. Dorbeck-Jung (n 21), at 57. See further the EC Communication on the use of experts (n 153) at 9: which provides for three core principles when seeking expert advice. The first is "quality of advice", which has three determinants: "excellence; the extent to which experts act in an independent manner; and pluralism." As to "independence" the Communication states: "It is a truism that no one is entirely 'independent': individuals can never entirely set aside all thoughts of their personal background – family, culture, employer,

declaration of interests by such experts.[162] Further, if sub-groups are installed for specific topics (as is apparently done for BCR), the risk of regulatory capture should be decreased by regular job rotation of the members of such subgroup.[163]

Recommendation 17

- Ensure the independence of the Working Party 29 in accordance with the criteria developed by the ECJ for independence of DPAs.
- Instruct the Working Party 29 to amend its Rules of Procedure to ensure its accountability as to independence by:
    - having any experts participating in its meetings issue a public declaration of interests;
    - introducing job rotation of the members of any sub-groups installed by the Working Party 29.

14.7.4 Accountability ex-post Working Party 29

As set out before, the role of the Working Party is mainly in the ex-ante norm-setting process. The key role in the ex-post accountability in relation to BCR is performed by the multinational, which role will be evaluated below. What remains relevant, however, is the ex-post accountability of the Working Party 29 towards the courts of the Member States and the ECJ. This accountability can be reduced to the question of whether the norm-setting by the Working Party 29 is subject to judicial review. Opinions of the Working Party are not binding, and as a consequence are not subject to review by the ECJ.[164] However, the flip side is that the national courts of the Member States are not bound by these opinions either. National courts

sponsor, etc. Nevertheless, as far as possible, experts should be expected to act in an independent manner. Experts can, of course, still bring to the table knowledge they hold by virtue of their affiliation, or nationality: indeed, experts may sometimes be selected for this very reason. Nevertheless, the aim is to minimise the risk of vested interests distorting the advice proffered by establishing practices that promote integrity, by making dependencies explicit, and by recognising that some dependencies – varying from issue to issue – could impinge on the policy process more than others."

162. Dorbeck-Jung (n 21), at 57.

163 Dorbeck-Jung (n 21), at 57.

164 The ECJ only reviews acts of the EU institutions and agencies "which are intended to have legal effects", see Case 22/70 *Commission v Council* [1971] ECR 263 at para. 42.

having to review decisions of their respective Lead DPA authorising BCR will therefore (have to) apply their own national data protection law. In that process the courts may take the WP Opinions into account, but they are not bound by them. To that extent, the WP Opinions are subject to judicial review by the national courts (and ultimately the ECJ). There is, however, an important qualification. In Paragraph 10.5, I concluded that at present the Data Protection Directive does not provide for the main substantive requirements for BCR to provide an adequate level of protection. Also for adequacy rulings, it is at present insufficiently defined what an "adequate level" of protection is.[165] As a consequence, if a national court (and ultimately the ECJ) has to review a decision by a Lead DPA on authorisation for individual BCR, this court has very little guidance on the rules against which the relevant BCR should be evaluated. Any judicial review in this respect is therefore difficult. The above confirms the necessity of *Recommendation 1* to European legislators, *i.e.* to recognise the BCR as an appropriate tool to provide adequate safeguards for the transfer of data and define the main substantive requirements for BCRs to be set at an adequate level. If this recommendation is indeed followed, the standard for judicial review of the WP Opinions becomes clear.

14.7.5 Norm-setting by a Lead DPA in respect of individual BCR

For a description of the approval procedure of individual BCR applications by the Lead DPA as part of the Mutual Recognition Procedure (**MRP**), I refer to Paragraph 10.4. At the time the first BCR applications to DPAs were made, it was very much the relevant DPA that decided what the BCR should look like. When over time the WP Opinions were issued, the norm-setting for BCR became more and more a top-down process by the Working Party 29 and the room to manoeuvre for the Lead DPAs became correspondingly smaller. For the DPAs that have joined the MRP, I would even claim that such DPAs are **applying** the BCR norms to the BCR application rather than **setting** norms for BCR applications. In these cases it may be maintained that the accountability requirements are no longer relevant. Insisting on participation of stakeholders in norm-setting is only relevant if actual influence can be exercised as to the outcome. At this time, however, not all DPAs have joined the MRP, and norm-setting still also takes place at the

[165] See WP Contribution on the Future of Privacy (Chapter 6, n 33), at 11: where the Working Party recommends to improve adequacy decisions, by i.e. "[d]efining more precisely the criteria for reaching the legal status of "adequacy", paying due attention to the approach of the WP29 and various other approaches to data protection around the world, and especially to the rights and principles laid down in the Joint proposal of International Standards on the Protection of Privacy."

national DPA level. I will not discuss in detail whether this norm-setting by the DPAs meets requirements of participation of and transparency to stakeholders. Briefly put, these requirements are not met. The stakeholders in the BCR (customers and employees of the multinational) are not consulted in the individual BCR authorisation procedures.[166] This would also not be advisable. The customers of the multinational are in most cases a diffuse group, spread out over numerous jurisdictions, and not represented in a specific body (other than in general by international consumer organisations like BEUC or privacy interest organisations). Inclusion of these international organisations in the national approval process before a Lead DPA does not seem opportune. This would require **international** consumer organisations and civil society organisations to participate in each and every **national** BCR authorisation procedure in the various Member States.[167] These international stakeholder organisations should be consulted on the BCR norm-setting process (i) **as part of revision of the Directive**, (ii) prior to further norm-setting on BCR by the European Commission and (iii) prior to the Working Party 29 issuing opinions on BCR (as per *Recommendation 15*). If properly consulted at those times, legitimacy demands do not require that these organisations be (again) consulted on individual BCR applications. Here "bringing the public back in" would be an

---

166 Though the employees are consulted on the BCR as part of the works council requirements, which have to be completed before the BCR are formally adopted by the multinational and submitted to the Lead DPA for formal approval. See para. 10.4, in particular para. 10.4.1.

167 The solution here would not be to organise the civil society and consumer organisations at the **national level** in order to support citizens in exercising their data protection rights (as recommended by some authors, see below). Again, as BCR apply worldwide, the stakeholders are not national organisations but international organisations. See the Rand Report (Chapter 6, n 27), at x and 45:

"**Recommendation 7 – Strengthened support for exercise of rights**

The DPAs, in conjunction with civil society stakeholders should work with consumer protection organisations (e.g. the European Consumers Association, BEUC) to institute a national network of grass-roots level 'accountability agents' to support citizens in the exercise of their fundamental rights. Although similar activities are currently undertaken by DPAs, resourcing constraints suggest that a more localised network would be a better approach, having a more widespread presence. These local accountability agents would act as another means for citizens to exercise their rights within existing arrangements." Dorbeck-Jung (n 21) at 56 notes that participation of consumers will be effective only if their representatives can rely on the relevant expertise and financial sources. This is also a recommendation of Raab and Koops (Chapter 8, n 23), at 220.

example of "too many eyes" and in any event a doubling of consultation of similar stakeholders on similar issues.[168]

The reason for not further elaborating on the legitimacy of current BCR norm-setting by DPAs is that norm-setting should not take place at Member State level at all. In Paragraph 10.6, I discussed that norm-setting for data protection is the prerogative of EU legislators, where under the TFEU regime delegation can be to the European Commission only. The role of the Working Party 29 should in principle subsequently be limited to providing further guidelines only. In this context there is no role for individual DPAs for further norm-setting. If norm-setting did take place at the national level, this could entail that norm-setting could be influenced by national interests, while the BCR have to apply on an EU (even global) level. To avoid undue influences, norm-setting should take place at the level that corresponds with the scope of application of the relevant norms. In any event it is not advisable that the DPAs are involved in norm-setting, application of norm-setting and enforcement.[169] At present for instance the DPAs in the UK and Austria[170] have issued their own national policy guidelines as to authorisation of BCR if such DPA acts as Lead DPA. In the new constellation I recommend that there is no longer room for such national policy guidelines.

If some of my previous recommendations are followed, the role of the Lead DPAs will be limited to **applying** the BCR norms rather than **setting** norms in respect of BCR: *Recommendation 2* to recognise the BCR as an appropriate tool to provide adequate safeguards for the transfer of data and define the main substantive requirements for BCRs to be set at an adequate level; *Recommendation 3* to define and impose the MRP upon all Member States) and *Recommendations 16 & 17* to ensure that the further details of

---

168 See Curtin and Senden (Chapter 6, n 67), at 15. An option that would be possible, but which I reject, is to prescribe in the revised Directive that the Lead DPA has to make the request for authorisation and the draft BCR available to the public for consultation for a prescribed period. During this time, interested parties may submit their comments prior to the Lead DPA deciding on the authorisation. This is, for instance, required by the Dutch Data Protection Act in respect of decisions of the Dutch DPA on conformity declarations in respect of self-regulatory codes (see n 85). However, these self-regulatory codes concern **national** self-regulatory codes specific for a certain industry sector. In those cases the relevant stakeholders are not yet consulted on such codes, and indeed if they are not consulted at that time, the stakeholders will not be consulted at all. Further, the national stakeholders for such codes are much better organised in the relevant Member State than at the EU level.

169 Cafaggi (Chapter 8, n61), at 222 and 224.

170 See Chapter 10, n 14.

these norms by the Working Party 29 would fully comply with the enhanced legitimacy requirements.

As BCR have EU-wide (even global) application, the most logical set-up would be to task the pan-EU Data Protection Supervisor (as per *Recommendation 4*) with central authorisation of the BCR applications. Though from a theoretical perspective this seems optimal, I do not recommend this option. If BCR becomes a mainstream tool, processing of all BCR authorisations would require a substantial organisation and will probably lead to more delays than already exist today.[171] If processing of all BCR applications were to prove quite a burden, the subsequent supervision and enforcement of all BCR on a pan-EU basis would even be more burdensome. I doubt whether setting up such an extensive EU enforcement organisation is justified as the Lead DPA (of the EU headquarters of the multinational) is in fact already well placed to supervise and enforce. In any event the pan-EU Data Protection Supervisor would in case of enforcement involve the DPA of the "home Member State" of the multinational (Lead DPA).

Below I make some final remarks on the norm-setting by the Lead DPAs.

Re (ii) Transparency

At present the Lead DPAs do not publish their authorisations of a BCR of a multinational. Also, the texts of these BCR are not publicly available. If multinationals rely on their authorisations in the course of business, their counterpart can therefore not verify whether this authorisation is indeed granted and whether the relevant data processing is indeed covered by the BCR. Insofar as the multinational itself publishes its BCR on its corporate website,[172] such counterpart cannot verify whether the published BCR indeed corresponds with the BCR as authorised. Though multinationals may not like the additional exposure of publication of the BCR authorisation (including its text)[173], transparency requirements to stakeholders dictate that the BCR authorisations, including the text of the BCR itself, should be published.

---

171 See para. 10.6.1, in particular n 52.

172 BCR requirement (xiv) requires that the beneficiaries "'should have easy access to the BCR," which, where customers of multinationals are consumers, entails that the BCR for Customer Data are published at the corporate website of the multinational.

173 The BCR regime does not require that BCR are published to the public at large. For instance BCR for Employee Data have to be made available to the employees only and not the public at large. Additional exposure may be generated for the multinational if the BCR for Employee Data would be published (see Paragraph 11.3).

Recommendation 18
Require Lead DPAs to publish the BCR authorisations including the text of the BCR authorised.

Re (iii) Independence of Lead DPA

As to the requirement of independence, it is clear that the Lead DPAs should be independent from their stakeholders.[174] Insofar as individual Member States have not sufficiently ensured the independence of their DPA, this should be remedied.[175] As the Commission has announced it will remedy this in the upcoming revision of the Directive[176] and has in the meantime already initiated enforcement action in this respect against certain Member States,[177] and since this is not of specific relevance to BCR only, no separate recommendation is included here.

---

174 Article 28(1) Data Protection Directive. See for the requirements of independence as to DPAs: Case C-518/07, *Commission v. Germany*, [2010] OJ C 113, at 3-4. On the role of DPAs, see Peter Hustinx, "The Role of Data Protection Authorities," in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 7, at 131. See more in general on the requirement of independence of national regulatory agencies: Annetje Ottow and Saskia Lavrijssen, 'The legality of independent regulatory authorities', in: L. Besselink, F. Pennings & A. Prechal (eds), The Eclipse of Legality, Kluwer Law International, 2010, Chapter 5, at 73-96.

175 The independence of DPAs is not adequately ensured in all Member States, see Korff (Chapter 6, n 27) for a review of the independence of the DPAs of the various Member States at 200-209.

176 EC Communication on the revision of the Directive (Chapter 6, n 34), at para. 2.5. See further the EDPS Opinion on the revision of the Directive (Chapter 6, n 35), at para. 181: "The EDPS fully supports the objective of the Commission to address the issue of the status of data protection authorities (DPAs), and to strengthen their independence, resources and enforcement powers. He recommends:

- Codifying in the new legal instrument the essential notion of independence of DPAs, as specified by the ECJ.
- Stating in the law that DPAs must be given sufficient resources.

Giving authorities harmonised investigation and sanctioning powers."

177 See Case C-518/07, *Commission v. Germany*, [2010] OJ C 113, at 3-4. On 6 April 2011, the European Commission formally requested that Germany immediately comply with this judgment. See memo/11/220 on 11 April 2011, to be found on http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/220&format=HTML&aged=0&language=EN&guiLanguage=en.

Re (iv) Accountability ex-post Lead DPA
The decision of a Lead DPA to authorise individual BCR is subject to judicial review by its national courts[178] (and ultimately by the ECJ).
But again such judicial review is difficult due to the fact that the BCR requirements are not included in the Data Protection Directive. If *Recommendation 1* is followed and BCR are embedded in the revised Directive, this issue will be solved.

14.7.6 Accountability ex-post: phase (b) monitoring and evaluation and phase (c) enforcement

The multinational is the actor involved in the monitoring and evaluation of the BCR and the enforcement thereof. As the criteria for evaluation of phases (b) and (c) to a certain extent overlap, I will discuss them together.

Re (i) Evaluation
This requires the multinational to implement processes to monitor and review progress and results against goals and objectives; to feed learning from this back into the organisation on an ongoing basis; and to report on the results of the process.[179] As discussed in Paragraph 13.5.3, these criteria are also requirements under the accountability principle (see the "common fundamental" sub 5 (ongoing risk assessment and mitigation) and sub 7 (program risk assessment oversight and validation). I concluded there that these elements are not (sufficiently) part of the present BCR regime, and recommended adding these as requirements for BCR as per *Recommendation 12*.

Re (ii) Complaints and response procedures
One of the requirements of the BCR regime is an internal complaints and response procedure (BCR requirement (viii)). If complaints are not adequately addressed, recourse is open to the Lead DPA and the courts of the Lead DPA (and ultimately the ECJ). This requirement is therefore adequately ensured.

Re (iii) Information
The information requirements can be divided into passive information requirements (where the multinational has to provide information at request) and active information requirements (where the multinational has to provide information at its own initiative).

---

178 As required by Article 28(3) Data Protection Directive.

179 See para. 14.6.3.

The **passive** information requirements are adequately safeguarded by the BCR regime:

- The multinational has an obligation to perform audits and has to provide the results of such audits to the Lead DPA[180] **upon its request** (see BCR requirement (xiii)).
- The Lead DPA has the right to perform audits itself (see BCR requirement (xii))
- Compliance with the BCR is enforceable by the individuals via the Lead DPA and the Court of the Lead DPA, as a part of which the multinational will have to provide information, explanations and justifications (BCR requirement (ix))
- The group companies have a duty to cooperate with the Lead DPA, to abide by its advice regarding the BCR and to submit to its audits (BCR requirement (xii))
- The burden of proof in respect of data protection breaches is on the multinational (BCR requirement (xi)).

As to **active** information requirements (i.e. mandatory periodical provision of information at the own initiative of the multinational) these are not adequately safeguarded in the current BCR regime. The active information obligations of the multinational are limited to reporting on privacy compliance to the **internal accountability forums** of the multinational:

- The results of the audit performed by the multinational have to be communicated to (i) the internal privacy function and (ii) the ultimate parent's board (BCR requirement (xiii)).
- Changes in the BCR must be reported to the Lead DPA (BCR requirement (xvi))
- Group companies have to "be transparent" if applicable law prevents them from complying with the BCR and, if in doubt what action to take, consult the Lead DPA (BCR requirement (xviii).

The BCR regime does not prescribe any further active information duties of the multinational either to the Lead DPA or to the stakeholders. In light of the strong **passive** information requirements towards the Lead DPA, introduction of additional **active** information obligations towards the Lead DPA does not seem efficient. This will just increase administrative burdens on the multinationals, while leading to an information overload with the Lead DPA. This may lead to expectations of review of such information by

[180] In para. 10.2, I discussed that the WP Opinions require that all DPAs obtain these rights, but that it has by now accepted that these rights may be concentrated with the Lead DPA. See Chapter 10, n 21.

the Lead DPA, which seems unrealistic and will therefore just work counterproductively.

Insofar as stakeholders are concerned, multinationals do not have any active information requirements and the current passive information requirements (in case of complaints or litigation) seem to be insufficient. An active information requirement is therefore indicated. Such transparency towards stakeholders also follows from the introduction of the accountability principle discussed in Paragraph 8.3, which led to *Recommendation 12* (To prescribe the reporting on BCR in the annual reports of company in a comparable format and further on the number of complaints received and the nature of these complaints under the internal complaints procedure).

Re (v) Debate and Re (vi) Pass judgement

These requirements do not require much discussion as any decision of the multinational on complaints under the BCR are subject to review by the Lead DPA and the courts of the Lead DPA. Both instances traditionally incorporate the possibility to debate and pass judgement. As to the enforcement powers of the Lead DPAs, there are concerns as to their harmonisation and whether some of their sanctions are sufficient. This has already been discussed in Paragraph 10.5 and led to *Recommendation 4 (*To provide for equal enforcement powers for DPAs and develop a common enforcement strategy for the DPAs to ensure equal enforcement).

14.8 Visualisation proposals

The following charts visualise my proposals by comparing the current and future situation for the three phases of the regulatory process (a) norm-setting, (b) evaluation and monitoring and (c) enforcement.[181]

[181] See Cafaggi (Chapter 8, n 61), at 215.

Chart 1

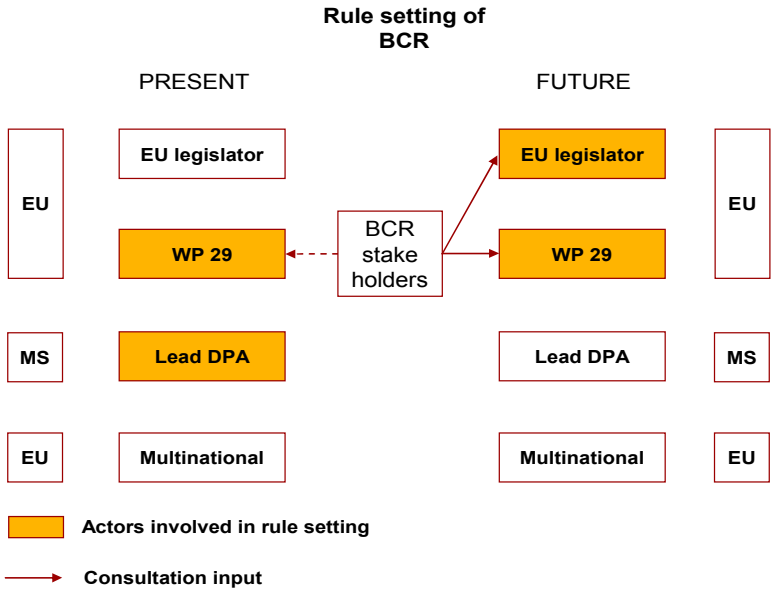


Chart 2

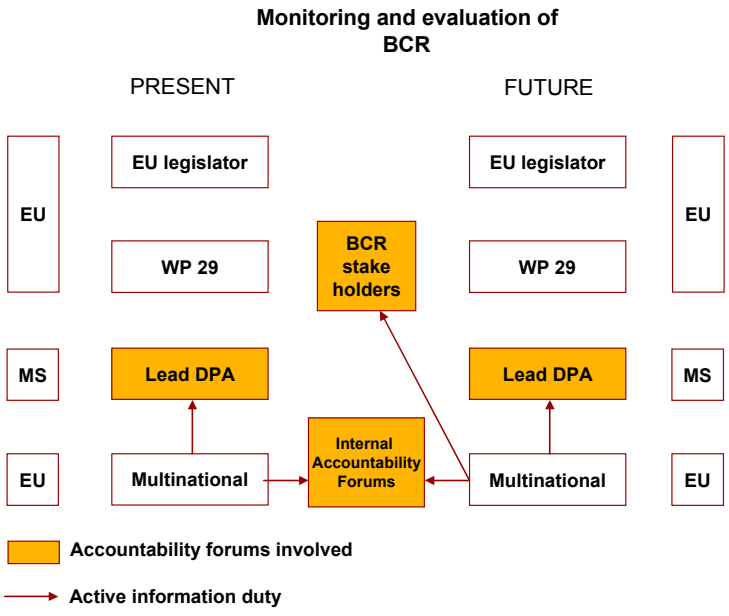
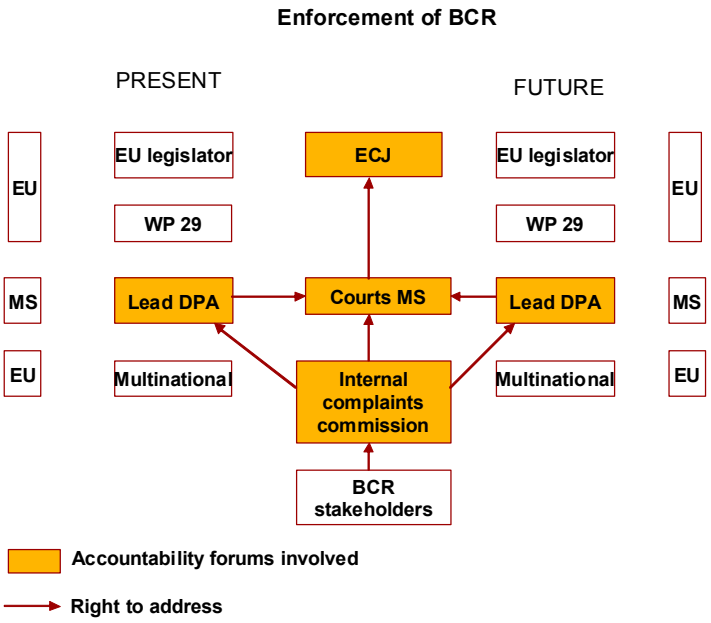


Chart 3



14.9 Conclusion as to legitimacy of BCR as a form of TPR

The conclusion is that the present requirements for BCR do require substantive updating to be aligned with legitimacy demands of TPR. This will not, however, lead to (many) new recommendations as these requirements also follow from an evaluation of the BCR regime against other disciplines (most notably the accountability perspective). Additional recommendations resulting from legitimacy demands to be made of the BCR as a form of TPR are:

Recommendation 15

- Hold a proper consultation of all stakeholders of BCR prior to enacting the norms for BCR in the revised Data Protection Directive (or the EU regulation);
- Instruct the European Commission to hold a consultation of all stakeholders of BCR prior to further norm-setting on BCR by the European Commission;

Recommendation 16
Instruct the Working Party 29 to amend its Rules of Procedure to remedy the lack of transparency as to its decision-making process.

Recommendation 17
- Ensure the independence of the Working Party 29 in accordance with the criteria developed by the ECJ for independence of DPAs.
- Instruct the Working Party 29 to amend its Rules of Procedure to ensure its accountability as to independence by:
    - having any experts participating in its meetings issue a public declaration of interests;
    - introducing job rotation of the members of any sub-groups installed by the Working Party 29.

Recommendation 18
Require Lead DPAs to publish BCR authorisations including the text of the BCR authorised.

15 BCR in the context of Corporate Social Responsibility (CSR)

CSR codes typically involve a commitment by multinationals (usually in their Code of Ethics or Business Principles) to enhanced concern for human and civil rights, the environment, opposition to bribery and corruption and fairness to their customers and suppliers. The number of multinationals adopting CSR codes has increased steadily over the years, and in the US all of the Fortune 500 companies have introduced CSR codes. The reporting on CSR has also steadily increased, 95 of the US top 100 companies produced a CSR report for 2005 - 06.[1] In December 2007 Vogel reported that approximately 300 CSR codes were issued governing "most major global economic sectors, such as energy, minerals and mining, forestry, chemicals, textiles, apparel, footwear, sporting goods, project finance, and coffee and cocoa".[2] The range of issues that multinationals include in their CSR codes is also constantly expanding and often now includes a commitment to protect the privacy of their employees and customers.[3] Many aspects of CSR codes have been discussed or referred to in previous Paragraphs (and especially in the footnotes) as CSR codes (i) present similar issues under contract law (see Chapter 11); (ii) are a form of TPR (see Chapter 14); and (iii) are based on the accountability principle (see Chapter 13). As a consequence, I already discussed how CSR codes implement contractual supply chain management (see Paragraph 11.4), how CSR codes being unilateral undertakings are enforced (see Paragraph 11.3), how legislators have introduced incentives to foster the introduction of CSR compliance programmes (see Paragraph 13.2), and whether self-regulatory CSR codes are a suitable tool to regulate human rights (see Paragraph 14.5). I have not yet discussed to what extent data protection is covered by **international instruments** setting guidelines for CSR codes, and if so, whether this has any repercussions for the BCR regime. This requires again a discussion of regulating human rights, not so much in the context of whether these may be regulated by self-regulation, but whether international instruments require that fundamental rights held by individuals should be viewed as imposing duties directly on multinationals even if these multinationals are active in countries **that do not recognise such human rights**. This is relevant for

---

1 For an overview of the percentages over the last ten years, see McBarnet (n Chapter 8, 23), at 10.

2 David Vogel, "Private Global Business Regulation," in: *Annu. Rev. Polit. Sci.* 2008. 11:261–82, at 262

3 See Gus Hosein, 'Challenges in Privacy Advocacy', in: Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?* (Springer 2009), Chapter 15, at 254. See for instance Article 1.5 of the General Business Principles of Royal Philips Electronics N.V. and its group companies, to be found at http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/GeneralBusinessPrinciples.pdf

BCR as the current BCR regime allows multinationals to limit the scope of BCR to for instance EU originated data only.[4] If international instruments on CSR require that the data of individuals in countries that do not provide for data protection also be covered, these scope limitations would be in violation of these CSR instruments.

15.1 Norms regulating CSR

Discussing **norms** regulating CSR seems a contradiction in terms. The adoption of CSR codes is routinely characterised as voluntary, companies going the extra mile to go beyond just compliance with law.[5] Though adoption of CSR codes is voluntary, there has been a firm push both from soft law (like international guidelines for CSR) and hard law (like disclosure and whistle-blowing requirements for CSR) that makes CSR codes much less voluntary than they may seem at first.[6] Further, once adopted, CSR codes are in most cases no longer voluntary.[7] However, also without explicit adoption of a CSR code, domestic and international courts have found avenues to grant binding effect to international soft law regarding CSR.[8]
What is relevant for BCR is to what extent any soft law concerning CSR also extends to data protection. And if so, whether such soft law actually requires (or is at least a strong driver for) multinationals to include data protection

4 See for other ways in which the scope of BCR may be limited para. 10.2, in particular n 17 and n 18.

5 The European Commission in its communication on CSR reported that there is large consensus that CSR is voluntary adopted behaviour by businesses over and above the legal requirement, see [COM (2002) 347, at 8. In its subsequent 'Framework for Action,' the EC made "recognition of the voluntary nature of CSR" its first principle, see [COM (2002) 347.

6 McBarnet (Chapter 8, n 23), 13.

7 Cafaggi (Chapter 6, n 67), at 1 and 16; and Eijsbouts (n 12), at 90 and fn 180 for further literature.

8 Cafaggi (Chapter 6, n 67), at 28: "While it is certainly true that the degree of "bindingness" is lower than (that of) hard law, it should be clearly acknowledged that domestic and international courts have granted binding effects to soft law through different avenues: international customary law, private law, mainly contract and civil liability," which various legal grounds are discussed at 27 – 3, with many examples in the footnotes see especially footnote 154, at 28). See Clapham (Chapter 14, n 66), at Chapter 10. See for a comprehensive overview of the many (indirect) ways in which international CSR norms works through in the Dutch legal order and the various legal bases for enforcement thereof, A.J.A.J. Eijsbouts, "Maatschappelijk (verantwoord) ondernemen: naast, in of met recht," in: A.J.A.J. Eijsbouts et. al., *Maatschappelijk Verantwoord Ondernemen en het Recht*, Preadviezen NJV 2010-1 (Kluwer 2010), at para. 4, at 10 and Eijsbouts (Chapter 11, n 12), at paras. 5, 6 and 7. See on enforcement of multilateral undertakings in general para. 11.3.

commitments in their CRS codes. In that case BCR would be more or less indispensible to ensure accountability in respect of these data protection commitments. Also, the question should be posed whether soft law in relation to CSR has by now become part of "good corporate governance" also labelled as "corporate accountability" and as such part of the norms against which corporate conduct has to be evaluated.

15.2 CSR and international law

15.2.1 Introduction

Discussing **international** norms regulating CSR also seems a contradiction in terms.[9] Multinationals are not subjects of international law as such.[10] Other than in specific EU regulations, etc., duties can only be imposed on them by national law, not by international law. As discussed in Paragraph 14.5, human rights have further traditionally been understood as rights that individuals enjoy against states. The fact is, however, that by now many multinationals wield as much or even more power than many states, and the conditions of individuals' lives are shaped as much by multinationals as by states, especially if such states are developing countries in need of revenues to repay their debts. As the CEO of Wal-Mart phrased it: "Our size and scale means that even one small environmental change in our policy or our customers' habits has exponential impact around the world";[11] a phenomenon that has been labelled "the Wal-Mart effect". As rights are at bottom a response to the problem of power, the perspective on the role of multinationals has shifted over time. Multinationals in the context of CSR are nowadays considered more like states than individuals and thus should be located more on the public than the private side in assigning human rights and duties.[12] As Clapham in his classic work on human rights puts it: "The definition of the public sphere (…) has to be adapted to include (…) new centres of power (…) such as (…) multinationals (…) the individual now perceives [as sources] of authority, repression, and alienation". [13] At the heart of these developments is the notion that companies owe obligations to the societies in which they operate, i.e. require a "license to operate", which license has a number of dimensions. Besides the legal dimension, these also

9 This Paragraph draws on Muchlinski (Chapter 13, n 26), at 431-485 and Sinden (Chapter 14, n 61), at 501 -526.

10 Cafaggi (Chapter 6, n 67), at 28.

11 As cited in McBarnet and Kurkchiyan (Chapter 9, n 41), at 61.

12 Sinden (Chapter 14, n 61), at 506 and 515.

13 Clapham, (Chapter 14, n 66), at 137.

include an economic and social dimension.[14] The social license concept includes the demands of social actors, i.e. where a company's failure to meet social expectations can impair the company's reputation and trigger demands for stronger legal controls.[15] Due to these developments, there seems to be growing consensus in general terms that certain fundamental rights held by individuals may under circumstances be viewed as imposing duties directly on multinationals even if these multinationals are active in countries that do not recognise such human rights.[16]

The question then arises as to what particular fundamental rights we are talking about. Clearly not all rights enforceable against states are relevant in the context of CSR of multinationals. For instance, a multinational will not act as prosecutor and the criminal procedure rights of individuals are therefore of no relevance vis-à-vis multinationals. Other rights will require some creative adaptation to apply in the context of multinationals.[17] Further, as indicated in Paragraph 6.3 there is a trend to bring increasingly more topics under the umbrella of CSR. At the moment consensus has not fully crystallised which fundamental rights should indeed lead to direct obligations for multinationals. I will argue below that (i) the right to data

---

14 See for a good overview of the different dimensions of the licence to operate, Gunningham (Chapter 9, n 38), at 480 -493. On licences to operate, see Eijsbouts (n 8), at para. 3 at 8 -10; and Eijsbouts (Chapter 11, n 12), at 61.

15 Gunningham (Chapter 9, n 38), at 482.

16 See McBarnet (Chapter 8, n 23), at 56; McBarnet and Schmidt (Chapter 11, n 12), at 148 – 176; Clapham (Chapter 14, n 66), at Chapter 6 in particular para. 6.11; and Chalmers (Chapter 14, n 66), Chapter 6, at 187 – 188. Willem van Genugten, "Handhaving van Wereldrecht, een kritische inspectie van valkuilen en dilemma's," [2010] Nederlands Juristenblad-1 at 12, as referred to in Chapter 14, n 66. See also in more detail Willem van Genugten, Kees Homan, Nico Schrijver and Paul de Waart, *The United Nations of the Future; Globalization with a Human Face* (Amsterdam: KIT Publishers 2006). Also Cafaggi (Chapter 6, n 67) at 28: "The limited direct applicability of soft law to private parties derives from the more general principle of public international law which, conventionally, imposes primary responsibility on States. This view has been criticized and increasingly international law obligations are also applied directly to private parties," referring to (see fn 156) "Case 36/74, Walrave v. Association Union Cycliste Internationale, 1974 E.C.R. 1405, where the ECJ held that anti-discriminatory provisions of the Treaty of Rome also apply to private entities (employment discrimination)." However, see C.C. van Dam, Onderneming en mensenrechten (oratie Utrecht), [2008], at 29-30, who indicates that only a few international norms are directly applicable to multinationals (i.e. have horizontal effect), which includes the right to privacy. All other norms have indirect horizontal effect in the national legal orders for instance via liability based on tort. See also Eijsbouts (Chapter 11, n 12), at 84 and 102.

17 Sinden (Chapter 14, n 61), at 520.

protection is included in the core human rights principles that are considered to impose direct duties on multinationals; and (ii) the rights to data protection do not require tailoring for application in this context.

15.2.2 Do the core CSR principles include data protection?

The following paragraphs will show that the right to privacy and data protection is one of the fundamental human rights covered by the international instruments of soft law on CSR. This is not surprising. Different from most human rights that traditionally are conceived of as norms primarily meant to shield individuals from repressive state action, data protection rights have from the outset been primarily directed at companies (see Paragraph 14.5.3). In the substantive literature on CSR, there is common ground on the international and intergovernmental human rights instruments that are leading in this respect, as evidenced by the consistent references thereto, such as the OECD Guidelines for Multinational Enterprises, the ILO's Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy, the UN Global Compact and the Draft UN Norms 2003. These instruments (including their relevance to data protection)[18] as well as the EU position on CSR and expected future developments based on the "Ruggie Report", refer to the right to data protection.

15.2.3 OECD Guidelines

In 1976, the first codification of CSR norms was undertaken by the OECD in the "OECD Guidelines for Multinational Enterprises" (**OECD Guidelines**).[19] The OECD Guidelines were revised in 2000[20] and a further revision has been announced.[21] While the OECD Guidelines are non-binding, they benefit from the commitment of adhering governments to promote their actual observance by business. The OECD Guidelines are therefore relevant for multinationals whose corporate headquarters are established in one of the OECD member states (30 in total of which a number are EU

---

[18] For a full overview, including how these instruments and initiatives relate to each other and their legal status, see the Report of the United Nations High Commissioner on Human Rights on the responsibilities of transnational corporations and related business enterprises with regard to human rights, UN Doc. E/CN.4/2005/91, 15 February 2005, to be found at <http://www2.ohchr.org/english/issues/globalization/business/reports.htm >.

[19] To be found at <www.oecd.org>.

[20] OECD Guidelines for multinational enterprises, Paris: OECD Publishing 2008, <www.oecd.org>.

[21] See OECD, Consultation on an update of the OECD Guidelines for Multinational Enterprises, Consultation Note, 8 December 2009 at <www.oecd.org>.

Member States) and 4 additional states that have committed to the OECD Guidelines. The OECD Guidelines are further supported by the EU. [22] The OECD Guidelines have an international monitoring mechanism by means of National Contact Points (**NCP**). Parties that have complaints about a multinational's adherence to the OECD Guidelines can file complaints there. The relevant NCP subsequently performs fact-finding after which a mediation process begins. If this mediation process does not have the desired result (or the multinational does not cooperate), the NCP may draw up its own conclusions and publish these. This *naming and shaming* is a *de facto* sanction. Adherence to the OECD Guidelines is further often a requirement for the awarding of export credits and government subsidies. The character of the OECD Guidelines is therefore less voluntary than they may seem at face value.[23]

Pursuant to Principle 1 of the OECD Guidelines, multinationals should "respect the human rights of those affected by their activities consistent with the host government's international obligations and commitments". The human rights respected by the OECD host governments will include the right to privacy and data protection as these are recognised as such in the international conventions on human rights to which these host states are party.[24] Further, pursuant to Principle 5 of Chapter VII of the OECD Guidelines, multinationals are required to "respect consumer privacy and provide protection for personal data". In the official commentary to this Principle, it is stated that "enterprises could look to the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data as a helpful basis for protecting personal data."[25]

---

22 For the list of adhering governments and the support of the EU, see the OECD Guidelines (n 20), at 6.

23 Eijsbouts (n 8), at 17.

24 See Article 12 of the Universal Declaration of Human Rights (1948); Article 17 of the International Covenant on Civil and Political Rights (1966); paras 5, 6 (14) and 12 (2b) of the ILO Code of Practice: Protection of Workers Personal Data (1997); Article 3(a) of the UN Guidelines for the regulation of Computerized Personal Data Files (1990); and Article 9 of the OECD Guidelines: On the Protection of Privacy and Transborder Flows of Personal Data (1980). See further for the recognition of privacy and data protection as human rights in the EU, footnote 3.

25 See Part II of the OECD Guidelines (Chapter 6, n 38)) at para. 52.

15.2.4 UN Global Compact

The United Nations Global Compact (**UN Global Compact**)[26] is a voluntary initiative for multinationals that are committed to aligning their operations and strategies with human rights, labour conditions, the environment and anti-corruption. Its ten Principles find their origin in the Universal Declaration of Human Rights (among three other declarations).[27] The UN Global Compact was "grandfathered" by UN Secretary-General Kofi Annan and launched on 26 July 2000. Currently about 6,400 business and 2,300 non-business participants in over 130 countries have engaged with the UN Global Compact. Pursuant to the first Principle, "Businesses should support and respect the protection of internationally proclaimed human rights". The commentary makes clear that this is understood to include the right to privacy and data protection of workers and consumers.[28]

15.2.5 Draft UN Norms 2003

At the level of the United Nations, there have been two initiatives to adopt instruments similar to the OECD Guidelines, but these have never passed the draft stage. The first is the Draft UN Code of Conduct for Transnational Corporations 1990[29] and the second is the Draft UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with regard to Human Rights 2003[30] (**Draft UN Norms 2003**). After various consultations and further research it was determined

---

26 <www.unglobalcompact.org>.

27 <http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html>.

28 On Principle 1: "Another approach some businesses find helpful is to start by looking at what the business is already doing to respect and support human rights, such as (…) respecting the privacy of customers and workers (…)," to be found at <http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/principle1.html>. The self-assessment tool provided for the business participants to the UN Global Compact also contains a question on privacy compliance: "Does the company respect the privacy of its employees whenever it gathers private information or monitors the workplace?" (Principle 1). The explanatory notes to this question say that: 'The question relates to the right to privacy. It is based on general principles contained in the following: Article 12 of the Universal Declaration of Human Rights (1948); Article 17 of the International Covenant on Civil and Political Rights (1966); paras. 5, 6 (14) and 12 (2b) of the ILO Code of Practice: Protection of Workers Personal Data (1997); Article 3(a) of the UN Guidelines for the Regulation of Computerized Personal Data Files (1990); and Article 9 of the OECD Guidelines: On the Protection of Privacy and Transborder Flows of Personal Data (1980)." See: <http://www.globalcompactselfassessment.org/humanrights/fairtreatment>.

29 UN Doc. E/1990/94.

30 UN Doc E/CN.4/Sub.2/2003/12/Rev.2.

that these Draft UN Norms 2003 would not become a legally binding instrument.

Pursuant to paragraph E, para. 12 of the Draft UN Norms 2003, multinationals have to "observe standards that protect civil and political rights and are otherwise in accordance with the International Covenant on Civil and Political Rights (ICCPR) and the relevant general comments adopted by the Human Rights Committee."[31] The right to privacy qualifies as a civil right under Article 17 of the International Covenant on Civil and Political Rights.

15.2.6 ILO's Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy

In 1977, the International Labour Organisation (ILO) adopted the Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy, which was subsequently amended in 2000 and 2006.[32] ILO's Governing Body includes representatives of governments and employers' and workers' organisations (i.e. it is tripartite). The principles laid down in this instrument offer guidelines to these social parties and multinationals in such areas as employment and conditions of work and life, which these parties are recommended to observe on a voluntary basis.

Pursuant to the first principle of the General Policy of the ILO Declaration, the social partners and multinationals should "respect relevant international standards", and the preamble contains a specific reference to the activities of the OECD and the UN Commission on Transnational Corporations (which include the right to privacy and data protection). Pursuant to the first principle, the parties should further "respect the Universal Declaration of Human Rights and the corresponding International Covenants adopted by the General Assembly of the United Nations" and "should also honour commitments which they have freely entered into, in conformity with the national law and accepted international obligations." The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights includes the right to privacy and data protection. In 1997,

---

[31] Commentary on the Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights, at 14 (e). To be found at: <http://www.unhchr.ch/Huridocda/Huridoca.nsf/0/293378ff2003ceb0c1256d7900310d90/$FILE/G0316018.pdf>

[32] As adopted by the Governing Body of the International Labour Office at its 204th Session (Geneva, November 1977) as amended at its 279th (November 2000) and 295th Session(March 2006), to be found at <www.ilo.org>.

the ILO itself issued the ILO Code of Practice: Protection of Workers Personal Data.[33]

15.2.7 EU position on CSR

The EU has opted to actively improve and promote the international instruments mentioned above.[34] So far, the EU approach to CSR has been based on voluntarism,[35] but the general expectation is that EU regulatory action on CSR is imminent.[36] Unlike the EU Commission, the European Parliament has consistently been in favour of a normative rather than a voluntary approach[37] and already in 1998 called the Commission to bring out a European directive that would address all CSR issues, including making corporate reporting on CSR mandatory.[38] The EU further promotes CSR

---

33 Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966). The ILO Code of Practice: Protection of Workers Personal Data, may be found at <www.ilo.org>.

34 This was made explicit for the first time in July 2001 in the European Commission, Green Paper, Promoting a European Framework for Corporate Social Responsibility, COM (2001) 366 final, at para. 17. This approach was reinforced by subsequent communications from the Commission, the European Council and the Parliament (European Commission, Communication Concerning Corporate Social Responsibility: A Business Contribution to Sustainable Development, COM (2002) 347 final, Council Resolution on Corporate Social Responsibility [2003] OJ C39/3). For an overview of activities of the EU to promote the international CSR instruments and further the debate thereon, see Voiculesco (n 55), at 378 – 386; and L.F.H. Enneking, "Crossing the Atlantic, The Political and Legal Feasibility of European Foreign Direct Liability Cases," [2009] The George Washington International Law Review, vol. 40, at 907 – 910.

35 The definition of CSR upon which the Green Paper is based is one of CSR: "a concept whereby companies integrate social and environmental concerns in their business operations and in their interaction with their stakeholders on a voluntary basis."

36 Voiculesco (Chapter 13, n 55) at 395; Eijsbouts (n 8), at 15 and Enneking (n 34), at 912.

37 Already in 1998, the European Parliament called for the establishment of a European framework setting a "legal basis for multinationals operations all over the world," see: European Parliament, Resolution on EU Standards for European Enterprises Operating in Developing Countries: Towards a European Code of Conduct, INI/1998/2075. See also A4-0508/98-Howitt and A4-0198/98-Fassa.

38 European Parliament, Report on the Commission's Green Paper on Promoting a European Framework for Corporate Social Responsibility, A5-0159/2002 Final, at 18. The European Parliament has been part of the European CSR debate from the beginning. For an initial publication on this topic, see European Parliament, Resolution on EU Standards for European Enterprises Operating in Developing Countries: Towards a European Code of Conduct, INI/1998/2075. See also A4-0508/98-Howitt and A4-0198/98-Fassa.

through the international development cooperation agreements it enters into with developing countries, by making human rights observance an essential element and a condition of trade terms and development aid.[39] This "human rights clause" now applies to over 120 countries.[40]

However, even without regulatory action at the EU level, the initial Green Paper of the European Commission on CSR is based on the premise that multinationals will observe both national and international legislation, in particular the human rights covenants.[41]

Further, the relevant international norms have now found their way into many of the legal orders of the Member States, by means of a wide range of government initiatives, which in most cases combine a mix of hard and soft law (codes of conduct and reporting mechanisms being among the most common).[42] Authors researching the status of CSR norms in the international instruments therefore generally conclude that these norms are (to a certain extent) already part of the legal orders of the Member States and enforceable against multinationals.[43] This will *a fortiori* be the case if companies have adopted CSR codes containing a unilateral undertaking to

---

39 Such a clause has been defined and refined since the early 1990s. To ensure consistency, in the text used and its application, a European Council Decision of May 1995 spelt out the modalities: Commission Communication on the Inclusion of Respect or Democratic Principles and Human Rights in Agreement Between the Community and Third Countries, COM(95) 216 of 23 May 1995 and Council Conclusions of 29 May 1995, EU Bulletin No 5 1995 at point 1.2.3. See on the impact of the human rights clause: Voiculescu (n 55), at 384.

40 Voiculesco (Chapter 13, n 55), at 385.

41 See Green Paper (n 34), at para. 52 and Voiculescu (Chapter 13, n 55), at 381 and 395.

42 Voiculescu (Chapter 13, n 55), at 394. See for an overview of the Dutch soft and hard law regulatory mix: Eijsbouts (n 19), at 10.

43 See McBarnet (Chapter 8, n 23), at 56.; McBarnet and Schmidt, (Chapter 11, n 12) at 148 – 176; and Clapham,(n 66), at para. 6.11. See further Stephen Bottomley and Anthony Forsyth, "The New Corporate law: Employees' Interest," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law* (Cambridge University Press 2007), at 335, where it is recognised that "in everyday corporate practice, the boundaries between the law and codes are not always felt so clearly. This idea builds on the argument developed elsewhere, that the category of law known as corporate law is being transformed into a broader category of law known as 'corporate governance': 'corporate law may in the past have been described as a one-dimensional body of law concerned with regulating the interests of investors, managers and directors. The impact of regulation has been to transform this body of law into an emerging law of corporate governance, which seeks to integrate the policies and concerns of broad areas of regulation into corporate law." See for a similar conclusion in respect of the Dutch legal order, Eijsbouts (n 12), at 82.

abide by these CSR norms.[44] Authors even conclude that corporate self-regulation may be indispensable to avoid liability, for instance in industries with a high potential of violating particular rights.[45] An example given in this context is the situation where a parent company influences the production process of its products by issuing corporate guidelines. If a subsidiary causes damages following these instructions, the parent may be liable if the procedures issued were below the required standard of a reasonable operator.[46] Taking this one step further, a parent company may breach a duty of care to employees and customers if a parent is establishing subsidiaries in another country (known not to have proper product safety requirements) without taking proper care of its production management by issuing corporate guidelines (including proper training and monitoring and auditing).[47] Regulatory action of European legislators on CSR will therefore to a certain extent be a codification of already existing and enforceable CSR norms.

15.2.8 The Ruggie Framework for future action

The extensive discussions and fundamental differences of opinion on the Draft UN Norms 2003, and a call for making these Norms legally binding for multinationals, in 2005 led to the appointment of John Ruggie as UN Special Representative for Business and Human Rights and in 2008 to the "Ruggie Report".[48] The Ruggie Report presents a framework for further action on CSR (**Ruggie Framework**) and was adopted by the UN following extensive consultations with leading NGOs and large global business organisations (and was relabelled **UN Framework**).[49] The UN Framework lists the core human rights principles on which business has an impact and therefore must be respected, which include the right to privacy and data protection.[50]

---

44 See para. 11.3 for possibilities of enforcing such unilateral undertakings. For a comprehensive overview of common legal basis for enforcement of CSR codes in the various jurisdictions, see Glinski (n 10), at 119-147.

45 See Glinski (Chapter 11, n 10), at 122 and 143.

46 Glinski (Chapter 11, n 10), at 143.

47 See for examples in a number of jurisdictions, Glinski (Chapter 11, n 10), at 143.

48 See the Ruggie Report (Chapter 14, n 64).

49 See the background paper on the UN Framework at 1, to be found at <http://198.170.85.29/Ruggie-protect-respect-remedy-framework.pdf>. The Human Rights Council of the UN has unanimously approved the Ruggie Framework and it is now referred to as the "UN Framework."

50 See the Ruggie Report (Chapter 14, n 64), at 16. This can further be derived from the references to the international instruments made in the Ruggie Report (Chapter 14, n 64) (i.e. the OECD

The UN Framework subsequently comprises three core principles: (i) the duty of the state to protect against human rights abuses by third parties, including business; (ii) the corporate responsibility to respect human rights; (iii) and the need for more effective access of individuals to remedies. As to the first principle concerning the duty of states, the UN Framework is clear in the position that states should help prevent human rights abuses **abroad** by corporations based within their territory, provided these actions meet an overall reasonableness test, which includes non-intervention in the internal affairs of other states and that states should be more creative in this respect than they are at present.[51]

As to the second principle, the UN Framework is clear that multinationals have a duty to observe human rights principles recognised by international law, even where national law does not provide so, and to have a system of "due diligence" to ensure such compliance:

> "23. The corporate responsibility to respect human rights is the second principle. It is recognized in such soft law instruments as the [ILO] Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy and the OECD Guidelines for Multinational Enterprises. It is invoked by the largest global business organizations in their submission to the mandate, which states that companies "are expected to obey the law, even if it is not enforced, and to respect the principles of relevant international instruments where national law is absent". It is one of the commitments companies undertake in joining the Global Compact. And the Special Representative's surveys document the fact that companies worldwide increasingly claim they respect human rights.
> 24. To respect rights essentially means not to infringe on the rights of others - put simply, to do no harm. Because companies can affect virtually all internationally recognized rights, they should consider the responsibility to respect in relation to all such rights, although some may require greater attention in particular contexts. There are situations in which companies may have additional responsibilities - for example, where they perform certain public functions, or because they have undertaken additional commitments voluntarily. But the responsibility to respect is the baseline expectation for all companies in all situations.

Guidelines, the ILO Declaration and the UN Global Compact), which all include the right of privacy and data protection. For actual impact of multinationals on privacy, see Addendum 2 to the Ruggie Report, at 13, reporting that in 20-25% of the cases reviewed an impact on privacy was reported.

51 See Ruggie Report (Chapter 14, n 64), at para. 17-22.

> 25. Yet how do companies know they respect human rights? Do they have systems in place enabling them to support the claim with any degree of confidence? Most do not. What is required is due diligence - a process whereby companies not only ensure compliance with national laws but also manage the risk of human rights harm with a view to avoiding it. The scope of human rights-related due diligence is determined by the context in which a company is operating, its activities, and the relationships associated with those activities."

The UN Framework further contains many suggestions for governments as to how to implement the UN Framework in both national and international jurisdictions.[52] The UN Framework is generally accepted as a milestone in the long-standing discussion on human rights obligations of multinationals.[53] Based on the Ruggie Report, the conclusion is justified that enforceable human rights obligations for multinationals are, or in any event will become, the norm rather than the exception.[54] This has consequences for the BCR regime as the BCR regime currently allows multinationals to limit the scope of BCR to for instance EU originated data only.[55] I therefore recommend that EU legislators provide that the BCR regime be applicable to all data processed by a multinational.

Recommendation 19
Provide that the BCR regime applies to all personal data processed by the multinational adopting the BCR.

15.2.9 Due diligence

The UN Framework requires that companies perform "due diligence" in respect of their human rights compliance, which requires not only that they ensure compliance with national law, but also manage the risk of harming human rights with a view to avoiding harm. The scope of this due diligence is, according to the UN Framework, determined by the context in which a company operates, its activities, and the relationships associated with those activities. It is not surprising that the "due diligence" as prescribed by the UN Framework to a large extent corresponds with the generally accepted accountability principles as discussed in Paragraph 13. This entails

52 See also Ruggie Report (Chapter 14, n 64) at 16.

53 Eijsbouts (n 8), at 15.

54 Eijsbouts (Chapter 11, n 12), at 102 suggests introducing a global treaty imposing liability on the parent company for its group companies for violations of CSR norms by its group companies.

55 See for other manners in which the scope of BCR may be limited para. 10.2, in particular n 17 and n 18.

implementation of a data protection compliance program similar to that of BCR, with proper supply chain management, worldwide training, monitoring, auditing and reporting.

> "The Special Representative's research and consultations indicate that a basic human rights due diligence process should include the following.
>
> **Policies**
>
> 60. Companies need to adopt a human rights policy. Broad aspirational language may be used to describe respect for human rights, but more detailed guidance in specific functional areas is necessary to give those commitments meaning.
>
> **Impact assessments**
>
> 61. Many corporate human rights issues arise because companies fail to consider the potential implications of their activities before they begin. Companies must take proactive steps to understand how existing and proposed activities may affect human rights. The scale of human rights impact assessments will depend on the industry and national and local context. While these assessments can be linked with other processes like risk assessments or environmental and social impact assessments, they should include explicit references to internationally recognized human rights. Based on the information uncovered, companies should refine their plans to address and avoid potential negative human rights impacts on an ongoing basis.
>
> **Integration**
>
> 62. The integration of human rights policies throughout a company may be the biggest challenge in fulfilling the corporate responsibility to respect. As is true for States, human rights considerations are often isolated within a company. That can lead to inconsistent or contradictory actions: product developers may not consider human rights implications; sales or procurement teams may not know the risks of entering into relationships with certain parties; and company lobbying may contradict commitments to human rights. Leadership from the top is essential to embed respect for human rights throughout a company, as is training to ensure consistency, as well as capacity to respond appropriately when unforeseen situations arise.
>
> **Tracking performance**
>
> 63. Monitoring and auditing processes permit a company to track ongoing developments. The procedures may vary across sectors and even among company departments, but regular updates of human rights impact and performance are crucial. Tracking generates information needed to create appropriate incentives and disincentives for employees and ensure continuous improvement. Confidential means to report non-compliance, such as hotlines, can also provide useful feedback."

Evaluating these due diligence requirements, they do not lead to additional recommendations for BCR other than those already made based on

evaluation of BCR against general accountability requirements (see *Recommendation 12*).

According to the UN Framework, companies further have to provide for **access to remedies**. In this respect the UN Framework explicitly notes that non-judicial mechanisms should be provided for by the company "as enforcement by traditional judicial means is not adequate for enforcement of CSR".[56]

> "84. For Non-judicial mechanisms play an important role alongside judicial processes. They may be particularly significant in a country where courts are unable, for whatever reason, to provide adequate and effective access to remedy. Yet they are also important in societies with well-functioning rule of law institutions, where they may provide a more immediate, accessible, affordable, and adaptable point of initial recourse."

The UN Framework further provides for criteria for such non-judicial mechanisms:

> "92. Non-judicial mechanisms to address alleged breaches of human rights standards should meet certain principles to be credible and effective. Based on a year of multi-stakeholder and bilateral consultations related to the mandate, the Special Representative believes that, at a minimum, such mechanisms must be:
> (a) Legitimate: a mechanism must have clear, transparent and sufficiently independent governance structures to ensure that no party to a particular grievance process can interfere with the fair conduct of that process;
> (b) Accessible: a mechanism must be publicized to those who may wish to access it and provide adequate assistance for aggrieved parties who may face barriers to access, including language, literacy, awareness, finance, distance, or fear of reprisal;
> (c) Predictable: a mechanism must provide a clear and known procedure with a time frame for each stage and clarity on the types of process and outcome it can (and cannot) offer, as well as a means of monitoring the implementation of any outcome;
> (d) Equitable: a mechanism must ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair and equitable terms;
> (e) Rights-compatible: a mechanism must ensure that its outcomes and remedies accord with internationally recognized human rights standards;
> (f) Transparent: a mechanism must provide sufficient transparency of process and outcome to meet the public interest concerns at stake and should presume

[56] Ruggie Report (Chapter 14, n 64) at para. 84.

> transparency wherever possible; non-State mechanisms in particular should be transparent about the receipt of complaints and the key elements of their outcomes."

Again, evaluating the dispute procedures of BCR, these seem to comply with the above criteria, but for the requirement of transparency of complaints made under these dispute procedures and their outcomes. The requirement on companies to report on their compliance with CSR was also already part of the first publications of the European Parliament on CSR.[57] These transparency requirements already resulted from the evaluation of BCR against general accountability requirements (Paragraph 13.5) and requirements of legitimacy (Paragraph 14.7.6) and will therefore not lead to a separate recommendation here.

Also, the UN Framework directs national governments (to the extent they have not done so yet) to ensure CSR norm-setting, enforcement and adequate remedies for individuals. Multinationals are therefore well advised to embark in a timely fashion on their "due diligence" in respect of data protection compliance as practice shows that implementation involves a time-intensive company-wide project, which requires the input and cooperation of nearly all business functions and suppliers of such company.[58] On the other hand, the BCR regime (as amended according to the *Recommendations*) may serve as a modern case study or even a template for the "due diligence" as envisaged by the UN Framework.

15.2.10 CSR and the trust game

Taking a momentary side step, but nonetheless interesting in this context, the recommendation for transparency about compliance is indicated also from the perspective of economic theory, especially game theory. Research on CSR from this perspective shows that a crucial part of effective CSR is the "reputation mechanism" which is the basis for the "trust game":[59]

---

57 European Parliament, Report on the Commission's Green Paper on Promoting a European Framework for Corporate Social Responsibility, A5-0159/2002 Final, at 18.

58 The implementation of BCR projects in most cases takes a period of at least two years.

59 Sacconi (Chapter 6, n 82), at 317. For a comprehensive description of the trust game, see Sacconi at 319 – 321. Simply put, the trust game evolves around transactions between a stakeholder and a company. The stakeholder has to decide whether or not to place trust in the firm, entering or not entering into an exchange relation with the firm. The firm then decides between abusing or not abusing the trust. If, after the stakeholder has entered, the firm does not abuse its trust, there will be a reasonably good outcome for both. However, if the stakeholder places trust in the firm, the latter has interest in abusing that trust, because in the short term

> "Reputation is one of the most valuable, albeit intangible, of the firm's assets. It is reputation that induces the stakeholders to trust the firm and consequently to cooperate with it, so that transactions come about at low costs of control or bargaining".

For the trust game to work:

> "principles and precautionary rules of behaviour must be communicated, given that reputation depends on them. The stakeholders base their judgements on the match among principles and rules announced ex ante, level of membership into the principles domain exhibited by any events [that] have occurred, and the behaviour adopted. Essential, therefore, is social accounting and reporting of the firm's performance in relation to the principles and norms announced."

This is not just a requirement for CSR codes to be effective. It may be elucidating for companies to realise that it is also in their interest to reap the benefits of this "trust game". To achieve this they will have to be transparent about their data protection compliance.

15.2.11 CSR of human rights

A final note is due on the topic of whether CSR codes are appropriate to regulate human rights. I have discussed TPR of human rights in Paragraph 14.5, where the conclusion was that TPR is not per se unsuitable to regulate human rights. Whether the relevant TPR is suitable will depend rather on how the TPR normative framework is set up. Given the general caveat for self- and co-regulation "when human rights are at stake" made by the EU

(for the relevant transaction) this will create the most remuneration. Consequently for the subsequent transaction, the stakeholder will not grant its trust and the transaction will not take place. The underlying idea of the game of reputation is that there is an alternative solution which permits the transactions between the two parties to take place, if the basic game is infinitely iterated and an incentive is thus created for the firm to protect its reputation. In the overall game there are an infinite series of stakeholders (each a short run player for just one game and deciding whether to enter or not) and the firm is the long-run player, lasting for all repetitions of the games. The firm's reputation is based on the probability assigned by each of the stakeholders that the firm will abuse or not abuse. The firm's reputation, whichever type it may be, increases as evidence is gathered that confirms it, but it diminishes dramatically if a single observation is made that falsifies the type. Short-run stakeholders will only decide to trust the firm after a series of non-abuses, as a result of which the expected utility of the entry decision is greater than non-entry. At this turning point, the firm may off-set the cost of its initial series of non-entries against subsequent entries.

institutions[60], it is not surprising that the view of the EU institutions **on CSR** also seems to be that these should not be based on voluntary guidelines and voluntary initiatives of multinationals.[61] Though the European Commission at an earlier time reported a "large consensus for voluntary CSR", this consensus already at the time did not include trade unions and civil society organisations that "emphasised that voluntary initiatives are not sufficient to protect workers' and citizens rights".[62] Also the Ruggie Report has made clear in many instances that "compliance efforts cannot succeed unless we bring governments back in the equation".[63] Based on the above, the general expectation is that EU regulatory action on CSR is imminent. If legislation on CSR is adopted, the question is whether this will make much difference for data protection obligations of multinationals and BCR. The answer is in all probability that this will make no difference. As indicated above, the Data Protection Directive (and non-EU data protection laws for that matter) are at present already directed at multinationals. Further, if *Recommendation 2* is indeed followed, the Data Protection Directive will provide for the required general framework legislation for BCR. Insofar as new CSR legislation were to be forthcoming containing obligations for multinationals in respect of CSR (including data protection), the expectation is that the BCR regime (as amended according to the Recommendations) will comply with any "due diligence" or other requirements under such CSR legislation. Even, such amended BCR regime may serve as a modern case study or template for such "due diligence" envisaged by the UN Framework.

---

60 White Paper on European Governance (Chapter 6, n 72), at 2; and the Inter-Institutional Agreement on 'Better Lawmaking' (Chapter 6, n 72), in particular Article 16.

61 The first to express this opinion was the European Parliament, in its Report on the Commission's Green Paper on Promoting a European Framework for Corporate Social Responsibility, A5-0159/2002 Final, at 18.

62 Communication from the Commission concerning CSR, COM (2002) 347, at 4.

63 See citation in McBarnet (Chapter 8, n 23), at 28.

16 Conclusions

BCR have come a long way. Initially multinationals put bottom-up pressure on the Working Party 29 and the individual DPAs to acknowledge their corporate privacy policies as an alternative legal tool for facilitating their intercompany transfers of personal data. Now the Working Party 29 and DPAs are proposing to use BCR as a general template for corporate data protection compliance programmes per se. Further, the parallel with CSR codes is compelling. CSR codes are also based on accountability. Though in principle companies are free to choose the manner in which they achieve CSR compliance, in the absence of a CSR code and a compliance program, non-compliance will in practice be a given. The same will apply if the accountability principle is also introduced for data protection. The conclusion is even justified that already at present soft law instruments regulating CSR require multinationals to include data protection commitments in their CSR codes as a consequence of which BCR are more or less indispensible to ensure accountability in this respect. This turns BCR from an alternative tool for data protection compliance into an indispensable tool for data protection for multinationals. In this light it is high time that the current uncertainties as to the validity and enforcement of BCR are solved (as per *Recommendations 2 & 9*), that the BCR authorisation procedure is streamlined (as per *Recommendation 4*) and that the enforcement powers of DPAs are harmonised and a common enforcement strategy for the DPAs is developed to ensure equal enforcement (as per *Recommendation 5)*. This should not be achieved by way of further opinions of the Working Party 29, but by a revision of the Data Protection Directive, which should preferably take the form of an EU regulation or, as the next best alternative, confer in the revised Directive the implementing powers in respect of such revised Directive on the Commission (as per *Recommendation 6*). In both cases EU legislators are advised to delegate in such EU regulation or revised Directive, the detailed norm-setting to the European Commission (as per *Recommendation 2*).

To ensure a wider uptake of BCR within the EU, European legislators are further advised to ensure that incentives are created for multinationals to adopt BCR (as per *Recommendation 14*). To further the recognition of BCR also in countries outside the EU for outbound data transfers form these countries, EU legislators are advised to engage with such countries to achieve mutual recognition and enforcement of BCR (as per *Recommendation 7*).

Multinationals introducing BCR have a strong interest in including a choice of law and forum clause in their BCR, as this will facilitate that all

complaints under the BCR are ultimately dealt with by the Lead DPA and the courts of the Lead DPA, as the provisions of the BCR are negotiated with this DPA under the applicability of the Lead DPA's own law (this being the law under which the provisions of the BCR were drafted). This ensures for the multinational a consistent and predictable interpretation and application of the BCR. For the same reason the multinational has an interest in the Lead DPA having central supervision over the BCR. This is also in the interest of the beneficiaries of the BCR. The conclusion of this study is that despite the fact that (i) the Data Protection Directive has a broad scope of application; (ii) individuals have broad legal rights and remedies under the Data Protection Directive; and (iii) DPAs have broad jurisdiction and enforcement powers, the current applicability and jurisdiction regime of the Data Protection Directive does not lead to data protection compliance in practice or meaningful redress for individuals. Even if the applicability and jurisdiction regime of the Data Protection Directive are harmonised and improved as per *Recommendations 1 -4* of Part I, this will not solve the cross-border enforcement issues encountered by individuals in this age of "big data". The BCR dispute procedure as backed up by central government enforcement by the DPA and courts of the Member State of origin of the multinational, provides individuals with a central facility where complaints and the many obstacles to cross-border enforcement of data protection by individuals will be addressed. The individual will be able to file a complaint in his own language, with the group company with which he has a relationship and this regardless of where the breach occurred or which of the group companies was responsible for the breach. The group company that receives the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and will ensure the required translations. If the complaints procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the Lead DPA or the courts of the Lead DPA. This procedure will lead to enforceable rights even if damages suffered by individuals are diffuse or too small to pursue through traditional judicial means, jurisdictions have no (adequate) data protection laws or if insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimises cost.

Given the uncertainties identified as to whether a valid choice of law and forum can be made in BCR for the laws and the courts of the Lead DPA, EU legislators are advised to ensure that such choices of law and forum may be made in BCR (as per *Recommendation 9*).

If European legislators were to (i) harmonise the applicability and enforcement regime of the Data Protection Directive (as per

Recommendations 1, 3 & 4 of Part I); and (ii) introduce the country-of-origin principle also for data protection (as per *Recommendation 2* of Part I and *Recommendation 1* of Part II), it would seem that the possibility of a choice of law and forum in BCR would no longer be necessary, as in that case (i) the data processing operations of the multinational would already be governed by (just) the data protection law of the Member State of origin of the multinational; and (ii) the DPAs and the courts of such Member State would already have central jurisdiction. Since the country-of-origin principle only applies to the extent the data processing operations of the multinational are governed by EU data protection law and since the BCR apply to the data processing operations of the multinational **worldwide**, the possibility of a choice of law and forum (and therefore *Recommendation 9*) remains relevant.

Is this then reason to drop *Recommendations 1-4* of Part I (i.e. to harmonise the applicability and enforcement regime of the Directive and to introduce the country-of-origin principle)? The answer is no, because without harmonisation and introduction of the country-of-origin principle, a choice of law and forum in BCR (leading to one applicable law and competent forum) would then be such a deviation from the situation without such choice (i.e. cumulation of applicable laws and concurrent jurisdiction of DPAs), that it is very unlikely that the proposal to allow such choice of law and forum in BCR would ever make the finish line.

Having embraced the introduction of the country-of-origin and in its wake having accepted that in BCR a choice of law and forum may be made, I recommended stretching the imagination yet one step further. A multinational having BCR will then have to comply with the data protection law of its Member State of origin only. Multinationals, however, would ultimately be best served if they could apply one uniform data processing regime on **a global basis**. In other words, they would be best served if they could apply the BCR regime on a global basis, **including in the EU** (as per *Recommendation 10*). This will further reduce the administrative burdens of multinationals as they will be able to apply the BCR regime also in the EU without the necessity of introducing additional EU-specific requirements.

To foster the acceptability of BCR on a global scale, the search for common reference points with other disciplines and perspectives has resulted in a number of common requirements across disciplines. A striking example is the requirement of transparency of compliance results. This led to *Recommendation 12* to impose on multinationals a reporting obligation on their data protection compliance in their annual report in a comparable

format. This transparency recommendation is based on the outcomes of an evaluation of the BCR regime from the:

(i) accountability perspective in general literature applicable to other fields of law;[1]
(ii) the introduction of the accountability principle for data protection;[2]
(iii) general policy research and literature in the area of consumer protection;[3]
(iv) general policy literature in the area of company law;[4]
(v) the law and economics approach;[5]
(vi) BCR as a form of TPR and legitimacy requirements in this respect;[6]
(vii) BCR as a form of CSR;[7]
(viii) economic policy theory.[8]

It is also true for most other recommendations that each is based on the outcomes of the evaluation from at least two of these disciplines (see overview below). Many of the recommendations further overlap with those made by the Rand Report, the Working Party 29, the European Data Protection Supervisor (**EDPS**), the Centre for Information Policy Leadership (**CIPL**) and the European Commission. The results thus combined may hopefully result in a better theoretical foundation for revision of the Data Protection Directive based on these Recommendations.

In summary my conclusions in respect of my research objective and hypotheses of Part I are that (see in detail Chapter 5):

(i) the applicability regime of the Data Protection Directive is presently not sufficiently harmonised and on the one hand leads to gaps in the protection and on the other hand to an arm's length scope with little hope of enforcement. If the applicability regime is harmonised and improved (as per *Recommendations 1 & 3* of Part I), these issues will no longer present themselves. If the country-of-origin principle is introduced (as per *Recommendation 2* of Part I), the unnecessary accumulation of applicable laws to data processing by controllers established in the EU will further be avoided; and

1 See para. 13.2.1
2 See para. 13.5.
3 See para. 8.4.2.
4 See para. 13.2.1.
5 See para. 13.2.1.
6 See para. 14.7.6.
7 See para. 15.2.9.
8 See para. 15.2.10.

(ii) (other than as assumed) the jurisdiction regime is presently not adequately harmonised. If the jurisdiction regime is harmonised (as per *Recommendation 4* of Part I), this will no longer pose a problem. If the applicability regime of the Data Protection Directive is amended (as per *Recommendations 1-3* of Part I), the jurisdiction regime does not lead to "exorbitant" jurisdiction. This being said, the jurisdiction regime does not provide for meaningful redress to individuals in practice.

Building on these conclusions in respect of Part I, my conclusions in respect of the hypotheses of Part II are as follows:

> ***Hypothesis 3***
> *BCR as an instance of TPR can do better than the present territory-based state regulation of data protection in terms of:*
> *(a) avoiding gaps in protection and enforcement as presented by the current patchwork of national data protection laws; and*
> *(b) regulating transborder data flows.*

Conclusion Hypothesis 3
My conclusion in respect of Hypothesis 3 is that even if the applicability and jurisdiction regime of the Data Protection Directive is harmonised and improved as per the *Recommendations 1 -4* of Part I, BCR as an instance of TPR can do better than the present territory-based state regulation as provided for by the Data Protection Directive in all three respects named (i) in providing data protection to individuals; (ii) in providing enforcement to individuals; and (iii) in regulating transborder data flows.

Re (i) avoiding gaps in data protection
If BCR have indeed a global scope (as per *Recommendation 19*), data protection is also provided to data processed by the multinational in countries where no or less data protection is provided for by state laws. Thus gaps in data protection left by the regulation of nation states are no longer relevant.

Re (ii) avoiding gaps in enforcement
If a choice of law and forum may indeed be validly made in BCR (as per *Recommendation 8*), and beneficiaries of BCR may indeed enforce their rights as unilateral undertakings under BCR (as per *Recommendation 9*) BCR will provide for better enforcement of data protection by individuals in practice. Individuals are provided with a central facility for complaints and the many obstacles to cross-border enforcement of data protection by individuals will be addressed. The individual will be able to file a complaint

in his own language, with the group company with which he has a relationship and this regardless of where the breach occurred or which of the group companies was responsible for the breach. The group company that receives the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and will ensure the required translations. If the complaints procedure does not lead to a satisfactory result for the individual, the group company will facilitate the filing of the complaint with the Lead DPA or the courts of the Lead DPA. This procedure will lead to enforceable rights even if damages of individuals are diffuse or too small to pursue through traditional judicial means, jurisdictions have no (adequate) data protection laws or if insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimises cost. These are all issues that presently constitute obstacles to the cross-border enforcement of data protection rights.

Re (iii) improved regulation of transborder data flows
BCR result in lower administrative burdens for multinationals while at the same time providing more material data protection and redress in practice to individuals. This is a vast improvement to the situation where transborder data flows within multinationals are regulated by means of the EU Standard Contractual Clauses, which leads to high administrative burdens for multinationals, while at the same time the broad contractual data protection rights and remedies of individuals do not lead to meaningful data protection and redress in practice. If the BCR regime defines the core accountability principles for the situation when a multinational transfers personal data to third parties (as per *Recommendation 14*), the same will apply in the case of data transfers by the multinational to a third party outside its group of companies.

> ***Hypothesis 4***
> *The BCR regime as currently developed by the Working Party 29 does not sufficiently incorporate or is not sufficiently aligned with principles of international private law, best practices when implementing the principle of accountability, generally accepted legitimacy demands made of TPR, and best practices as to CSR, in order for BCR to be acceptable on a global basis as a form of TPR to regulate global corporate conduct in the area of data protection*

Conclusion Hypothesis 4
My conclusion is that the BCR regime is indeed at present not sufficiently aligned with principles of PIL, best practices when implementing the principle of accountability, generally accepted legitimacy demands made of

TPR, and best practices as to CSR. If *Recommendations 12 - 18* are followed, BCR will be better positioned to be globally acceptable as a form of TPR to regulate global corporate conduct in the area of data protection.

17 Summary

The digital era shows an unprecedented continuous worldwide flow of data both within multinational companies as well as with their external service providers. While large corporations operate internationally, state governments legislate nationally. Besides leaving gaps in the patchwork of national data protection regulations, this situation also leads to overlaps in applicable national rules that often deviate or outright conflict. These conflicts make it impossible for multinational corporations to comply fully and consistently as to their many forms of cross-border data processing. Further, the traditional territory-based enforcement tools are not adequate for states to force compliance. This legal landscape provides a challenging background to test whether transnational private regulation of data protection can provide solutions where legislation fails to.

Introduction: the global data protection regulatory landscape

In the digital age, data protection is of increasing concern for governments, individuals and companies alike. While many multinational companies fully act on a seamless worldwide basis, states remain bound to their respective territories. The maturing of the internet especially led to a vast increase in cross-border flows of personal data both within and between groups of companies. Though all countries face essentially the same dilemma of how to regulate these vast flows of personal information, their governments have chosen substantially different solutions. Within the European Union (**EU**), the protection of individuals prevails, and the rights of individuals in respect of the processing of their personal data became a fundamental right and freedom. The desire to avoid gaps in the protection of personal data and to prevent circumvention of the Data Protection Directive led EU legislators to provide for a very broad scope of applicability of the Data Protection Directive ("long arm reach"). The wish to regulate the outbound European data streams as well, resulted in another "long arm" provision in the Data Protection Directive, where it prohibited data transfers to countries outside the EU without an adequate level of data protection. This extraterritorial provision prompted many countries outside the EU to follow suit in adopting comprehensive data protection legislation to secure that their multinational companies kept access to the EU market. These states also struggled to regulate their outbound transnational data streams which resulted in many states adopting equally "long arm reach" data protection laws and multiple instances of "overregulation" (i.e. where rules are made so

generally applicable that they apply prima facie to processing of personal data of their nationals wherever processed around the world). In addition, many of these countries have imposed restrictions on the outbound transfer of personal data from their respective countries. Such outbound data transfer requirements are considered necessary by most countries as there are still many countries with no data protection laws at all as well as countries (most notably the US) with a limited regime, which mostly focus on the public sector and certain sensitive industries (most notably healthcare and telecommunications). As a consequence, the worldwide data protection regulatory landscape presently consists of at best a patchwork of very diverse national data protection laws, which laws often deviate or even outright conflict.

A specific challenge for data protection regulators across the world is posed by the fact that enforcement of data protection legislation is based on a jurisdictional approach. In the international environment, this leads to many long arm reach data protection laws having no hope of enforcement in practice if the relevant company or data processing operation is not established in the relevant jurisdiction also. Further, the concepts of applicable law and jurisdiction are embedded in a long tradition of international private law, where laws that over-extend their jurisdictional reach are considered an unacceptable form of 'hyper-regulation' if they apply so indiscriminately, that there is no hope of enforcement. The applicability and jurisdiction regime of data protection laws is therefore inherently delineated and cannot be looked to for solving the present gaps in the protection of personal data and the enforcement thereof.

At present, countries that have a data protection supervisory authority aim to solve the cross-border enforcement issues by a "network approach", where data protection supervisory authorities of different jurisdictions cooperate in the event of cross-border violations. Until all jurisdictions have adequate data protection laws and supervision thereof, this network approach cannot adequately solve the enforcement issues presently faced by data protection regulators. Though there is a persistent call for a legally binding global standard for data protection, and there are some concrete initiatives in this respect, it is not expected that a global standard will be realised within the coming 10 years. The present regulatory landscape is still too diverse for such a standard to be acceptable for adoption on a global level. In any event, the adoption of a global standard should not be taken as the holy grail for all international jurisdiction and enforcement issues as presently seen in the data protection field. Even if global standards exist, differences in enforcement between countries will remain as, in practice, regulatory enforcement at the national level proves patchy, whether because

of lack of resources or the prioritisation by national governments of national commercial or other interests above regulatory enforcement. Solutions may therefore only be forthcoming if some form of central enforcement is implemented by, for instance, the supervisory authorities and courts of the company headquarters.

From the perspective of individuals whose data are processed, the present jurisdictional approach also does not provide effective protection. This is not always for a lack of rights and remedies of individuals. For instance, the Data Protection Directive provides for broad remedies and liabilities and, in principle, allows individuals ample opportunity to ensure that a breach is remedied and compensation is obtained. Due to the networked economy, however, even relatively simple breaches of data protection present complicated cross-border jurisdictional and enforcement issues. It is often not viable in practice for individuals to effectuate these rights and remedies through traditional judicial means (or via a complaint with a foreign supervisory authority). The main reason being that Data protection breaches in most cases involve no (or relatively small levels of) economic damages for individuals, making it too costly to pursue a claim or complaint.

At first glance the absence of effective enforcement of data protection may seem to be to the advantage of multinationals processing data, who can avoid potential liabilities. This is, however, not per definition the case. Rather, there are compelling reasons for multinationals to implement their own global privacy policies to be able to ensure (to a certain extent) uniform data processing rules throughout their organisation and to ensure central supervision and enforcement in respect thereof, preferably by the supervisory authority and the courts of its headquarters. This would avoid the present patchwork of local and cross-border privacy rules and jurisdiction of supervisory authorities and courts in about as many as 60 different jurisdictions in the world.

Part I
Assessment of the applicability and jurisdiction regime of the Data Protection Directive

In Part I of this dissertation, I discuss current applicable law and jurisdiction rules of the Data Protection Directive, and evaluate whether these are still appropriate in light of the present seamless technical landscape and the worldwide data protection regulatory landscape as it exists today. In summary, my conclusions are that the applicability regime of the Data Protection Directive is presently (i) not sufficiently harmonised; (ii) leads to unnecessary cumulation of applicable laws; (iii) leads to gaps in the

protection; and (iv) in certain cases leads to an arm's length scope with no hope of enforcement and which may qualify as "overregulation". Based on these findings, I make recommendations on how to harmonise and improve the applicability regime. In particular, in order to avoid the current unnecessary cumulation of applicable data protection laws to data processing by controllers established in the EU, I propose introducing a country-of-origin principle for EU data protection law as well.

Introduction of the country-of-origin principle

According to the country-of-origin principle, each Member State applies its own law to data processing by data controllers who are "established" in their territory (i.e. such data processing is governed by the law of their "country-of-origin"). What is relevant here is that application of the country-of-origin principle results in no more than one place of establishment of the controller in respect of the data processing operations of the involved. For instance, if a multinational has more group companies that are all involved in the data processing operations of the group, the country-of-origin principle entails that one law applies to all data processing activities of a multinational which are covered by the Data Protection Directive. This would preferably be the law of the multinational's EU headquarters (the company having control in the EU of all data processing operations of such multinational).

As a consequence, the data protection authority (**DPA**) of such EU headquarters will have central supervision powers, and the DPAs of the other Member States must assist the DPA in the country-of origin. This is a form of integral enforcement which requires that the DPA of the country-of-origin has supervisory powers to the detriment of other DPAs (i.e. such other DPAs will have to relinquish their supervisory powers as to the secondary establishments in their respective territories). In return, such other DPAs obtain central enforcement in respect of the processing activities of multinationals with primary establishment in their territories.

Introduction of the country-of-origin principle will, however, be only a partial solution. Even if introduction of the country-of-origin principle were forthcoming at the EU level, it is not expected that this will be feasible on a truly international scale. Further, the country-of-origin principle addresses some, but not all, obstacles presently encountered by individuals in effectuating their rights and remedies. These issues show many parallels with the issues encountered by consumers in enforcing their consumer protection rights: often the damages involved are too small to justify court action or a complaint with a supervisory authority. In cross-border cases, language and time zone issues prove to be additional obstacles. Also, based on the research in the consumer protection area, my conclusion is that in the

area of data protection, the traditional forms of private enforcement (i.e. by individuals through judicial means) complemented by governmental enforcement by supervisory authorities (i.e. the DPAs) are inadequate to force data protection compliance. More creativity is required, and my research into the general literature in both the international ICT and consumer protection area points in the direction that this is best achieved by self-regulation backed up by governmental enforcement. The underlying assumption is that by transnational self-regulation, uniform rules can be imposed on multinationals that operate on a cross-border basis. A choice of law and forum in such self-regulation would make it possible for such companies to have their operations governed by one uniform regime and to have their self-regulation supervised and enforced by the supervisory authority and the courts of one country only, preferably the headquarters of such multinational. If this form of central enforcement is at the same time accompanied by an obligation of the multinational to implement an internal complaints procedure and to facilitate cross-border enforcement within their group of companies, the beneficiaries of the transnational self-regulation would also be better off. For instance, if a data protection breach occurs, the individual affected will then be able to file a complaint with the group company with which he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The individual will therefore not have to prove which of the group companies was at fault (which is currently one of the obstacles to bringing and succeeding in a claim). There is also no issue as to which law applies and whether the relevant law provides for data protection. Also, if the country of the individual does not provide for data protection at all, the transnational self-regulation will apply. The complaint may be filed by the individual in his own language. The group company that received the complaint will be responsible for ensuring that the complaint is processed through the complaints' procedure of the multinational, and for ensuring that the required translations are provided. If the complaints' procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the lead DPA or the courts of the lead DPA. This procedure will lead to enforceable rights even in jurisdictions where no (adequate) data protection laws are in place or where insufficient enforcement (infrastructure) is available. It further overcomes language issues, time zone obstacles and minimises costs.

The question of whether any gaps and deficiencies in the present applicability and jurisdiction regime of the Data Protection Directive may be addressed by transnational self-regulation backed up by governmental enforcement is addressed in Part II of this study. Before addressing this issue, I will first give a short introduction on a specific form of corporate

transnational self-regulation as presently developed by multinationals in the area of data protection, as well as the relevance thereof in the global context.

Part II: Binding Corporate Rules

Introduction of transnational self-regulation in the area of data protection
Multinationals process personal data as a course of business. Employee data are processed, for instance, for purposes of execution of the employment agreement (salary payment, performance evaluation, succession planning). Multinationals selling consumer products further process the personal data of their customers. Specific industries, like the pharmaceutical sector, may process specific categories of personal data, for instance, in the course of performing scientific research involving patients. Due to the globalisation of the activities of these multinationals, these data are not relevant to one group company only (for instance, the group company employing the relevant employee), but are relevant to many other group companies. Examples include performance evaluations and succession planning. Most multinationals have matrix organisations, which means that their business is managed not so much on a country-by-country basis but per business unit, which may extend over many countries. Group companies therefore exchange employee and customer data as a course of business. Another development is that the transfers are no longer point-to-point but between multiple computers communicating through a network or the internet. Multinationals have started to integrate their various local IT systems and to process their employee and customer data in central IT systems, which entails a continuous worldwide transfer of data between their group companies. These central IT systems are subsequently outsourced to third-party service providers. For cost reasons these service providers often provide their services from offshore locations outside the EU. Such offshoring involves a transfer of the data at the multinational to all service centres of the outsourcing supplier in the countries involved.

These data transfers between group companies and the offshoring by multinationals of their data processing operations to third countries attracts a multitude of applicable data protection laws. The existing overlap and conflicts in applicable data protection laws makes 100% worldwide compliance by multinationals a practical impossibility. Compliance would require multinationals not only to track and comply with the material data protection rules of each jurisdiction, but also to track and comply with all requirements relating to data transfers between specific countries. Further, multinational companies largely ignore the EU (and other countries') data transfer rules as these lead to disproportionate administrative burdens and provide little additional material protection for individuals. Practice shows

that multinationals, rather than striving to comply with applicable national data protection laws on a country-by-country basis, implement worldwide self-regulation by introducing corporate privacy policies. Their corporate privacy policies provide for both company-wide data protection rules and for an adequate level of data protection throughout the group, and ignore possible stricter national provisions. The foregoing significantly affects the capacity of national (and especially EU) regulators to force compliance by multinationals in the area of data protection. The introduction of corporate privacy policies by multinationals has created bottom-up pressure on national legal orders. This is reflected in the number of beneficiaries who invoke these policies before national courts (so far mainly in the US). It is also reflected in the pressure exerted by multinationals on the EU DPAs to recognise their corporate privacy policies as a tool to comply with the EU data transfer rules (as their policies ensure an adequate level of protection of personal data when transferred throughout their group of companies). The advisory committee to the European Commission on data protection (**Working Party 29**)[1] recognises the added value of transnational private regulation in the data protection area in light of the gaps and deficiencies of the present EU data transfer regime. In a series of opinions, the Working Party 29 set criteria for these corporate privacy policies to provide for a minimum level of protection for the processing of data by a multinational on a worldwide basis. These policies should (inter alia):

(i) be **internally** binding within the organisation (on all group companies and on employees) and **externally** binding for the benefit of the beneficiaries of the privacy policy (i.e. must create third-party beneficiary rights for these individuals);

(ii) incorporate the material data processing principles of the Data Protection Directive and the restrictions on onward transfers to third parties outside the group;

(iii) provide for a network of privacy officers for ensuring compliance with the rules;

(iv) provide for an internal complaint handling process;

(v) provide for an auditing programme covering all aspects of the corporate privacy policy;

[1] The Working Party 29 was established as an advisory body to the European Commission under Article 29 of the Data Protection Directive. The Working Party 29 has advisory status only and acts independently. Members are representatives of each of the DPAs, of the European Data Protection Supervisor and of the European Commission. Though the opinions of the Working Party 29 are non-binding, they are often followed in practice by the DPAs and as such, often de facto set the rules for application of the Data Protection Directive. The DPAs are, however, not obliged to do so and on specific topics (in particular on BCR) some DPAs follow their own course.

(vi) ensure suitable training of the employees who process the data;
(vii) be enforceable by the beneficiaries of the corporate privacy policy (i.e. the employees and consumers) via the DPA and the courts in the Member State of EU headquarters of the multinational;
(viii) the EU headquarters should accept liability for paying compensation and remedying breaches of the corporate privacy policy; and
(ix) group companies should have a duty to cooperate with the DPAs, to abide by their advice regarding the corporate privacy policy and to submit to their audits.

To express the binding character of these corporate privacy policies, the Working Party 29 has labelled these "Binding Corporate Rules" (**BCR**). With BCR, the Working Party 29 introduced a complex hybrid system of self-regulation (corporate privacy policies) with public arrangements (the DPAs validating such corporate privacy policies and providing support in the area of supervision and enforcement).

Despite the opinions issued by the Working Party 29 on the concept of BCR, some DPAs still do not agree to these requirements and refuse to recognise BCR as a valid tool for inter-company data transfers. Uncertainty also exists as to whether BCR will be accepted as a valid tool for data transfers by non-EU jurisdictions that have their own data transfer restrictions. As a consequence, it remains uncertain whether the BCR concept will work on an EU-wide basis, let alone at a global level, and the timeframe within which this may be ultimately achieved. The Working Party 29 acknowledges the shortcomings of the present BCR regime and has advised the European Commission to address these in the upcoming revision of the Data Protection Directive, which was launched by the European Commission on 1 July 2009. Subsequently, the European Commission announced that it will indeed improve and streamline the BCR regime.

For a number of reasons the introduction of the BCR regime is an important development in the global data protection arena and is expected to gain further relevance in the coming years.

- The expectation is that increasingly more countries will introduce data protection legislation, which in most cases will also include outbound data transfer rules. As it is not expected that a global standard will be realised in the near future, data transfer instruments such as BCR are therefore expected to gain importance as instruments in facilitating cross-border data transfers.
- Governments choose very different approaches to data transfer rules. For instance the EU transfer rules are **territory-based** rules

(i.e. the main rule is that data transfers are allowed to adequate countries only) and the APEC rules are **organisation-based** rules (i.e. data may be transferred by an organisation to another organisation if it has put appropriate contractual safeguards in place). However, the Data Protection Directive also facilitates "organisation-based" data transfer tools that legitimise data transfers between organisations, such as the EC Standard Contractual Clauses and now the BCR regime. The APEC Privacy Framework also facilitates a similar organisational tool, where it encourages organisations to adopt "Cross Border Privacy Rules" (**CBPR**) as a manner to facilitate their cross-border data transfers. Though it is expected that the EU and APEC systems of data transfer rules will further converge, it is clear that in the near future, BCR and CBPR will be an important common factor of the two systems. BCR will thus fulfil a bridging function between the two systems, facilitating international data transfers even where (in this case) the EU and the APEC Member Economies cannot agree on what the appropriate universal level of data protection should be.

- In some areas of law (notably the financial services field) legislators have introduced the "principle of accountability" in respect of compliance with the relevant legal requirements. The main purpose of "accountability" is to use the law to hold businesses accountable for taking their responsibilities seriously by using various mechanisms to encourage or force businesses to put internal governance structures and management systems in place. The expectation is that the accountability principle will also be introduced into the revised Data Protection Directive. This will entail that in addition to the obligation to comply with the EU data protection requirements, an independent obligation will be introduced to implement a proper data protection compliance program. The principle of accountability is not new in the field of data protection and has from the start been one of the main principles in the OECD Privacy Guidelines and the APEC Privacy Framework. Also, in the opinion of the Working Party 29, the BCR regime is a prime example of such corporate data protection compliance program. BCR are therewith (again) a common factor between the systems of the EU and the APEC Member Economies.
- As discussed, the applicability and enforcement regimes are inherently delineated and cannot be instrumental in filling in the gaps in the cross-border protection of personal data and the enforcement thereof. A solution may be that in BCR a choice of law and forum is made which would make it possible for multinationals to have their data processing operations governed by one uniform

regime, and to have their BCR supervised and enforced by one "lead" DPA and the courts of this DPA only preferably, the place of establishment of the headquarters of such multinational. BCR may thus function as a private regulatory response to the inherent limitations of rules on applicable law and jurisdiction.

- The application of BCR by multinationals to group companies in countries where no (or less) data protection exists may provide an important example function in those countries, as their nationals also benefit from this protection. Though no hard research has been carried out in this respect, in general transnational private regulation that is based on non-binding "soft law" is often a stepping stone to hard law.
- Many multinationals voluntarily adopt "Corporate Social Responsibility" (**CSR**) codes to overcome differences in regulations and regulatory approaches between countries and as part of their global reputation management. Typically, CSR codes involve a commitment by multinationals (usually in their Code of Ethics or Business Principles) to respect human and civil rights, to protect the environment, to oppose bribery and corruption and to commit to fairness to their customers and suppliers. The range of issues brought under the umbrella of CSR is constantly expanding and often now also includes a commitment to protect the privacy of employees and customers. The parallel between BCR and CSR codes is compelling. CSR compliance is based on accountability. Though in principle companies are free to choose the manner in which they achieve CSR compliance, in the absence of a CSR code and a CSR compliance program, non-compliance will in practice be a given. Various international non-governmental and intergovernmental organisations have issued international instruments with guidelines for CSR codes (so-called soft law). These soft law instruments regulating CSR require multinationals to include data protection commitments in their CSR codes. The consequence of this is that BCR are more or less indispensible to ensure accountability in this respect. This turns BCR from an alternative tool for data protection compliance into an indispensable tool for data protection for multinationals.

In light of the above, I evaluate the BCR regime as introduced by the Working Party 29 in more detail in order to determine whether this transnational self- regulatory tool is indeed suitable to regulate data protection, being one of the fundamental rights and freedoms of EU nationals.

The quest for meta-rules for BCR

As transnational self-regulation operates in a plurality of public and private orders and with a plurality of actors, such self-regulation has to function within many different spheres. For transnational self-regulation to be acceptable, existing research suggests it has to "construct relationships of recognition with the different public and private orders it comes into contact with." Also, BCR have to operate within many different spheres: the national jurisdiction where the multinational has its primary establishment, the national jurisdictions where the multinational has secondary establishments, the contractual relationships the multinational has with its employees, its customers, its suppliers, its sub-contractors and further the many supra-national regulatory spheres (at the EU, APEC, global level, etc). For BCR to be acceptable in all of the different public and private spheres it touches upon, it must be aligned with the existing legal disciplines and the other "bodies of thought" it interacts with. The main discipline BCR touches upon is that of private international law (**PIL**). As one author puts it, PIL is the "queen mother of all transnational legal thought". The interaction with PIL is twofold. First, there is the traditional function of PIL where, for instance, a choice of law and forum made in BCR has to comply with rules of PIL. BCR raise several questions of PIL if the beneficiaries are employees and consumers. The European rules of PIL, for instance, entail that a choice of law and forum in BCR may not affect the substantive rights and remedies or the dispute settlement procedures which are available to EU employees or EU consumers. This is also called the function of PIL as a "mechanism" or the "touch down" function. Due to these rules of PIL, state law becomes relevant, again, as a choice of law and forum leads to the competence of the courts and questions arise as to enforcement of judgments of such courts. A second legal discipline BCR touch upon is the rules of international contract law. BCR raise questions of enforceability by the beneficiaries thereof. BCR are further, to a certain extent, effectuated through contractual "supply chain management" as the BCR require that the multinational impose the BCR requirements on any third parties it transfers personal data to in the course of its business. Supply chain management also raises issues of enforceability by the beneficiaries of these contracts.

Next to the "touch down" function of PIL and international contract law, these legal disciplines (and other bodies of thought BCR interacts with) also potentially provide a source of "meta-norms" for BCR. "Meta-norms", have been labelled as "norms to which parties can commit without betraying their loyalty to their own legal systems". BCR will also have to accommodate this duality. Multinationals implementing BCR cannot ignore the national rules of the jurisdictions in which they operate, but they also have to operate on a global level which sets its own demands. For BCR (operating at the global

level) to be acceptable at the national level, BCR will have to "build on the assumption of common reference points" between national jurisdictions and different disciplines. Sidelining, for instance, the underlying policy choices behind PIL instruments (especially in relation to exceptions to the main principle of choice of law and forum) will not achieve universal acceptance of BCR.

The quest for the universality of BCR seems a bit daunting, but a first attempt at identifying common reference points (meta-norms) for BCR is undertaken in this dissertation by evaluating the concept of BCR as a form of meta-regulation from the disciplines of PIL and international contract law and further:

- BCR and the accountability principle
  The regulatory initiatives to achieve accountability of organisations are often called "meta-regulation", i.e. the regulation of private self-regulation. The main purpose of "accountability" is to use the law to hold businesses accountable for taking their responsibilities seriously by using various mechanisms to encourage or force business to put internal governance structures and management systems in place.
  One aspect of this meta-regulation, is how regulators can best provide companies with incentives and tools to use their own inherent 'regulatory capacities'. The BCR regime is evaluated against:
    - the general body of research in respect of the principle of accountability as introduced in other fields of law;
    - the proposal of the Working Party 29 on the accountability principle; and
    - other data protection legislation that incorporates the accountability principle.

- BCR as a form of transnational private regulation
  Another aspect of meta-regulation relates to the **optimal form** of meta-regulation to choose from. The discipline of how to best regulate (the rules for rule-making, the search for meta-norms) has in the EU become known under the label "Better Regulation" (**BR**). Legislators (including the European Commission) that wish to regulate global corporate conduct opt for "regulating" transnational private regulation (**TPR**) rather than introducing public regulation with its inherent limitations as to jurisdictional and authoritative

scope of state competence. In the substantial body of research concerning the concept of TPR, questions are raised as to:

- the suitability of TPR to regulate human rights;
- how to best regulate TPR (i.e. which of the forms of regulation would be most suitable to regulate TPR);
- the legitimacy of TPR as compared to public regulation.

- BCR in the context of Corporate Social Responsibility
  Various topics concerning CSR are also of relevance to BCR. In the substantial body of research concerning CSR, similar issues are raised as set out above in respect of TPR, such as the suitability of CSR to regulate human rights and legitimacy issues. Additional issues that are raised which equally apply to BCR are:

  - Various international non-governmental and intergovernmental organisations have issued instruments with guidelines for CSR codes (so-called soft law). Relevant for BCR is to what extent the right to data protection of a company's stakeholders is covered by these soft law instruments and whether this has any repercussions for the BCR regime as it presently stands;
  - CSR codes are voluntarily unilateral undertakings, but global legal practice shows how the law is being used to hold multinationals legally accountable for application of their CSR codes, which is of relevance to BCR as well.

Perhaps not so surprisingly, the evaluation of the above disciplines will show many common denominators across the disciplines. Though at present there are no hard and fast rules against which TPR (let alone BCR) should be evaluated. I take such common denominators of the different disciplines as meta-norms for evaluating BCR. On this basis, I make suggestions for improving the BCR regime, as well as provide suggestions on how to fit the BCR concept into the regulatory data protection regimes of other countries or regions like the APEC Privacy Framework. The objective is to demonstrate that BCR can be accepted as a mainstream global solution to regulate global corporate conduct in the area of data protection, also in countries where at present no (or insufficient) data protection is afforded. BCR may then indeed provide a solution to avoid the present gaps in

protection and enforcement as presented by the current patchwork of national data protection laws.

Summary conclusions Part II

BCR and rules of private international law

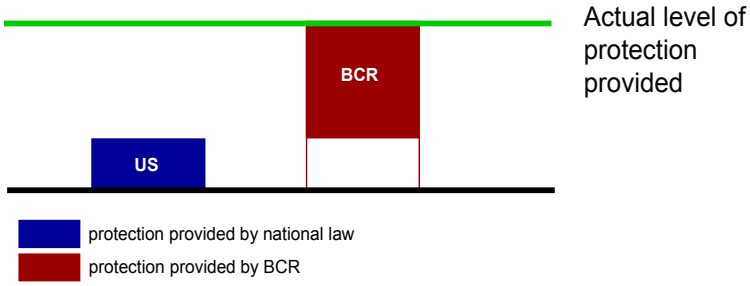
The Opinions of the Working Party 29 on BCR seem to be based on the assumption that BCR should provide for a **minimum level of protection** for the processing of personal data by the multinational, setting aside the national data protection laws at least to the relevant minimum level. Further, the WP Opinions require that BCR provide for the possibility of enforcement of BCR via the forum of either (i) the EU group company at the origin of the transfer or (ii) the EU headquarters of the multinational, therewith setting aside the jurisdiction that the courts of other Member States may have under applicable rules of PIL. These requirements of the Working Party 29 pose problems with (i) the mandatory nature of the applicability and enforcement regime of the Data Protection Directive and (ii) the EU rules of PIL (and also non-EU rules of PIL for that matter). As to rules of PIL, an additional problem is posed by the fact that the main personal data processed by multinationals under BCR concern personal data of their employees and those of their customers, who are in many cases consumers. As far as employee and consumer contracts are concerned, the rules of PIL create a mandatory regime – both in terms of applicable substantive law and in terms of dispute resolution mechanisms – which may not be set aside to the detriment of the employee or the consumer by a choice of law or forum. Similar issues under PIL are posed by the fact that multinationals introducing BCR have a strong interest in including a choice of law and forum clause in their BCR. Again, as under the BCR, mainly employee and consumer data are processed. This poses problems as to (i) the mandatory nature of the applicability and enforcement regime of the Data Protection Directive and (ii) EU rules of PIL.

The conclusion of my research is that at this time it is uncertain whether a choice of law and forum may be made in BCR. Multinationals are therefore currently best advised to set up the applicability and enforcement regime of BCR in such a manner that the pitfalls of deviation from the mandatory applicability and enforcement regime of the Data Protection Directive and the consumer and employee protection regime of PIL are avoided. This can be done by ensuring that BCR do not provide for a **minimum** protection where the applicable national data protection rules apply only if they provide for **more data protection,** but rather the reverse. The BCR should provide that any processing by the multinational of personal data will remain governed by applicable national law and that the BCR provide for

supplemental protection only. In other words, the BCR apply only if the BCR contain rights or remedies that go beyond those provided by applicable national law. If rights and remedies are equal under national law and the BCR, national law prevails. The BCR therewith does not provide for a minimum protection, but provides a "top on" protection until an adequate level of data protection is achieved. The scope of applicability of BCR is illustrated by the following examples.

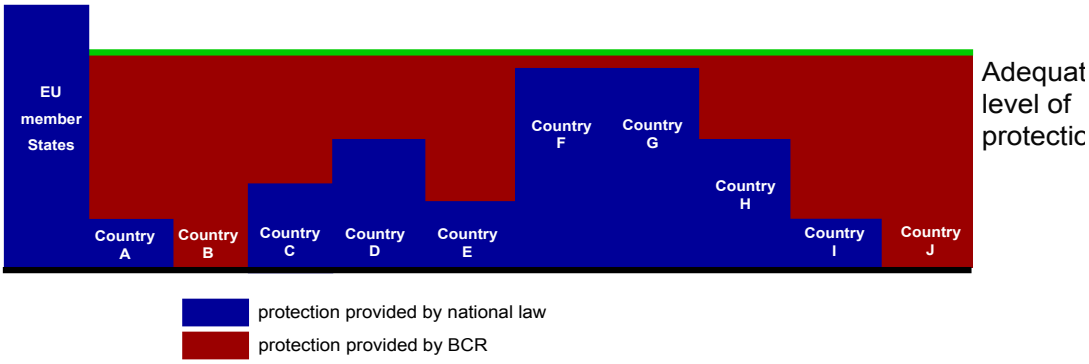
Example 2

- National law provides some protection, BCR provide supplemental protection (e.g. in the US)



Example 4

- BCR provide a 'top on' or 'blanket of protection' to ensure an adequate level



By setting up the BCR in this manner, the choice of law and forum in BCR relate to the **supplemental** protection provided by the BCR only. Such choice of law and forum thus do not contravene the mandatory nature of the protection provided by the Data Protection Directive and the consumer and employee protection regime of PIL (i.e. such choice does not take away any rights and remedies individuals may have under their national law, but adds to such rights and remedies only).
It may be argued that such system of providing supplemental protection may in turn pose problems for individuals, requiring them to specify which data protection rights are governed by their national law (and have to be brought before their own court) and which by the BCR (and have to be brought before the DPA and the courts of the EU corporate headquarters of the company). Though this seems a valid point, in practice this does not seem to pose problems. Apparently the benefits for individuals provided by the internal complaints procedure in BCR (backed up by the Lead DPA and its courts) demonstrate that individuals prefer to follow this procedure instead of addressing their own court under their national law. As following this procedure is also the preference of the multinationals, multinationals do not contest this choice. If a defendant (i.e the multinational) voluntarily appears before a DPA or in court, rules of PIL subsequently lead to jurisdiction of the court.

However, even if BCR are drafted as recommended and provide for supplemental protection only, my research shows that PIL issues may still arise, especially in relation to requirements as to **form** in which a choice of law and forum clause in BCR are made. This is the case despite the fact that such choice of law and forum is not contrary to the underlying policy choices of the consumer, and the employee protection regimes of PIL. To the contrary, such choice of law and forum will drastically improve the data protection and the access to remedies for individuals covered by the BCR. Based on this I recommend that in the revised Directive, European legislators enact that a valid choice of law and forum may be made in BCR.

Having embraced the introduction of the country-of-origin principle, and in its wake having accepted that in BCR a choice of law and forum may be made, I recommend stretching the imagination yet one step further. A multinational having BCR will then have to comply with the data protection law of its Member State of origin only. Multinationals, however, would ultimately be best served if they could apply one uniform data processing regime on **a global basis**. In other words, they would be best served if they could apply the BCR regime on a global basis, **including in the EU**. This will further reduce the administrative burdens of multinationals as they will

be able to apply the BCR regime also in the EU without the necessity of introducing additional EU-specific requirements.

BCR and contract law

The first requirement set by the Working Party 29 in respect of BCR is that the BCR should be "internally binding" within the organisation (on all group companies and on employees) and "externally binding" for the benefit of individuals (i.e. must create third-party beneficiary rights for the individuals). The first requirement can be met by having intra-corporate agreements in place, and employment agreements which bind employees. The second requirement may however pose problems. BCR are in principle a unilateral undertaking by the multinational and not a contract. Most, but not all, Member States seem to take the view that rights may be granted to third parties by means of unilateral undertakings. However, even if certain jurisdictions do not consider unilateral undertakings to have a binding effect, such legal orders, to varying extents, recognise the protection of reliance on promises. Where in a business context one party makes a promise which induces reliance by another party, such other party must be protected by law. An important parallel here is the enforcement of unilateral undertakings made by companies in their CSR codes. For a long time, many corporations and lawyers thought these promises constituted moral obligations at best, but which had no legal effect. However, by now in many jurisdictions creative legal bases have been developed to enforce CSR codes against the parent company for human rights violations by their group companies or manufacturers in developing countries. In the literature regarding CSR and TPR, authors comment that the conventional principles of contract law are not adequate to cater for enforceability of TPR by the beneficiaries of TPR, and that the law needs to be reformed to accommodate this. As such, general reform of the law to facilitate enforcement by third-party beneficiaries of unilateral undertakings (like BCR) is outside the scope of my research. Thus, I have limited my recommendation to EU legislators to provide that BCR can be enforced as unilateral undertakings by the beneficiaries of BCR. This recommendation is of paramount importance as the enforceability of BCR will be shown to be a requirement under all disciplines against which BCR will be evaluated in this dissertation, i.e. these all require that the BCR provide for "sufficient possibilities of redress for the beneficiaries". Though enforceability of BCR may be achieved by putting a contractual framework around BCR, this however results in unnecessary administrative burdens, with no additional benefit. The enforceability of BCR as unilateral undertaking is therefore the preferred form of redress.

Similar limitations under contract law are presented when TPR are imposed by a party on other parties in the supply chain, through contractual

provisions in their supply chain contracts. To a certain extent the BCR regime also relies on supply chain management to ensure protection of the employee and consumer data governed by the BCR. In the general literature regarding contractual supply chain management of TPR, there are two issues identified, which are of equal relevance to the contractual safeguards imposed by the multinational on its external suppliers. The first is that the present third-party beneficiary doctrine (in the absence of a specific contractual clause thereto) in most cases does not provide for the possibility of TPR beneficiaries to enforce their rights under the TPR against the third-party supplier as well. The second issue is that, even in cases where the contract with a third-party supplier contains a third-party beneficiary clause, enforcement by the beneficiaries against such third-party supplier is not realistic, i.e. does not provide for meaningful redress in practice. A third more general issue raised in the literature regarding contractual supply management of TPR, is the inherent weakness of a chain of contracts along the supply chain replicating the required contractual clauses. This is also a feature of IT outsourcing arrangements, since in most cases the main outsourcing supplier not only involves many of its group companies as a sub-processor, but also includes third parties which do not form part of its group of companies. As a backdrop to the discussion of these three issues, it is important to realise that at present supply chain management, especially in the consumer protection area, appears to be the strongest tool to achieve protection for consumers in practice. Based on my research, my conclusion is that third-party beneficiary clauses in supply chain contracts – though they look good on paper – do not offer any meaningful form of redress for third-party beneficiaries. The recommendation to EU legislators concerning BCR is therefore not to focus on traditional judicial legal rights and remedies of individuals, but to concentrate on means of redress that actually lead to compliance in practice. A solution suggested in literature that could improve compliance with contractually imposed TPR obligations, is to require that TPR contain a provision allowing the pursuit of remedies against the multinational if it has not imposed proper contractual protections on the external supplier as required by the TPR. If the multinational fails to do so, the beneficiaries of the TPR can act against the multinational. Another practical solution would be that the internal complaints procedure that is required under BCR is open to complaints of beneficiaries as to the processing of their data by the external suppliers of the multinational, complemented by an obligation of the multinational to follow up these complaints with its external suppliers. These suggestions come very close to introducing the accountability approach to data transfers as provided by the APEC Privacy Framework, and the countries that have already introduced the accountability principle (as further discussed below).

BCR and the accountability principle

My observation is that on all accounts the 'accountability principle' does seem to be a good fit with EU data protection law. 'Accountability' is part of risk-based regulation, where companies themselves prioritise and tailor their compliance efforts dependent on the level of risk involved. This fits well with many provisions in the Data Protection Directive, requiring for instance "appropriate" security measures, "adequate" data protection safeguards, etc. This risk-based approach is also how multinationals manage their data protection in practice. In the digital society, data flows in networks, whether within multinationals, between multinationals, or between multinationals and individual customers (i.e. internet users). The participants in such networks manage risks: they accept them, try to limit or minimise them, or transfer them to co-contractors or other partners whether through supply chain management or otherwise. In practice therefore, data protection is regulated through risk management. Because so many partners and actors are involved in the data protection context, it seems impossible for regulators to regulate the data streams in any meaningful way without indeed "latching onto companies' inherent capacity to manage their risks". This is not a new insight, but a fact well known in other areas of law and a reason for states to resort to TPR, since the contracting parties have more power to enforce compliance in transnational situations than does the threat of traditional judicial means.

The general literature further makes abundantly clear that the introduction of the accountability principle should be accompanied by both sticks and carrots (i.e. should provide for clear incentives for companies to implement robust compliance programs and disincentives if they don't). It is clear that the present "carrot" for introducing BCR (i.e authorisation of intra-company data transfers) apparently does not provide a strong enough incentive, as evidenced by the current very low adoption of BCR. My recommendation to EU legislators is to introduce incentives for multinationals to adopt BCR, such as: abolishing the notification requirements, introducing risk-based sanctions (where the implementation of a proper compliance programme is a mitigating factor), and providing that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States. Comparing the BCR requirements with general accountability requirements in the general literature on the accountability principle in other fields of law and as listed by the Working Party 29, the Madrid Draft Proposal for International Standards and the Centre for Information Policy Leadership[2], lead me to conclude that the present requirements for BCR will

[2] The Centre for Information Policy Leadership is a private initiative. In this case the Centre acted as secretariat to a working group facilitated by various DPAs, which included 60 representatives

not require substantive updating. Indeed, the conclusion seems to be justified as the Working Party 29 put serious thought into making the BCR regime into a template for a model data compliance program for all companies (also in case the relevant company does not transfer data across borders). This being said, I recommend updating the BCR requirements, as they are often too specific and may prove counterproductive to achieving optimal data protection compliance by multinationals. The BCR requirements must be limited to setting the **core material data protection requirements** that need to be put in place by a multinational for internal compliance, without prescribing the **means and form** by which these requirements have to be achieved. A good example of such general accountability requirements are the "common fundamentals" for data protection accountability as defined by the Centre for Information Policy Leadership. These common fundamentals are however limited to accountability of a company in respect of **its own data processing operations**. Part of the business activities of any multinational is, however, that data are also transferred to third parties outside the group of companies (which also constitutes processing of data). Similar common fundamentals have to be formulated regarding the accountability of companies in respect of such outbound data transfers. For this inventory, I formulate some general starting points. One of the requirements should be that individuals will have "proper means of redress" (as previously identified as part of the evaluation of proper supply chain management). A more general guideline for drafting the inventory is the realisation that data processing is performed in networks rather than in neat one-to-one relationships. As discussed, a chain of contracts along the supply chain, replicating the required contractual clauses where regulatory obligations are passed on in the chain, has inherent weaknesses. A straightforward requirement for multinationals to impose certain contractual obligations on its contracting party may therefore not do the trick. The main objective of supply chain management is to minimise risks of non-compliance and to improve effectiveness and efficiency of control **at the source of such risk**. Rather than imposing requirements on all parties in the network, a more productive exercise may be to first identify the risks, the source of these risks and then allocate responsibilities accordingly. A factor in allocating responsibilities may also be identifying which of the parties has the best contracting power to enforce compliance. Taking it one step further, even if the responsibilities of the parties may be clearly established across the network, rather than the

of business, civil society, government, data protection and privacy enforcement agencies, and the European Data Protection Supervisor that on October 2010 issued a discussion document which identifies 9 common fundamentals that an accountable organisation should be prepared to implement and demonstrate to regulators.

fragmented liability of the different parties accumulating to full liability, liability of each could be imposed for the outcome of the network as a whole. Thought should be given to the question of whether the present set-up of the Data Protection Directive where the controller is the sole bearer of all data protection obligations is indeed the best **incentive** to achieve compliance in case of complex data processing operations which are part of a network. In light of the diminishing contracting power of multinationals vis-à-vis their multinational outsourcing suppliers, an obligation on **all parties** involved in data processing (whether controller or data processor) to achieve accountability as to the end result, may ultimately prove the better option. This may work as an incentive for all parties to come to a proper allocation of obligations in relation to the network as a whole. By separating the contractual form from the liability regime, it is left to the parties involved in the processing operation to allocate responsibilities where they are best placed.

BCR as a form of transnational private regulation

Many consider TPR unsuitable for regulating human rights. For instance, the European Commission in its White Paper on European Governance and the 2003 Inter-Institutional Agreement on Better Lawmaking, which promote co- and self-regulation when possible, provide that these mechanisms are not available if fundamental rights or important political options are at stake. The underlying assumption here seems to be that the fundamental rights expressed in the Constitution, being the expression of the state, only confer rights against the state (i.e. against public authority). In this view, human rights do not have a horizontal effect, i.e. do not confer obligations on private parties. The consequence would be that if private parties issue self-regulation, these could tread on human rights without these human rights being enforceable against such private parties. In such cases the state has to intervene. Hence, the requirement that any abridging of human rights should be through a legislative act, where a proper balancing of rights can be ensured. For a number of reasons, I conclude that this assumption is no longer valid. This view of human rights finds its basis in the origin of human rights, which were traditionally crafted to protect individuals from abuse of power by the state, which at the time were the biggest aggregations of power in society. In that tradition, companies are treated based on the notion that they are private, not public, entities, i.e. more like individuals than states. Accordingly, they are traditionally treated as **rights holders** of human rights, rather than duty holders. The fact is, however, that many multinationals now wield as much or even more power than many states, and the conditions of individuals' lives are shaped as much by multinationals as by states, especially in the area of workers' rights (e.g. equal pay, working hours, etc). Hence there now seems to be broad

consensus in the literature that multinationals should be (in addition to states) also **duty holders** as to certain human rights. In this view human rights do have "horizontal effect". Many national and international courts have applied human rights principles in private disputes and in some countries, the fundamental rights in the Constitution also apply equally to private and public relationships. Further, history shows that there are many instances where fundamental rights are pre-eminently regulated by self-regulation. Notable examples are found in the field of freedom of the press and the church, where self-regulation is often constitutionally preferred to forms of public regulation and, to some extent, public regulation is even prohibited.

My conclusion is that while the concerns of the Commission and EU institutions are understandable, a wholesale rejection of using self- and co-regulation to regulate human rights is contrary to current traditions and lacks theoretical foundation. The key issue should be on how concerns regarding human rights should influence the **regulatory design** for self-regulation and co-regulation, for instance by ensuring that the relevant rights and especially the outcome of any balancing of those rights against other fundamental rights, are safeguarded by public framework legislation. Indeed, in the literature, general public framework legislation for TPR is considered to be the appropriate form to apply if fundamental rights are at stake. The next question is whether the Data Protection Directive provides for an appropriate public legal framework for BCR. I first note that as opposed to most other human rights, data protection rights have from the outset also been directed at companies (and therefore not just states). The Data Protection Directive (when implemented into national legislation) thus already imposes direct data protection duties on multinationals (i.e. these therefore have per definition horizontal effect). This being said, the Data Protection Directive does not currently explicitly recognise that BCR are an appropriate tool to provide adequate safeguards for the transfer of data. In any event, it does not define the main substantive requirements for the adequate level to be provided by BCR. In its opinions, the Working Party 29 has recognised BCR as a valid tool for data transfers and defined these criteria, but these opinions are not binding (i.e. do not qualify as public regulation). As a consequence at present no proper formal legal framework exists for DPAs to review and authorise individual BCR, or for the national courts (and ultimately the ECJ) to be able to review BCR authorisation decisions of the DPAs. However, if this is remedied (as per my recommendations), there is no obstacle to having data protection regulated by BCR.

Evaluation of TPR

Despite differences in opinion about how to evaluate TPR, there seems to be more or less consensus among all authors that **public law making** should be evaluated based on four key criteria: Quality, Legitimacy, Effectiveness and Enforcement. These evaluation criteria (adapted to the particulars of TPR) may be taken as a starting point for evaluating TPR as well. To understand the issues in adapting (or "privatising") the evaluation criteria of public law to TPR, it is essential to realise that other than with public law, the norm-setting in respect of TPR often takes place at various levels, leading to more actors playing a role than "just" the public legislator. The criteria for evaluation of public law may therefore have to be divided over the various levels of norm-setting according to the involvement of the relevant actor in the overall norm-setting process. For instance, the BCR norm-setting presently not undertaken by EU legislators, but by the Working Party 29 and individual DPAs who issue opinions setting out the requirements of the BCR regime. Most authors agree that if the norm-setting for TPR is done by a *de facto* regulator, the "legitimacy" test cannot merely reproduce the model of the public regulation process. Legitimacy must then be provided through a "surrogate" legislative process that requires additional measures**,** such as stronger participation of the stakeholders of the TPR in the regulation process, increased transparency of the norm-setting process, as well as increased accountability and control of the de facto regulators.

The only valid manner in which a full assessment may be made of BCR against any such "transposed" criteria is to perform empirical research. All of the above evaluation criteria contain a perception element (i.e. are the norms in BCR **perceived** as predictable and legitimate, to lead to compliance in practice, to be enforced in practice, etc). At the time this dissertation is written, this empirical research is undertaken as part of the HiiL Program,[3] where BCR are one of the forms of TPR, which is evaluated against the transposed criteria. The expectation is that based on these findings, an informed assessment may be made as to (i) the extent to which the BCR norms, the creation process of BCR, the validation and implementation of BCR and the enforcement regime meet the "transposed" criteria of Quality, Legitimacy, Effectiveness and Enforcement and (ii) the

[3] HiiL Research Program 'Private Actors and Self-Regulation', into the legitimacy, effectiveness, enforcement and quality of different forms of TPR (**HiiL Program**). For the scope of the HiiL Program's research, see HiiL 2008, "The Added Value of Private Regulation in an International world? Towards a Model of the Legitimacy, Effectiveness, Enforcement and Quality of Private Regulation" and the "Draft Inventory Report", both dated May 2008 and to be found at <www.hiil.org>.

relative merits of BCR as compared with the "maturity" level of data protection compliance of multinationals prior to implementation of their BCR. Proposals for improvement of the BCR regime will subsequently be made based on these assessments.

This being said, there are some **normative elements** in the evaluation criteria which are known to influence how norms are ultimately perceived and responded to in practice. The pivotal factor for TPR in this respect is the question of legitimacy. Legitimacy requirements vary per phase of the regulatory process (a) norm-setting, (b) evaluation and monitoring and (c) enforcement. Legitimacy requirements are not absolute; different legitimacy demands may be made by the different addressees of the regulatory norms. In the BCR context, the addressees of the data protection rules are: (i) the multinationals; and (ii) the beneficiaries of the BCR (i.e. the employees and customers of the multinationals (if these are consumers). In the case of BCR, different legitimacy demands may be made by the multinationals to which the rules are addressed, and the beneficiaries of BCR, which may lead to a "legitimacy dilemma" for a regulatory regime.
To ensure accountability **ex-ante** of the de facto regulators, the following legitimacy requirements have to be complied with in the **norm-setting phase**:

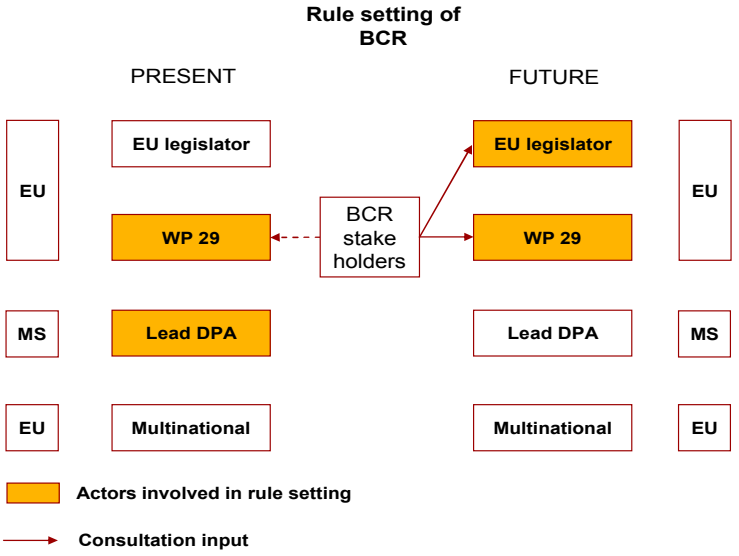
(i) Participation (key stakeholders have to play an active role in the decision-making processes and activities which affect them).
(ii) Transparency (key stakeholders should have accessible and timely information)
(iii) Independence (regulators should be independent).

To ensure accountability **ex-post** of the de facto regulators, additional requirements apply to the **monitoring and evaluation phase** and the **enforcement phase**.

My findings in respect of the norm-setting phase are that the BCR regime as developed by (mainly) the Working Party 29 in its opinions does not meet the legitimacy requirements as to norm-setting. The norm-setting process has **not** been inclusive in the sense that the beneficiaries of BCR (i.e. employee or consumer organisations and civil society stakeholders) have been sufficiently included in the norm-setting process. As business organisations (both as addressees of the BCR regime) were amply represented in the norm-setting process, even the risk exists that the Working Party 29, while deciding on its BCR opinions, was subject to "regulatory capture" (if not all stakeholders are involved or heard, impartiality of the regulator is at risk). The norm-setting procedure by the Working Party 29 is further not sufficiently transparent and the

independence of the Working Party 29 is currently not sufficiently ensured. This potential lack of legitimacy should be remedied in the future by enacting the norms for BCR in the revised Data Protection Directive and to hold a proper prior consultation of all stakeholders. Further, in the event that the norms for BCR are enacted in the revised Directive, the Working Party 29 will maintain a role in providing further guidelines in respect of these rules, therewith *de facto* setting norms for DPAs and controllers. Legitimacy demands require that also in respect of such *de facto* norm-setting, proper stakeholder consultation will take place. This proposal can be visualised as follows:

Chart 1



In my dissertation, I make similar evaluations and proposals in respect of the **ex-ante** accountability of the de facto BCR regulators involved in the (i) monitoring and evaluation phase and (ii) the enforcement phase.

BCR and corporate social responsibility

As indicated before, the parallel between BCR and CSR codes is compelling. CSR codes are also based on accountability. Though in principle companies are free to choose the manner in which they achieve CSR compliance, in the absence of a CSR code and a compliance program, non-compliance will in practice be a given. The same will apply if the accountability principle is also introduced for data protection. The conclusion is even justified that at

present, soft law instruments regulating CSR already require multinationals to include data protection commitments in their CSR codes as a consequence of which BCR are more or less indispensible to ensure accountability in this respect. This turns BCR from an alternative tool for data protection compliance into an indispensable tool for data protection for multinationals.

Overall conclusion of the study

In light of the above findings, it is high time that the current uncertainties as to the validity and enforcement of BCR are solved, that the BCR authorisation procedure is streamlined and that the enforcement powers of DPAs are harmonised and a common enforcement strategy for the DPAs is developed to ensure equal enforcement. This should not be achieved by way of further opinions of the Working Party 29, but by a revision of the Data Protection Directive, which should preferably take the form of an EU regulation or, as the next best alternative, confer in the revised Directive the implementing powers in respect of such revised Directive onto the European Commission. In either case, EU legislators are advised to delegate the **detailed norm-setting** to the European Commission in such EU regulation or revised Directive.

To ensure a wider adoption of BCR within the EU, European legislators are further advised to ensure that incentives are created for multinationals to adopt BCR. To further the recognition of BCR also in countries outside the EU for outbound data transfers from these countries, EU legislators are advised to engage with such countries to achieve mutual recognition and enforcement of BCR.

To foster the acceptability of BCR on a global scale, the search for common reference points with other disciplines and perspectives has resulted in a number of common requirements across disciplines. The current BCR regime does not incorporate all such common reference points. A striking example is the requirement of transparency of compliance results with the BCR. This led to the recommendation of imposing a reporting obligation on multinationals regarding data protection compliance under their BCR in their annual report or in a comparable format. This transparency recommendation is based on the outcomes of an evaluation of the BCR regime from the:

(i) accountability perspective in general literature as to other fields of law;
(ii) the introduction of the accountability principle for data protection;
(iii) general policy research and literature in the area of consumer protection;

(iv) general policy literature in the area of company law;
(v) the law and economics approach;
(vi) BCR as a form of TPR and legitimacy requirements in this respect;
(vii) BCR as a form of CSR;
(viii) economic policy theory.

It is also true for most other recommendations that each is based on the outcomes of the evaluation from at least two of these disciplines. Many of the recommendations further overlap with those made by the Working Party 29, the European Data Protection Supervisor, the Centre for Information Policy Leadership and the European Commission. The results thus combined may hopefully result in a better theoretical foundation for revision of the Data Protection Directive based on these recommendations.

Building on my findings in Part I, my overall conclusions in respect of Part II is that even if the applicability and jurisdiction regime of the Data Protection Directive is harmonised and improved as recommended, BCR as an instance of TPR can do better than the present jurisdiction-based application and enforcement of the Data Protection Directive: (i) in providing data protection to individuals; (ii) in providing enforcement mechanisms to individuals; and (iii) in regulating trans-border data flows.

Ad (i) avoiding gaps in data protection
If BCR have indeed a global scope, data protection is also provided to data processed by the multinational in countries where no or less data protection is provided for by state laws. Thus gaps in data protection left by the regulation of nation states are no longer relevant.

Ad (ii) avoiding gaps in enforcement
If a choice of law and forum may indeed be validly made in BCR, and beneficiaries of BCR may indeed enforce their rights as unilateral undertakings under BCR, BCR will provide for better enforcement of data protection by individuals in practice. Individuals are provided with a central facility for complaints and the many obstacles to cross-border enforcement of data protection by individuals will be addressed. The individual will be able to file a complaint in his own language, with the group company with which he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The group company that receives the complaint will be responsible for ensuring that the complaint is processed through the complaints' procedure of the multinational and will ensure the required translations. If the complaints' procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the Lead DPA or the

courts of the Lead DPA. This procedure will lead to enforceable rights even if damages of individuals are diffuse or too small to pursue through traditional judicial means, jurisdictions have no (adequate) data protection laws or if insufficient enforcement (infrastructure) is available. It further overcomes language issues, time zone obstacles and minimises costs. These are all issues that presently constitute challenges to the cross-border enforcement of data protection rights.

Ad (iii) improved regulation of transborder data flows

BCR result in lower administrative burdens for multinationals while at the same time provide for more material data protection and redress to individuals. This is a vast improvement to the situation where trans-border data flows within multinationals are regulated by means of the EU Standard Contractual Clauses, which leads to high administrative burdens for multinationals, while at the same time the contractual data protection rights and remedies of individuals do not lead to meaningful data protection and redress in practice. If the BCR regime does indeed define the core accountability principles in situations where a multinational transfers personal data to third parties, the same will apply to data flows to such third parties.

Annex I Overview of Recommendations to EU legislators

RECOMMENDATIONS PART I

1. Ensure an adequate harmonisation of the applicability regime of the Data Protection Directive.
2. Introduce the country-of-origin principle.
3. Delete Article 4(1)(a) and (c) Data Protection Directive and instead provide that the data protection law of a Member State applies:
- to the processing of personal data in the context of the activities of the controller in or directed at the territory of the Member State;
- and if the first ground is not applicable, to the processing of personal data in the territory of the Member State, but only insofar as it implements the obligations of a data processor to ensure that the data processing (i) is adequately secured in accordance with Article 17 of this Directive and (ii) provides for an adequate level of protection for the data processed within the meaning of Article 25(2) of the Directive.

4. Ensure an adequate harmonisation of the jurisdiction regime of the Data Protection Directive.
5. Provide that the DPA of the country-of-origin of the controller will have jurisdiction.

RECOMMENDATIONS PART II

1. Introduce the country-of-origin principle and extend this principle also to countries having obtained an adequacy ruling under Article 25(6) Data Protection Directive.
2. Recognise BCR as an appropriate tool to provide adequate safeguards for the transfer of data and define the main substantive requirements for BCRs:
- to be defined in general principles
- to be set at an adequate level

and to delegate the further norm-setting to the European Commission pursuant to Article 290(1) TFEU.
3. Investigate whether it is indicated to establish a pan-European Data Protection Supervisory Authority to which certain decision-making and enforcement powers are delegated in case of data protection violations with an EU dimension
4. Define the MRP and impose the MRP on all Member States.
5. Provide for equal enforcement powers for DPAs and develop a common enforcement strategy for the DPAs to ensure equal enforcement.
6. Replace the Data Protection Directive by an EU regulation when revising the Directive, or, as the next best alternative, to confer implementing powers in respect of the revised Directive on the Commission pursuant to Article 291(1) TFEU.
7. Engage with non-EU countries in mutual recognition and enforcement of BCR as a tool for cross-border data transfers.

8. Provide that BCR can be enforced as unilateral undertakings by the beneficiaries of BCR.

9. Provide that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA and further that the Lead DPA will have central supervision in respect of such BCR, and may involve other DPAs if so required for enforcement in the territories of the other Member States.

10. Provide that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States.

11. Introduce incentives for multinationals to adopt BCR, such as:

- risk-based sanctions for a violation of data protection by multinationals that have implemented BCR (whereby the implementation of a proper compliance program is a mitigating factor);
- providing that if multinationals adopt BCR, the BCR apply instead of the national data protection laws of the Member States (as per *Recommendation 10*), or as next best alternative, providing that in BCR a choice of law and forum may be made for the laws and courts of the Member State of the Lead DPA (see *Recommendation 9*);
- abolishing the notification requirements, or, as next best alternative, providing for the possibility of central notification of all data processing of a multinational to the Lead DPA.

12. Add as requirements for BCR:

- prescribing the reporting on BCR in the annual reports of company in a comparable format;
- the multinational should be transparent vis-à-vis the third-party beneficiaries as to the number of complaints received and the nature of these complaints under the internal complaints procedure;
- defining the BCR requirements as to accountability in general obligations of the multinational on the basis of the common fundamentals defined by the Centre for Information Policy Leadership.

13. Not to follow the recommendation by the Working Party 29 to include a provision in the revised Data Protection Directive that controllers remain accountable and responsible for the protection of data for which they are controllers, even if the data have been transferred to other controllers.

14. Define the core accountability principles for the situation when a multinational transfers personal data to third parties, taking into account the guidelines identified in this paragraph.

15. Hold a proper consultation of all stakeholders of BCR prior to enacting the norms for BCR in the revised Data Protection Directive (or the EU regulation);

- Instruct the European Commission to hold a consultation of all stakeholders of BCR prior to the further norm-setting on BCR by the European Commission;
- Instruct the Working Party 29 to hold a consultation of relevant stakeholders prior to the Working Party 29 issuing opinions on BCR.

16. Instruct the Working Party 29 to amend its Rules of Procedure to remedy the lack of transparency as to its decision making progress.

17.
- Ensure the independence of the Working Party in accordance with the criteria developed by the ECJ for independence of DPAs
- Instruct the Working Party 29 to amend its Rules of Procedure to ensure its accountability as to independence by:
  - having any experts participating in its meetings issue a public declaration of interests;
  - introducing job rotation of the members of any sub-groups installed by the Working Party 29.

18. Require Lead DPAs to publish the BCR authorisations including the text of the BCR authorised.

19. Provide that the BCR regime should apply to all personal data processed by the multinational adopting the BCR.

	Contract Law	PIL	Accountability	TPR	CSR	First Report	Rand Report	WP 29	EC	EDPS	CIPL
Recommendation											
1								•			
2			•	•	•	•	•	•	•	•	•
3							•	•	•	•	•
4											
5							•	•	•	•	
6										•	
7							•				•
8	•	•	•	•	•						
9		•									
10											
11	•		•		•		•	•	•	•	•
12			•	•	•						
13											
14											
15				•			•				
16				•		•			•	•	
17				•						•	
18			•	•	•						
19					•						

Annex II BCR for Employee Data

[Company]

Privacy Code for Employee Data

Introduction
[Company] has committed itself to the protection of personal data of [Company] employees in the [Company] **[Code of Conduct]**.

This Privacy Code for Employee Data indicates how this principle shall be implemented. For the privacy code applicable to customer, supplier and business partner data, refer to the *Privacy Code for Customer, Supplier and Business Partner Data*. **[insert hyperlink to Code]**

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of [Company] Employees (**Employee Data**) by [Company] or a Third Party on behalf of [Company].
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Employee Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Employees keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Employee Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, this Code shall apply.
Sub-policies and notices	1.4	[Company] may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The [**Responsible Executive**] shall be responsible for compliance with this Code.

Effective Date 1.6 This Code has been adopted by the **[Head of Legal or Head of Compliance]** of **[Company Holding]** and shall enter into force as of [ ] (**Effective Date**) and shall be published on the **[Company Intranet]** and be made available to Employees upon request.

Code supersedes prior policies 1.7 This Code supersedes all [Company] privacy policies and notices that exist on the Effective Date to the extent they address the same issues.

Implementation 1.8 This Code shall be implemented in the [Company] organization based on the timeframes specified in Article 21.

Role of [Company EU Headquarters] 1.9 [Company Holding] has tasked [Company EU Headquarters] with the coordination and implementation of this Code.

Article 2 – Purposes for Processing Employee Data

Legitimate Business Purposes 2.1 Employee Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (**Business Purposes**):

(i) **[Human resources and personnel management.** This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the employment-at-will relationship, e.g. management and administration of recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, and Employee communications

(ii) **Business process execution and internal management.** This purpose addresses activities such as scheduling work, recording time, managing company assets, provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, implementing business controls, and managing and using Employee directories

(iii) **Health, safety and security.** This purpose addresses activities such as those involving occupational safety and health, the protection of company and Employee assets, and the authentication of Employee status and access rights

(iv) **Organizational analysis and development and management reporting.** This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis

(v) **Compliance with legal obligations.** This purpose addresses the Processing of Employee Data as necessary for compliance with a legal obligation to which [Company] is subject or

(vi) **Protecting the vital interests of Employees.** This is where Processing is necessary to protect the vital interests of an Employee.

list all categories of business purposes]

Where there is a question whether a Processing of Employee Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Employee consent

2.2 Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes must exist for any Processing of Employee Data. If applicable local law so requires, in addition to having a Business Purpose for the relevant Processing, [Company] shall also seek Employee consent for the Processing. If none of the Business Purposes applies, [Company] may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee.

A request for Employee consent requires the authorization of the appropriate Privacy Officer prior to seeking consent.

Denial or withdrawal of Employee consent

2.3 The Employee may both deny consent and withdraw consent at any time without consequence to his employment relationship. Where Processing is undertaken at the Employee's request (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.

When seeking Employee consent, [Company] must inform the

Employee:

(i) of the purposes of the Processing for which consent is requested

(ii) of the possible consequences for the Employee of the Processing and

(iii) that he is free to refuse and withdraw consent at any time without consequence to his employment relationship.

Limitations on Processing Data of Dependants of Employees

2.4 [Company] will Process Data of Dependants of an Employee if:

(i) the Data were provided with the consent of the Employee or the Dependant

(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship or

(iii) the Processing is required or permitted by applicable local law.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

3.1 Generally, Employee Data shall be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Employee Data may be Processed for a legitimate Business Purpose of [Company] different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Employee Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee, the secondary use may require additional measures such as:

(i) limiting access to the Data

(ii) imposing additional confidentiality requirements

(iii) taking additional security measures

(iv) informing the Employee about the Secondary Purpose

(v) providing an opt-out opportunity or

(vi) obtaining Employee consent in accordance with Article 2.2.

Generally permitted uses of Data for Secondary Purposes

3.2 It is generally permissible to use Employee Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1:

(i) transfer of the Data to an Archive

(ii) internal audits or investigations

(iii) implementation of business controls

(iv) statistical, historical or scientific research
(v) preparing for or engaging in dispute resolution
(vi) legal or business consulting or
(vii) insurance purposes.

Article 4 – Purposes for Processing Sensitive Data

Specific purposes for Processing Sensitive Data

4.1 This Article sets forth specific rules for Processing Sensitive Data. [Company] shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose.

The following categories of Sensitive Data may be collected, used or otherwise Processed only for one or more of the purposes specified below:

[(i) **Racial or ethnic data**:
(a) in some countries photos and video images of Employees qualify as racial or ethnic data. [Company] may process photos and video images for the protection of [Company] and Employee assets, site access and security reasons and for inclusion in Employee directories
(b) providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection to the relevant Processing

(ii) **Physical or mental health data** (including any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy):
(a) providing health services to an Employee provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements
(b) administering pensions, health and welfare benefit plans, maternity, paternity or family leave programmes, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee
(c) reintegrating or providing support for Employees

entitled to benefits in connection with illness or work incapacity

(d) assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities

(e) providing facilities in the workplace to accommodate heath problems or disabilities

(iii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):

(a) assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee

(b) protecting the interests of [Company] with respect to criminal offenses that have been or, given the relevant circumstances are suspected to have been, committed against [Company] or its Employees

(iv) **Sexual preference** (including data relating to partners of Employees):

(a) administering Employee pensions and benefits programs

(b) administering Employee memberships

(v) **Religious or philosophical beliefs**:

(a) accommodating religious or philosophical practices, dietary requirements or religious holidays.]

General Purposes for Processing of Sensitive Data

4.2 In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed for one (or more) of the following:

(i) as required by or allowed under applicable local law

(ii) for the establishment, exercise or defence of a legal claim

(iii) to protect a vital interest of an Employee, but only where it is impossible to obtain the Employee's consent first

(iv) to the extent necessary to comply with an obligation of international public law (e.g. treaties) or

(v) [where the Sensitive Data have manifestly been made public by the Employee].

Employee consent for Processing Sensitive

4.3 Employee consent generally cannot be used as a legitimate basis for Processing Sensitive Data. One of the grounds listed in Article 4.1 or 4.2 must exist for any Processing of Sensitive Data. If applicable local law so requires, in addition to having one of the grounds listed in

Data		Article 4.1 or 4.2 for the relevant Processing, [Company] shall also seek Employee consent for the Processing. If none of the grounds listed in Article 4.1 or 4.2 applies, [Company] may request Employee consent for Processing Sensitive Data, but only if the Processing has no foreseeable adverse consequences for the Employee (e.g. Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.3 applies to the granting, denial or withdrawal of Employee consent.
Prior Authorization of Privacy Officer	4.4	Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, or based on the consent of the Employee, the Processing requires the prior authorization of the appropriate Privacy Officer.
Use of Sensitive Data for Secondary Purposes	4.5	Sensitive Data of Employees or Dependants may be Processed for Secondary Purposes in accordance with Article 3.

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	[Company] shall restrict the Processing of Employee Data to those Data that are reasonably adequate for and relevant to the applicable Business Purpose. [Company] shall take reasonable steps to delete Employee Data that are not required for the applicable Business Purpose.
Storage period	5.2	[Company] generally shall retain Employee Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations. [Company] may specify (e.g. in a sub-policy, notice or records retention schedule) a time period for which certain categories of Employee Data may be kept. Promptly after the applicable storage period has ended, the Responsible Executive shall direct that the Data be: (i) securely deleted or destroyed

(ii) anonymized [alternative: de-identified] or
(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Data 5.3 Employee Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

'Self-service' 5.4 Where [Company] requires an Employee to update his own Employee Data, [Company] shall remind him at least once a year to do so.

Article 6 – Employee Information Requirements

Information requirements 6.1 [Company] shall inform Employees through a published privacy policy or notice about:
(i) the Business Purposes for which their Data are Processed
(ii) which Group Company is responsible for the Processing and
(iii) other relevant information (e.g. the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any), and how Employees can exercise their rights).

Article 7 – Employee Rights of Access and Rectification

Rights of Employees 7.1 Every Employee has the right to request an overview of his Employee Data Processed by or on behalf of [Company]. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant Employee Data.
If the Employee Data are incorrect, incomplete or not Processed in compliance with applicable law or this Code, the Employee has the right to have his Data rectified, deleted or blocked (as appropriate).

In addition, the Employee has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

Procedure 7.2 The Employee should send his request to the appropriate Privacy Officer.

Prior to fulfilling the request of the Employee, [Company] may require

the Employee to:

(i) specify the type of Employee Data to which he is seeking access
(ii) specify the data system in which the Employee Data are likely to be stored
(iii) specify the circumstances in which [Company] obtained the Employee Data
(iv) show proof of his identity and
(v) in the case of a request for rectification, deletion, or blockage, specify the reasons why the Employee Data are incorrect, incomplete or not Processed in accordance with applicable law or the Code.

Response period 7.3 Within four weeks of [Company] receiving the request, the Privacy Officer shall inform the Employee in writing either (i) of [Company] position with regard to the request and any action [Company] has taken or will take in response or (ii) the ultimate date on which he will be informed of [Company's] position, which date shall be no later than [x] weeks thereafter.

Complaint 7.4 An Employee may file a complaint in accordance with Article 16.1 if:

(i) the response to the request is unsatisfactory to the Employee (e.g. the request is denied)
(ii) the Employee has not received a response as required by Article 7.3 or
(iii) the time period provided to the Employee in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

Denial of requests 7.5 [Company] may deny an Employee request if:

(i) the request does not meet the requirements of Articles 7.1 and 7.2
(ii) the request is not sufficiently specific
(iii) the identity of the relevant Employee cannot be established by reasonable means
(iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval.

Article 8 – Security and Confidentiality Requirements

Data security 8.1 [Company] shall take appropriate commercially reasonable technical, physical and organizational measures to protect Employee Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, [Company] has developed and implemented the [Company] [**list main ICT policies**] and other policies relating to the protection of Employee Data.

Staff access 8.2 Staff members shall be authorized to access Employee Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

Confidentiality obligations 8.3 Staff members who access Employee Data must meet their confidentiality obligations.

Article 9 – Automated Decision Making

Automated decisions 9.1 Automated tools may be used to make decisions about Employees but decisions may not be based solely on the results provided by the automated tool. This restriction does not apply if:

(i) the use of automated tools is required or authorized by law

(ii) the decision is made by [Company] for purposes of (a) entering into or performing a contract or (b) managing the employment-at-will relationship, provided the underlying request leading to a decision by [Company] was made by the Employee (e.g. where automated tools are used to filter job applications) or

(iii) suitable measures are taken to safeguard the legitimate interests of the Employee, e.g. the Employee has been provided with an opportunity to express his point of view.

Article 10 – Transfer of Employee Data to Third Parties

Transfer to Third Parties 10.1 This Article sets forth requirements concerning the transfer of Employee Data from [Company] to a Third Party. Note that a transfer of Employee Data includes situations in which [Company] discloses Employee Data to Third Parties (e.g. in the context of corporate due

diligence) or where [Company] provides remote access to Employee Data to a Third Party.

Third Party Controllers and Third Party Processors

10.2 There are two categories of Third Parties:

(i) **Third Party Processors**: these are Third Parties that Process Employee Data solely on behalf of [Company] and at its direction (e.g. Third Parties that Process Employee salaries on behalf of [Company])

(ii) **Third Party Controllers**: these are Third Parties that Process Employee Data and determine the purposes and means of the Processing (e.g. government authorities or service providers that provide services directly to Employees).

Transfer for applicable Business Purposes only

10.3 [Company] shall transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose for which the Employee Data are Processed (including Secondary Purposes as per Article 3 or purposes for which the Employee has provided consent in accordance with Article 2).

Third Party Controller contracts

10.4 Third Party Controllers (other than government agencies) may Process Employee Data only if they have a written contract with [Company]. In the contract, [Company] shall seek to contractually protect the data protection interests of its Employees. All such contracts shall be drafted in consultation with the appropriate Privacy Officer.

Third Party Processor contracts

10.5 Third Party Processors may Process Employee Data only if they have a written contract with [Company]. The contract with a Third Party Processor must include the following provisions:

(i) the Processor shall Process Employee Data only in accordance with [Company]'s instructions and for the purposes authorized by [Company]

(ii) the Processor shall keep the Employee Data confidential

(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Employee Data

(iv) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to [Company] without the prior written consent of [Company]

(v) [Company] has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by [Company] or any relevant government

authority

(vi) the Third Party Processor shall promptly inform [Company] of any actual or suspected security breach involving Employee Data and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide [Company] with all relevant information and assistance as requested by [Company] regarding the security breach.

Transfer of Data to a Non-Adequate Country

10.6 This Article sets forth additional rules for the transfer of Employee Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Employee Data (**Non-Adequate Country**).

Employee Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Employee, for managing the employment-at-will relationship or to take necessary steps at the request of the Employee prior to entering into a contract or an employment-at-will relationship, e.g. for processing job applications

(ii) a contract has been concluded between [Company] and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any)

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Employee between [Company] and a Third Party (e.g. in case of the booking of an airline ticket)

(iv) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection

(v) the Third Party has implemented binding corporate rules or a similar transfer control mechanisms which provide adequate safeguards under applicable law

(vi) the transfer is necessary to protect a vital interest of the Employee

(vii) the transfer is necessary for the establishment, exercise or defence of a legal claim

(viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society or

(ix) the transfer is required by any law to which the relevant Group

Company is subject.

Items (viii) and (ix) above require the prior approval of the Chief Privacy Officer.

Employee consent for transfer

10.7 [Company] generally shall not seek Employee consent for a transfer of Employee Data to a Third Party located in a Non-Adequate Country. One of the grounds for transfer listed in Article 10.6 must exist. If applicable local law so requires, in addition to having one of the grounds listed in Article 10.6, [Company] shall also seek Employee consent for the relevant transfer. If none of the grounds listed in Article 10.6 exists, [Company] may request Employee consent for a transfer to a Third Party located in a Non-Adequate Country, but only if

(i) the transfer has no foreseeable adverse consequences for the Employee or
(ii) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Requesting Employee consent for a transfer requires the prior approval of the appropriate Privacy Officer. Prior to requesting Employee consent, the Employee shall be provided with the following information:

(i) the purpose of the transfer
(ii) the identity of the transferring Group Company
(iii) the identity or categories of Third Parties to which the Data will be transferred
(iv) the categories of Data that will be transferred
(v) the country to which the Data will be transferred and
(vi) the fact that the Data will be transferred to a Non-Adequate Country.

Transfers between Non-Adequate Countries

10.8 This Article sets forth additional rules for transfers of Employee Data that were collected in connection with the activities of a Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 10.6, these transfers are permitted if they are:

(i) necessary for compliance with a legal obligation to which the relevant Group Company is subject
(ii) necessary to serve the public interest or

(iii) necessary to satisfy a Business Purpose of [Company].

Article 11 – Overriding Interests

Overriding Interests

11.1 Some of the obligations of [Company] or rights of Employees under this Code may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Employee (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) protect the legitimate business interests of [Company] including
  (a) the health, security or safety of Employees
  (b) [Company]'s intellectual property rights, trade secrets or reputation
  (c) the continuity of [Company]'s business operations
  (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business or
  (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes

(ii) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law, breaches of the terms of employment, or non-compliance with the [Company] Code of Ethics or other [Company] policies or procedures or

(iii) otherwise protect or defend the rights or freedoms of [Company], its Employees or other persons.

Exceptions in the event of Overriding Interests

11.2 If an Overriding Interest exists, one or more of the following obligations of [Company] or rights of the Employee may be set aside:

(i) Article 3.1 (the requirement to Process Employee Data for closely related purposes)

(ii) Article 6.1 (information provided to Employees)

(iii) Article 7.1 (rights of Employees)

(iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements) and

(v) Articles 10.4, 10.5 and 10.6 (ii) (contracts with Third Parties).

Sensitive Data

11.3 The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 11.1 (i) (a), (c) and (e), (ii) and (iii).

Consultation with Chief Privacy Officer 11.4 Setting aside obligations of [Company] or rights of Employees based on an Overriding Interest, requires the prior consultation of the Chief Privacy Officer.

Information to Employee 11.5 Upon request of the Employee, [Company] shall inform the Employee of the Overriding Interest for which obligations of [Company] or rights of the Employee have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1, in which case the request shall be denied.

Article 12 – Supervision and compliance

Chief Privacy Officer 12.1 **[Company EU Headquarters] [of [Company Holding]?]** shall appoint a Chief Privacy Officer who is responsible for:

(i) supervising compliance with this Code

(ii) providing periodic reports, as appropriate, to the **[Head of Legal/Head of Compliance]** on data protection risks and compliance issues and

(iii) coordinating, in conjunction with the appropriate Privacy Officer, official investigations or inquiries into the Processing of Data by a government authority.

Privacy Council 12.2 [The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for:

(i) the development, implementation and updating of local Employee data protection policies and procedures

(ii) the development of the policies, procedures and system information (as required by Article 13)

(iii) the development, implementation and updating of the training and awareness programs

(iv) the monitoring and reporting on compliance with this Code

(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints and

(vi) determining and updating appropriate sanctions for violations of this Code (e.g. disciplinary standards).]

Privacy Officers 12.3 Each Group Company shall designate a Privacy Officer. **[The Chief Privacy Officer shall act as the Privacy Officer for [Company Holding]]** These Privacy Officers may, in turn, establish a network of

Privacy Officers sufficient to direct compliance with this Code within their respective organizations.
The Privacy Officers shall:

(i) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues
(ii) maintain (or ensure access to) an inventory of the system information (as required by Article 13.2)
(iii) establish a framework for a privacy compliance program as required by the Chief Privacy Officer and
(iv) cooperate with the Chief Privacy Officer and the other Privacy Officers, and the **[[Company] Compliance Officers]**.

Responsible Executive 12.4 **[Tasks and responsibilities of Responsible Executive]**

Default Privacy Officer 12.5 If at any moment in time there is no Privacy Officer designated for a function or business, the designated **[compliance officer for the [Company] Code of Conduct]** for the relevant function or business is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position 12.6 Where a Privacy Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

Article 13 – Policies and procedures

Policies and procedures 13.1 [Company] shall develop and implement policies and procedures to comply with this Code.

System information 13.2 [Company] shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Employee Data (e.g. inventory of systems and processes, privacy impact assessments).

Article 14 – Training

Staff training 14.1 [Company] shall provide training on this Code and related confidentiality obligations to Staff members who have access to

Employee Data.

Article 15 – Monitoring and auditing compliance

Audits 15.1 [Company] Internal Audit shall audit business processes and procedures that involve the Processing of Employee Data for compliance with this Code. The audits shall be carried out in the course of the regular activities of [Company] Internal Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article 15.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Officers shall be informed of the results of the audits. A copy of the audit results will be provided to the Dutch Data Protection Authority upon request.

Annual Report 15.2 The Chief Privacy Officer shall produce an annual Employee Data privacy report for the **[Head of Legal or Head of Compliance?]** on compliance with this Code and other relevant issues.

Each Privacy Officer shall provide information relevant to the report to the Chief Privacy Officer.

Mitigation 15.3 [Company] shall, if so indicated, ensure that adequate steps are taken to address breaches of this Code identified during the monitoring or auditing of compliance pursuant to this Article 15.

Article 16 – Complaints procedure

Complaint to Privacy Officer 16.1 Employees may file a complaint regarding compliance with this Code or violations of their rights under applicable local law:

(i) in accordance with the complaints procedure set forth in the [Company] Code of Conduct or

(ii) with the appropriate Privacy Officer.

The appropriate Privacy Officer shall:

(a) notify the Chief Privacy Officer;

(b) initiate an investigation and

(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through completion,

the steps designed to achieve compliance.

The appropriate Privacy Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Employee 16.2 Within four weeks of [Company] receiving a complaint, the appropriate Privacy Officer shall inform the Employee in writing either (i) of [Company] position with regard to the complaint and any action [Company] has taken or will take in response or (ii) when he will be informed of [Company]'s position, which date shall be no later than [x] weeks thereafter. The appropriate Privacy Officer shall send a copy of the complaint and his written reply to the Chief Privacy Officer.

Complaint to Chief Privacy Officer 16.3 An Employee may file a complaint with the Chief Privacy Officer if:

(i) the resolution of the complaint by the appropriate Privacy Officer is unsatisfactory to the Employee (e.g. the complaint is rejected)

(ii) the Employee has not received a response as required by Article 16.2

(iii) the time period provided to the Employee pursuant to Article 16.2 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response Or

(iv) in the events listed in Article 7.4.

The procedure described in Articles 16.1 through 16.2 shall apply to complaints filed with the Chief Privacy Officer.

Article 17 – Legal issues

Local law and jurisdiction 17.1 Any Processing by [Company] of Employee Data shall be governed by applicable local law. Employees keep their own rights and remedies as available in their local jurisdictions. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

Law applicable 17.2 This Code shall be governed by and interpreted in accordance with Dutch law. This Code shall apply only where it provides supplemental

to Code; Code has supplemental character		protection for Employee Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, this Code shall apply.
Lead Authority for supervision of Rules	17.3	Compliance with this Code shall be exclusively supervised by the Dutch Data Protection Authority in the Netherlands, which is also exclusively authorized to advise **[Company EU Headquarters]** on the application of this Code at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act. To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of this Code.
Exclusive jurisdiction under Code	17.4	Any complaints or claims of an Employee concerning any supplemental right the Employee may have under this Code shall be directed to **[Company EU Headquarters]** only and shall be brought before the Dutch Data Protection Authority in the Netherlands or the competent court in Amsterdam, the Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, the Netherlands have exclusive jurisdiction over any supplemental rights provided by this Code. Complaints and claims shall be admissible only if the Employee has first followed the complaints procedure set forth in Article 16 of this Code.
Code enforceable against [Company EU Headquarters] only	17.5	Any additional safeguards, rights or remedies granted to Employees under this Code are granted by and enforceable in the Netherlands against [Company EU Headquarters] only.
Available remedies, limitation of damages, burden of proof re damages	17.6	Employees shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, **[Company EU Headquarters]** shall be liable only for direct damages suffered by an Employee resulting from a violation of this Code. Provided an Employee can demonstrate that it has suffered damage and establish facts which show it is plausible that the damage has occurred because

of a violation of the Code, it will be for **[Company EU Headquarters]** to prove that the damages suffered by the Employee due to a violation of the Code are not attributable to the relevant Group Company.

Mutual assistance and redress

17.7 All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:

(i) a request, complaint or claim made by an Employee or

(ii) a lawful investigation or inquiry by a competent government authority.

The Group Company employing the Employee is responsible for handling any communication with the Employee regarding his request, complaint or claim except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse **[Company EU Headquarters]**.

Article 18 – Sanctions for non-compliance

Non compliance

18.1 Non-compliance of Employees with this Code may result in disciplinary action up to and including termination of employment.

Article 19 – Conflicts between the Code and applicable local law

Conflict of law when transferring Data

19.1 Where a legal requirement to transfer Employee Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Chief Privacy Officer. The Chief Privacy Officer shall seek the advice of the Head of Legal. The Chief Privacy Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Conflict between Code and law

19.2 In all other cases, where there is a conflict between applicable local law and the Code, the relevant Responsible Executive shall consult with the Chief Privacy Officer to determine how to comply with this Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New

19.3 The relevant Responsible Executive shall promptly inform the Chief

conflicting legal require-ments

Privacy Officer of any new legal requirement that may interfere with [Company]'s ability to comply with this Code.

Article 20 – Changes to the Code

Prior approval 20.1 Any changes to this Code require the prior approval of the **[Head of Legal or Head of Compliance of [Company Holding]**. [Company EU Headquarters] shall notify the Dutch Data Protection Authority in case of significant changes to the Code on a yearly basis.

No employee consent 20.2 This Code may be changed without Employee consent even though an amendment may relate to a benefit conferred on Employees.

Entry, no force 20.3 Any amendment shall enter into force after it has been approved and published on the **[Company Intranet]**.

Relevant code 20.4 Any request, complaint or claim of an Employee involving this Code shall be judged against this Code that is in force at the time the request, complaint or claim is made.

Article 21 – Transition Periods

General Transition Period 21.1 Except as indicated below, there shall be a two-year transition period for compliance with this Code. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Employee Data shall be undertaken in compliance with the Code. During any transition period, [Company] shall strive to comply with the Code.

Transition Period for New Group Companies 21.2 Any entity that becomes a Group Company after the Effective Date shall comply with the Code within two years of becoming a Group Company.

Transition Period for IT Systems 21.3 Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four years from the Effective Date or from the date an entity becomes a Group Company, or any longer

period as is reasonably necessary to complete the update, change or replacement process.

Transition Period for Existing Agreements 21.4 Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Transitional Period for Local-for-Local Systems 21.5 Processing of Employee Data that were collected in connection with activities of a Group Company located in a Non-Adequate Country shall be brought into compliance with this Code within five years of the Effective Date.

Contact details [Company] Privacy Office
c/o [Company EU Headquarters]

Archive	ARCHIVE shall mean a collection of Employee Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Employee Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer as referred to in Article 12.1.
Code	CODE shall mean this Privacy Code for Employee Data.
Dependant	DEPENDANT shall mean the spouse, partner or child belonging to the household of the Employee.
Effective Date	EFFECTIVE DATE shall mean the date on which this Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean an employee, job applicant or former employee of [Company]. This term does not include people working at [Company] as consultants or employees of Third Parties providing services to [Company].
Employee Data or Data	EMPLOYEE DATA or DATA shall mean any information relating to an identified or identifiable Employee (and his Dependants).
EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
EU Data Protection Directive	EU DATA PROTECTION DIRECTIVE shall mean the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of and the free movement of such data.
Group Company	GROUP COMPANY shall mean [Company Holding] and any company or legal entity of which [Company Holding], directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a

	liaison and/or relationship exists, and that is covered by the [Company] Code of Conduct.
Head of Legal	HEAD OF LEGAL shall mean the Head of Legal of [Company Holding].
Head of Compliance	HEAD OF COMPLIANCE shall mean the Head of Compliance of [Company Holding].
Non-Adequate Country	NON-ADEQUATE COUNTRY shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an "adequate" level of data protection.
Original Purpose	ORIGINAL PURPOSE shall mean the purpose for which Employee Data was originally collected.
Overriding Interest	OVERRIDING INTEREST shall mean the pressing interests set forth in Article 11.1 based on which the obligations of [Company] or rights of Employees set forth in Article 11.2 and 11.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Employee.
Privacy Council	PRIVACY COUNCIL shall mean the council referred to in Article 12.2
Privacy Officer	PRIVACY OFFICER shall mean a privacy officer appointed by the Chief Privacy Officer pursuant to Article 12.3.
Processing	PROCESSING shall mean any operation that is performed on Employee Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Employee Data.
[Company Holding]	[Company Holding] shall mean [Company Holding], having its registered seat in [ ].
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean **[lowest grade executive with primary budget responsibility]**.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Employee Data is further Processed.
Sensitive Data	SENSITIVE DATA shall mean Employee Data that reveal an Employee's racial or ethnic origin, political opinions or membership in political parties or similar

	organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
[Company]	[Company] shall mean [Company Holding] and its Group Companies.
[Company EU Headquarters]	[Company EU Headquarters] shall mean [Company EU Headquarters], having its registered seat in [ ], the Netherlands.
Staff	STAFF shall mean all Employees and other persons who Process Employee Data as part of their respective duties or responsibilities using [Company] information technology systems or working primarily from [Company]'s premises.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside [Company].
Third Party Controller	THIRD PARTY CONTROLLER shall mean a Third Party that Processes Employee Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR shall mean a Third Party that Processes Employee Data on behalf of [Company] that is not under the direct authority of [Company].

Interpretations

INTERPRETATION OF THIS CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in construing any provision of this Code

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning

(iv) the male form shall include the female form

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa and

(vi) a reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Code or that other document.

Annex III BCR for Customer Data

[Company]

Privacy Code for Customer, Supplier and Business Partner Data

Introduction

[Company] has committed itself to the protection of personal data of [Company] Customers, Suppliers and Business Partners in the [Company] [Code of Conduct].

This Code indicates how this principle shall be implemented. For the rules applicable to Employee Data, refer to the *Privacy Code for Employee Data*. **[hyperlink]**

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Customers, Suppliers and Business Partners by [Company] or a Third Party on behalf of [Company]. This Code does not address the Processing of Employee Data of [Company].
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Individuals keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.
Sub-policies and notices	1.4	[Company] may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The [**Responsible Executive**] shall be responsible for compliance with this Code.
Effective	1.6	This Code has been adopted by the **[Head of Legal or Head of**

Date		**Compliance]** of **[Company Holding]** and shall enter into force as of [ ] (Effective Date) and shall be published on the [Company website and Company intranet] and be made available to Individuals upon request.
Code supersedes prior policies	1.7	This Code supersedes all [Company] privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	This Code shall be implemented in the [Company] organization based on the timeframes specified in Article 22.
Role of [Company EU Headquarters]	1.9	[Company Holding] has tasked [Company EU Headquarters] with the coordination and implementation of this Code.

Article 2 – Purposes for Processing Personal Data

Legitimate Business Purposes 2.1 Personal Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (**Business Purposes**):

[(i) **Development and improvement of products and/or services.** This purpose includes Processing that is necessary for the development and improvement of [Company] products and/or services, research and development

(ii) **Conclusion and execution of agreements with Customers, Suppliers and Business Partners.** This purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Customers, Suppliers and Business Partners and to record and financially settle delivered services, products and materials to and from [Company]

(iii) **Relationship management and marketing.** This purpose addresses activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls and the development, execution and analysis of market surveys and marketing strategies.

(iv) **Business process execution, internal management and management reporting.** This purpose addresses activities such as managing company assets, conducting internal audits and investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes managing mergers, acquisitions and divestitures, and Processing Personal Data for management reporting and analysis.

(v) **Health, safety and security.** This purpose addresses activities such as those involving safety and health, the protection of [Company] and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights

(vi) **Compliance with legal obligations.** This purpose addresses the Processing of Personal Data necessary for compliance with a legal obligation to which [Company] is subject; or

(vii) **Protection vital interests of Individuals.** This is where Processing is necessary to protect the vital interests of an Individual.]

Where there is a question whether a Processing of Personal Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Consent 2.2 If a Business Purpose does not exist or if applicable local law so requires [Company] shall (also) seek consent from the Individual for the Processing.

Where Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.
When seeking consent, [Company] must inform the Individual:

(i) of the purposes of the Processing for which consent is required and

(ii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any) and how Individuals can exercise their rights).

Denial or 2.3 The Individual may both deny consent and withdraw consent at any

withdrawal of consent time.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes 3.1 Generally, Personal Data shall be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for a legitimate Business Purpose of [Company] different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Individual, the secondary use may require additional measures such as:

(i) limiting access to the Data
(ii) imposing additional confidentiality requirements
(iii) taking additional security measures
(iv) informing the Individual about the Secondary Purpose
(v) providing an opt-out opportunity or
(vi) obtaining Individual consent in accordance with Article 2.2.

Generally permitted uses of Data for Secondary Purposes 3.2 It is generally permissible to use Personal Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1:

(i) transfer of the Data to an Archive
(ii) internal audits or investigations
(iii) implementation of business controls
(iv) statistical, historical or scientific research
(v) preparing for or engaging in dispute resolution
(vi) legal or business consulting or
(vii) insurance purposes.

Article 4 – Purposes for Processing Sensitive Data

Specific purposes for Processing Sensitive Data 4.1 This Article sets forth specific rules for Processing Sensitive Data. [Company] shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose.

The following categories of Sensitive Data may be collected, used or otherwise Processed only for one (or more) of the purposes specified

below:

[(i) **Racial or ethnic data**: in some countries photos and video images of Individuals qualify as racial or ethnic data. [Company] may process photos and video images for the protection of [Company] and Employee assets, site access and security reasons, and the authentication of Customer, Supplier or Business Partner status and access rights

(ii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior) for protecting the interests of [Company] with respect to criminal offenses that have been or, given the relevant circumstances are suspected to have been, committed against [Company] or its Employees.]

General Purposes for Processing of Sensitive Data

4.2 In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed under (one or more of) the following circumstances:

(i) the Individual has given his explicit consent to the Processing thereof

(ii) as required by or allowed under applicable local law

(iii) for the establishment, exercise or defence of a legal claim

(iv) to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first

(v) to the extent necessary to comply with an obligation of international public law (e.g. treaties) or

(vi) [if the Sensitive Data have manifestly been made public by the Individual.]

Denial or withdrawal of consent

4.3 The information requirements of Article 2.2 and Article 2.3 apply to the granting, denial or withdrawal of consent.

Prior Authorization of Privacy Officer

4.4 Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, the Processing requires the prior authorization of the appropriate Privacy Officer.

Use of Sensitive Data for Secondary

4.5 Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3.

Purposes

Article 5 – Quantity and Quality of Data

No Excessive Data 5.1 [Company] shall restrict the Processing of Personal Data to Data that are reasonably adequate for and relevant to the applicable Business Purpose. [Company] shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.

Storage period 5.2 [Company] generally shall retain Personal Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations. [Company] may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Responsible Executive shall direct that the Data be:

(i) securely deleted or destroyed
(ii) anonymized [alternative: de-identified] or
(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Data 5.3 Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

Accurate, complete and up-to-date Data 5.4 It is the responsibility of the Individuals to keep his Personal Data accurate, complete and up-to-date. Individuals shall inform [Company] regarding any changes in accordance with Article 7.

Article 6 – Individual Information Requirements

Information requirements 6.1 [Company] shall inform Individuals through a privacy policy or notice about:

(i) the Business Purposes for which their Data are Processed
(ii) which Group Company is responsible for the Processing and
(iii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which

the Data are disclosed (if any) and how Individuals can exercise their rights).

Personal Data not obtained from the Individual

6.2 If applicable local law so requires, where Personal Data have not been obtained directly from the Individual, [Company] shall provide the Individual with the information as set out in Article 6.1:

(i) at the time that the Personal Data are recorded in a [Company] database or

(ii) at the time that the Personal Data are used for a mailing, provided that this mailing is done within six months after the Personal Data are recorded in a [Company] database.

Exceptions

6.3 The requirements of Article 6.2 may be set aside if:

(i) it is impossible or would involve a disproportionate effort to provide the information to Individuals or

(ii) it results in disproportionate costs.

These exceptions to the above requirements qualify as Overriding Interests.

Article 7 – Individual Rights of Access and Rectification

Rights of Individuals

7.1 Every Individual has the right to request an overview of his Personal Data Processed by or on behalf of [Company]. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant Personal Data.

If the Personal Data are incorrect, incomplete or not Processed in compliance with applicable law or this Code, the Individual has the right to have his Data rectified, deleted or blocked (as appropriate).

In addition, the Individual has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

Procedure

7.2 The Individual should send his request to the contact person or contact point indicated in the relevant privacy policy. If no contact person or contact point is indicated, the Individual may send his request **[ ]**.

Prior to fulfilling the request of the Individual, [Company] may require

the Individual to:

(i) specify the type of Personal Data to which he is seeking access

(ii) specify, to the extent reasonably possible, the data system in which the Data are likely to be stored

(iii) specify the circumstances in which [Company] obtained the Personal Data

(iv) show proof of his identity and

(v) in the case of a request for rectification, deletion, or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with applicable law or the Code.

Response period 7.3 Within four weeks of [Company] receiving the request, the contact person, [contact point,] or Privacy Officer shall inform the Individual in writing either (i) of [Company] position with regard to the request and any action [Company] has taken or will take in response or (ii) the ultimate date on which he will be informed of [Company's] position, which date shall be no later than [x] weeks thereafter.

Complaint 7.4 An Individual may file a complaint in accordance with Article 17.1 if:

(i) the response to the request is unsatisfactory to the Individual (e.g. the request is denied)

(ii) the Individual has not received a response as required by Article 7.3 or

(iii) the time period provided to the Individual in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

Denial of requests 7.5 [Company] may deny an Individual request if:

(i) the request does not meet the requirements of Articles 7.1 and 7.2

(ii) the request is not sufficiently specific

(iii) the identity of the relevant Individual cannot be established by reasonable means or

(iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval.

Article 8 – Security and Confidentiality Requirements

Data security 8.1 [Company] shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

Staff access 8.2 Staff members shall be authorized to access Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

Confidentiality obligations 8.3 Staff members who access Personal Data must meet their confidentiality obligations.

Article 9 – Direct Marketing

Direct marketing 9.1 This Article sets forth requirement concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).

Consent for direct marketing (opt-in) 9.2 If applicable law so requires, [Company] shall only sent to Individuals unsolicited commercial communication by fax, email, sms and mms with the prior consent of the Individual ("opt-in"). If applicable law does not require prior consent of the Individual, [Company] shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.

Exception (opt-out) 9.3 Prior consent of the Individual for sending unsolicited commercial communication by fax, email, sms and mms is not required if:

(i) an Individual has provided his electronic contact details to a Group Company in the context of a sale of a product or service of such Group Company; and

(ii) such contact details are used for direct marketing of such Group Company's own similar products or services

(iii) provided that an Individual clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his electronic contact details when they are collected by the Group Company.

Information to be provided in each communication	9.4	In every direct marketing communication that is made to the Individual, the Individual shall be offered the opportunity to opt-out of further direct marketing communication.
Objection to direct marketing	9.5	If an Individual objects to receiving marketing communications from [Company], or withdraws her consent to receive such materials, [Company] will take steps to refrain from sending further marketing materials as specifically requested by the individual. [Company] will do so within the time period required by applicable law.
Third Parties and Direct marketing	9.6	No Data shall be provided to, or used on behalf of, Third Parties for purposes of direct marketing without the prior consent of the Individual.
Personal Data of Children	9.7	[Company] shall not use any Personal Data of Individuals under the age of fourteen (14) years for direct marketing.
Direct marketing records	9.8	[Company] shall keep a record of Individuals that used their "opt-in" or "opt-out" right and will regularly check to public opt-out registers.

Article 10 – Automated Decision Making

Automated decisions	10.1	Automated tools may be used to make decisions about Individuals but decisions may not be based solely on the results provided by the automated tool. This restriction does not apply if: (i) the use of automated tools is required or authorized by law (ii) the decision is made by [Company] for purposes of (a) entering into or performing a contract or (b) managing the contract, provided the underlying request leading to a decision by [Company] was made by the Individual (e.g., where automated tools are used to filter promotional game submissions) or (iii) suitable measures are taken to safeguard the legitimate interests of the Individual, e.g., the Individual has been provided with an opportunity to express his point of view.

Article 11 – Transfer of Personal Data to Third Parties

Transfer to Third Parties

11.1 This Article sets forth requirements concerning the transfer of Personal Data from [Company] to a Third Party. Note that a transfer of Personal Data includes situations in which [Company] discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where [Company] provides remote access to Personal Data to a Third Party

Third Party Controllers and Third Party Processors

11.2 There are two categories of Third Parties:

(i) **Third Party Processors**: these are Third Parties that Process Personal Data solely on behalf of [Company] and at its direction (e.g., Third Parties that Process online registrations made by Customers)

(ii) **Third Party Controllers**: these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., [Company] Business Partners that provide their own goods or services directly to Customers).

Transfer for applicable Business Purposes only

11.3 [Company] shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 3 or purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller contracts

11.4 Third Party Controllers (other than government agencies) may Process Personal Data only if they have a written contract with [Company]. In the contract, [Company] shall seek to contractually safeguard the data protection interests of its Individuals. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. Individual Business Contact Data may be transferred to a Third Party Controller without a contract if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to Individual's job responsibilities.

Third Party Processor contracts

11.5 Third Party Processors may Process Personal Data only if they have a written contract with [Company]. The contract with a Third Party Processor must include the following provisions:

(i) the Processor shall Process Personal Data only in accordance

with [Company]'s instructions and for the purposes authorized by [Company]

(ii) the Processor shall keep the Personal Data confidential

(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data

(iv) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to [Company] without the prior written consent of [Company]

(v) [Company] has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by [Company] or any relevant government authority

(vi) the Third Party Processor shall promptly inform [Company] of any actual or suspected security breach involving Personal Data and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide [Company] with all relevant information and assistance as requested by [Company] regarding the security breach.

Transfer of Data to a Non-Adequate Country

11.6 This Article sets forth additional rules for the transfer of Personal Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Personal Data (**Non-Adequate Country**).

Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Individual, for managing a contract with Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders

(ii) a contract has been concluded between [Company] and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any)

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between [Company] and a Third Party (e.g. in case of recalls)

(iv) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection

(v) the Third Party has implemented binding corporate rules or a similar transfer control mechanisms which provide adequate safeguards under applicable law
(vi) the transfer is necessary to protect a vital interest of the Individual
(vii) the transfer is necessary for the establishment, exercise or defence of a legal claim
(viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society or
(ix) the transfer is required by any law to which the relevant Group Company is subject.

Items (viii) and (ix) above require the prior approval of the Chief Privacy Officer.

Consent for transfer 11.7 If none of the grounds listed in Article 11.6 exist or if applicable local law so requires [Company] shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country.
Prior to requesting consent, the Individual shall be provided with the following information:
(i) the purpose of the transfer
(ii) the identity of the transferring Group Company
(iii) the identity or categories of Third Parties to which the Data will be transferred
(iv) the categories of Data that will be transferred
(v) the country to which the Data will be transferred and
(vi) the fact that the Data will be transferred to a Non-Adequate Country.
Article 2.3 applies to denial or withdrawal of consent.

Transfers between Non-Adequate Countries 11.8 This Article sets forth additional rules for transfers of Personal Data that were collected in connection with the activities of a Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 11.6, these transfers are permitted if they are:
(i) necessary for compliance with a legal obligation to which the relevant Group Company is subject
(ii) necessary to serve the public interest or
(iii) necessary to satisfy a Business Purpose of [Company].

Article 12 – Overriding Interests

Overriding Interests

12.1 Some of the obligations of [Company] or rights of Individuals under this Code may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) protect the legitimate business interests of [Company] including
  (a) the health, security or safety of Employees or Individuals
  (b) [Company]'s intellectual property rights, trade secrets or reputation
  (c) the continuity of [Company]'s business operations
  (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business or
  (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes
(ii) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law or
(iii) otherwise protect or defend the rights or freedoms of [Company], its Employees or other persons.

Exceptions in the event of Overriding Interests

12.2 If an Overriding Interest exists, one or more of the following obligations of [Company] or rights of the Individual may be set aside:

(i) Article 3.1 (the requirement to Process Personal Data for closely related purposes)
(ii) Article 6.1 and 6.2 (information provided to Individuals, Personal Data not obtained from the Individuals)
(iii) Article 7.1 (rights of Individuals)
(iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements) and
(v) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).

Sensitive Data

12.3 The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (c) and (e), (ii) and (iii).

Consultation with Chief

12.4 Setting aside obligations of [Company] or rights of Individuals based on an Overriding Interest requires prior consultation of the Chief Privacy Officer.

Privacy Officer

Information to Individual

12.5 Upon request of the Individual, [Company] shall inform the Individual of the Overriding Interest for which obligations of [Company] or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1, in which case the request shall be denied.

Article 13 – Supervision and compliance

Chief Privacy Officer

13.1 **[Company EU Headquarters] [of [Company Holding]?]** shall appoint a Chief Privacy Officer who is responsible for:

(i) supervising compliance with this Code

(ii) providing periodic reports, as appropriate, to the **[Head of Legal/Head of Compliance]** on data protection risks and compliance issues and

(iii) coordinating, in conjunction with the appropriate Privacy Officer, official investigations or inquiries into the Processing of Data by a government authority.

Privacy Council

13.2 [The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for:

(i) the development, implementation and updating of local Individual data protection policies and procedures

(ii) the development of the policies, procedures and system information (as required by Article 14)

(iii) the development, implementation and updating of the training and awareness programs

(iv) the monitoring and reporting on compliance with this Code

(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints and

(vi) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).]

Privacy Officers

13.3 Each Group Company shall designate a Privacy Officer. [The Chief Privacy Officer shall act as the Privacy Officer for [Company Holding]] These Privacy Officers may, in turn, establish a network of Privacy Officers sufficient to direct compliance with this Code within their respective organizations.

The Privacy Officers shall:

(i) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues

(ii) maintain (or ensure access to) an inventory of the system information (as required by Article 14.2)

(iii) establish a framework for a privacy compliance program as required by the Chief Privacy Officer and

(iv) cooperate with the Chief Privacy Officer and the other Privacy Officers, and the **[[Company] Compliance Officers]**.

Responsible Executive 13.4 **[Tasks and responsibilities of Responsible Executive]**

Default Privacy Officer 13.5 If at any moment in time there is no Privacy Officer designated for a function or business, the designated **[compliance officer for the [Company] Code of Conduct]** for the relevant function or business is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position 13.6 Where a Privacy Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

Article 14 – Policies and procedures

Policies and procedures 14.1 [Company] shall develop and implement policies and procedures to comply with this Code.

System information 14.2 [Company] shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Data (e.g. inventory of systems and processes, privacy impact assessments).

Article 15 – Training

Staff training 15.1 [Company] shall provide training on this Code and related confidentiality obligations to Staff members who have access to Personal Data.

Article 16 – Monitoring and auditing compliance

Audits 16.1 [Company] Internal Audit shall audit business processes and procedures that involve the Processing of Personal Data for compliance with this Code. The audits shall be carried out in the course of the regular activities of [Company] Internal Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Officers shall be informed of the results of the audits. A copy of the audit results will be provided to the Dutch Data Protection Authority upon request.

Annual report 16.2 The Chief Privacy Officer shall produce an annual Personal Data privacy report for the **[Head of Legal or Head of Compliance?]** on compliance with this Code and other relevant issues.

Each Privacy Officer shall provide information relevant to the report to the Chief Privacy Officer.

Mitigation 16.3 [Company] shall, if so indicated, ensure that adequate steps are taken to address breaches of this Code identified during the monitoring or auditing of compliance pursuant to this Article 16.

Article 17 – Complaints procedure

Complaint 17.1 Individuals may file a complaint regarding compliance with this Code or violations of their rights under applicable local law in accordance with the complaints procedure set forth in the relevant privacy policy or contract. The complaint shall be forwarded to the appropriate Privacy Officer.

The appropriate Privacy Officer shall:

(a) notify the Chief Privacy Officer;

(b) initiate an investigation and

(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance.

The appropriate Privacy Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Individual 17.2 Within four weeks of [Company] receiving a complaint, the appropriate Privacy Officer shall inform the Individual in writing either (i) of [Company] position with regard to the complaint and any action [Company] has taken or will take in response or (ii) when he will be informed of [Company]'s position, which date shall be no later than [x] weeks thereafter. The appropriate Privacy Officer shall send a copy of the complaint and his written reply to the Chief Privacy Officer.

Complaint to Chief Privacy Officer 17.3 An Individual may file a complaint with the Chief Privacy Officer if:

(i) the resolution of the complaint by the appropriate Privacy Officer is unsatisfactory to the Individual (e.g., the complaint is rejected)

(ii) the Individual has not received a response as required by Article 17.2

(iii) the time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response or

(iv) in one of the events listed in Article 7.4.

The procedure described in Articles 17.1 through 17.2 shall apply to complaints filed with the Chief Privacy Officer.

Article 18 – Legal issues

Local law and jurisdiction 18.1 Any Processing by [Company] of Personal Data shall be governed by applicable local law. Individuals keep their own rights and remedies as available in their local jurisdictions. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

Law applicable to Code; Code has 18.2 This Code shall be governed by and interpreted in accordance with Dutch law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code

supplemental character

provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.

Lead authority for supervision of rules

18.3 Compliance with this Code shall be exclusively supervised by the Dutch Data Protection Authority in the Netherlands, which is also exclusively authorized to advise **[Company EU Headquarters]** on the application of this Code at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act. To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of this Code.

Exclusive jurisdiction under Code

18.4 Any complaints or claims of an Individual concerning any supplemental right the Individual may have under this Code shall be directed to **[Company EU Headquarters]** only and shall be brought before the Dutch Data Protection Authority in the Netherlands or the competent court in Amsterdam, the Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, the Netherlands have exclusive jurisdiction over any supplemental rights provided by this Code. Complaints and claims shall be admissible only if the Individual has first followed the complaints procedure set forth in Article 17 of this Code.

Code enforceable against [Company EU Headquarters] only

18.5 Any additional safeguards, rights or remedies granted to Individuals under this Code are granted by and enforceable in the Netherlands against **[Company EU Headquarters]** only.

Available remedies and, limitation of damages

18.6 Individuals shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, **[Company EU Headquarters]** shall be liable only for direct damages suffered by an Individual resulting from a violation of this Code. Where an Individual can demonstrate that it has suffered damage and establish facts which show it is plausible that the damage has occurred because of a violation of the Code, it will be for **[Company EU Headquarters]** to prove that the damages suffered by the Individual due to a violation of

the Code are not attributable to the relevant Group Company.

Mutual assistance and redress

18.7 All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:

(i) a request, complaint or claim made by an Individual or

(ii) a lawful investigation or inquiry by a competent government authority.

The Group Company who receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his request, complaint or claim except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse **[Company EU Headquarters]**.

Article 19 – Sanctions for non-compliance

Non compliance

19.1 Non-compliance of Employees with this Code may result in disciplinary action up to and including termination of employment.

Article 20 – Conflicts between the Code and applicable local law

Conflict of law when transferring Data

20.1 Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Chief Privacy Officer. The Chief Privacy Officer shall seek the advice of the Head of Legal. The Chief Privacy Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Conflict between Code and law

20.2 In all other cases, where there is a conflict between applicable local law and the Code, the relevant Responsible Executive shall consult with the Chief Privacy Officer to determine how to comply with this Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal

20.3 The relevant Responsible Executive shall promptly inform the Chief Privacy Officer of any new legal requirement that may interfere with [Company]'s ability to comply with this Code.

require-ments

Article 21 – Changes to the Code

Prior approval 21.1 Any changes to this Code require the prior approval of the **[Head of Legal or Head of Compliance of [Company Holding]**. [Company EU Headquarters] shall notify the Dutch Data Protection Authority in case of significant changes to the Code on a yearly basis.

No employee consent 21.2 This Code may be changed without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.

Entry, into force 21.3 Any amendment shall enter into force after it has been approved and published on the **[Company website]**.

Relevant code 21.4 Any request, complaint or claim of an Individual involving this Code shall be judged against this version of the Code as it is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

General transition period 22.1 Except as indicated below, there shall be a two-year transition period for compliance with this Code. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with the Code. During any transition period, [Company] shall strive to comply with the Code.

Transition period for new Group Companies 22.2 Any entity that becomes a Group Company after the Effective Date shall comply with the Code within two years of becoming a Group Company.

Transition period for IT Systems 22.3 Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition period for existing agreements	22.4	Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.
Transitional period for local-for-local systems	22.5	Processing of Personal Data that were collected in connection with activities of a Group Company located in a Non-Adequate Country shall be brought into compliance with this Code within five years of the Effective Date.

Contact details

[Company] Privacy Office
c/o [Company EU Headquarters]
[insert contact details]

ANNEX 1 Definitions

Archive	ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.
Article	ARTICLE shall mean an article in this Code.
Business Contact Data	BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Individual in his contact with [Company].
Business Partner	BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or had a business relationship or strategic alliance with [Company] (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer as referred to in Article 13.1.
Code	CODE shall mean this Privacy Code for Customer, Supplier and Business Partner Data.
Customer	CUSTOMER shall mean any Third Party that purchases, may purchase or has purchased a [Company] product or service.
Effective Date	EFFECTIVE DATE shall mean the date on which this Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean an employee, job applicant or former employee of [Company]. This term does not include people working at [Company] as consultants or employees of Third Parties providing services to [Company].
Employee Data	EMPLOYEE DATA shall mean any information relating to an identified or identifiable Employee.

EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
EU Data Protection Directive	EU DATA PROTECTION DIRECTIVE shall mean the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of and the free movement of such data.
Group Company	GROUP COMPANY shall mean [Company Holding] and any company or legal entity of which [Company Holding], directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a liaison and/or relationship exists, and that is covered by the [Company] Code of Conduct.
Head of Legal	HEAD OF LEGAL shall mean the Head of Legal of [COMPANY HOLDING].
Head of Compliance	HEAD OF COMPLIANCE shall mean the Head of Compliance of [Company Holding].
Individual	INDIVIDUAL shall mean any (employee of or any person working for) Customer, Supplier or Business Partner.
Personal Data or Data	PERSONAL DATA shall mean any information relating to an identified or identifiable Individual.
Non-Adequate Country	NON-ADEQUATE COUNTRY shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an "adequate" level of data protection.
Original Purpose	ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.
Overriding Interest	OVERRIDING INTEREST shall mean the pressing interests set forth in Article 12.1 based on which the obligations of [Company] or rights of Individuals set forth in Article 12.2 and 12.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.
Privacy Council	PRIVACY COUNCIL shall mean the council referred to in Article 13.2
Privacy	PRIVACY OFFICER shall mean a privacy officer appointed by the Chief

Officer	Privacy Officer pursuant to Article 13.3.
Processing	PROCESSING shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
[COMPANY HOLDING]	[COMPANY HOLDING] shall mean [Company Holding], having its registered seat in [ ].
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean **[lowest grade executive with primary budget responsibility]**.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.
Sensitive Data	SENSITIVE DATA shall mean Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Supplier	SUPPLIER shall mean any Third Party that provides goods or services to [Company] (e.g. an agent, consultant or vendor).
[Company]	[Company] shall mean [COMPANY HOLDING] and its Group Companies.
[Company EU Headquarters]	[Company EU Headquarters] shall mean [Company EU Headquarters], having its registered seat in [ ], the Netherlands.
Staff	STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using [Company] information technology systems or working primarily from [Company]'s premises.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside [Company].
Third Party	THIRD PARTY CONTROLLER shall mean a Third Party that Processes

Controller	Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of [Company] that is not under the direct authority of [Company].

Interpretations

INTERPRETATION OF THIS CODE:
(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time
(ii) headings are included for convenience only and are not to be used in construing any provision of this Code
(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning
(iv) the male form shall include the female form
(v) the words “include”, “includes” and “including” and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa and
(vi) a reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Code or that other document.

BIBLIOGRAPHY PART I

Books

Berkvens, J.M.A., *Wet bescherming persoonsgegevens; Leiddraad voor de praktijk*, supplement 3, Deventer: Kluwer 2002

Brownlie, I. , *Principles of Public International Law*, Oxford University Press 2008

Capps, P., M. Evans and S. Konstadinidis (eds.), *Asserting Jurisdiction: International and European Legal Perspectives*, Oxford: Hart Publishing 2003

Castendyk, O., E. Dommering, and A. Scheuer, *European Media Law*, Alphen aan den Rijn: Kluwer Law International 2008

Dammann, U. and S. Simitis, *EG-Datenschutzrichtlinie*, Berlin: Nomos 1997

Goldsmith, J. and T. Wu, *Who controls the Internet? Illusions of a Borderless World*, Oxford University Press 2008

Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Gutwirth, S., Y. Poullet, P. de Hert, R. Leenes (eds.), *Computers, Privacy, and data Protection: an Element of Choice*, Dordrecht: Springer 2010

Hart, H.L.A. , *The Concept of Law*, Oxford University Press 1997

Kelsen, H., *General Theory of Law and State*, New Brunswick, NJ: Transaction Publishers 2005

Kohl, U., *Jurisdiction and the Internet: a Study of Regulatory Competence over Online Activity*, Cambridge University Press 2007

Koops, B.J. et. al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Kuner, C., *European Data Protection Law: Corporate Compliance and Regulation*, Oxford: Oxford University Press 2007

Magnus, U. and P. Mankowksi (eds.), *Brussels I Regulation*, Munich: Sellier European Law Publishers 2007

Mann, F.A., *Studies in International Law*, Oxford: Clarendon Press 2008

Nuyts, A., *International Litigation in Intellectual Property and Information Technology*, Kluwer International 2008

Prins, J.E.J. and J.M.A. Berkvens, *Privacyregulering in theorie en praktijk* (Privacy regulation in theory and practice); Series Recht en Praktijk, part 75, Deventer: Kluwer 2007

Schulz, W. and T. Held, *Regulated self-regulation as a form of modern government. An analysis of case studies from media and telecommunications law*, Luton: University of Luton Press 2004

Svantesson, D.J.B., *Private International Law and the Internet*, Kluwer Law International 2007

Vries, H. de, *T&C Telecommunicatiewet*, Deventer: Kluwer 2002
Restatement of the Law (Third), The Foreign Relations Law of the United States (American Law Institute Publishers 1987), vol 1, 237, stating 'in a number of contexts the question of jurisdiction to prescribe resembles questions traditionally

Articles

Bing, J., "Data protection, jurisdiction and the Choice of Law", (1999) *Privacy Law and Policy Reporter* (Available at http://www.austlii.edu.au/au/journals/PLPR/1999/65.html)

Blok, P.J., "Privacybescherming in alle staten" (Privacy protection; a problem everywhere), (2005) 6 *Computerrecht*, 297-304

Bygrave, L.A., "Determining Applicable Law Pursuant to European Data Protection Legislation", (2000) *Computer Law and Security Report* 252
(http://folk.uio.no/lee/oldpage/articles/Applicable_law.pdf)

Carey, P., *Data Protection, A Practical guide to UK and EU law*, Oxford University Press 2009

Chen, C., "Comment, United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce", (2004) 25 *U. P. J. Int'l Econ. L.* 423

Dammann, U., "Internationaler Datenschutz", (2002) *Recht der Datenverarbeitung*, 70

Fontein-Bijnsdorp, M.A.H., "Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens", (2008) *Computerrecht*, 287–291

Foss, M. and L.A. Bygrave, "International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law", (2000) 8 *International Journal of Law and Information Technology*, 99 – 138

Goldsmith, J., "Against Cyberanarchy", (1998) 65 *University of Chicago Law Review*, 1199

Goldsmith, J., "Unilateral Regulation of the Internet: A Modest Defence", (2000) 11 *European Journal of International Law*, 135

Hill, J., "The Exercise of Jurisdiction in Private International Law" in: P. Capps, M. Evans and S. Konstadinidis (eds.), *Asserting Jurisdiction: International and European Legal Perspectives*, Oxford: Hart Publishing 2003

Hooghiemstra, T. and S. Nouwt, Explanation to Article 4, in: Tekst en Toelichting Wet Bescherming Persoonsgegevens (Text and explanation Personal Data Protection, The Hague: Sdu 2007

Kuner C., "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 176 (Available at SSRN: http://ssrn.com/abstract=1496847)

Kuner, C., "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2) ", (2010) 18 *International Journal of Law and Information Technology* (Available at SSRN: http://ssrn.com/abstract=1689495)

Michaels, R., 'Two Paradigms of Jurisdiction', (2006) 1003 *Michigan Journal of International Law*

Moerel, E.M.L., "The country of origin principle in the E-commerce Directive: the expected "one stop shop"?", (2001) *Computer Technology Law Report*, 84-90

Moerel, E.M.L., "Back 2 Basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?, " (2008) *Computerrecht*, 81 – 92

Moerel, E.M.L., "Art. 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines", (2008) *Computerrecht*, 290

Moerel, E.M.L., "The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", (2011) 1 *International Data Privacy Law*, 23-41

Moerel, E.M.L., "Back to basics: when does EU data protection law apply?", (2011) 2 *International Data Privacy Law*, 92-110

Oren, J.S.T., "Electronic Agents and the notion of Establishment", (www.eclip.org), also published in (2001) *International Journal of Law and Information Technology*, 249-274

Poullet, Y., J-M. Van Gyseghem, J-Ph. Moiny, J. Gerard and C. Gayrel "Data Protection in the Clouds" in: Gutwirth, S., Y. Poullet, P. de Hert, R. Leenes (eds.) *Computers, Privacy, and data Protection: an Element of Choice*, Dordrecht: Springer 2010

Schultz, T., "Carving up the Internet: Jurisdiction, legal Orders, and the private/Public International Law Interface", (2008) 19 *European Journal of International Law*, 799-839

Prins, C., "Should ICT Regulation Be Undertaken at an International Level?", in Koops, B.J. et. al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Simitis, S., "From the Market to the Polis: The EU Directive on the Protection of Personal Data," (1994-95) 445 *Iowa L. Rev.*, 445

Slot, P.J. and E. Grabandt, "Extraterritoriality and jurisdiction", (1986) 23 *Common Market Law Review 23*

Swire, P., "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," (1998) 32 *International Lawyer*, 991

Swire, P.P. "Elephants and Mice Revisited: law and Choice of Law on the Internet," (2005) 153 *University of Pensylvania Law Review*, 1975-2001

Terstegge, J.H.J "Home Country Control – Improving Privacy Compliance and Supervision", (2002) *Privacy & Informatie*, 257-259

Terstegge, J.H.J., Comment on Article 4(1) Directive in: *Concise European IT Law*, The Hague: Sdu 2007, 39-41

Terwangne, C. and S. Louveaux, "Data protection and online networks", (1997) 13 *Computer Law & Security Report*, 234-246

M.B.J. Thijssen, "Grensoverschrijdend gegevensbeschermingsrecht" (Cross-border data protection law), (2005) *Privacy & Informatie*, 110

G-J Zwenne and Ch. Erents, "Reikwijdte Wbp; enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp", (2009) *Privacy & Informatie*, 60

Papers/Reports/Other Publications

"The Added Value of Private Regulation in an International Word? Towards a Model of the Legitimacy, Effectiveness, Enforcement and Quality of Private Regulation", HiiL May 2008 (www.hiil.org)

"CNIL facilitates the use of outsourcing services performed in France on behalf of non-European companies", dated 15 March 2011 (http://www.cnil.fr/english/news-and-events/news/article/cnil-facilitates-the-use-of-outsourcing-services-performed-in-france-on-behalf-of-non-european-compa/)

Comments of the US Council for International Business (USCIB) for the Review of the EU Data Protection Directive (30 July 2002) (Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/paper/uscib_en.pdf)

"Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments," January 2010 (Available at http://ec.europa/eu/justice/policies/privacy/studies/index_en.htm)

"The Draft Inventory Report", HiiL May 2008 (www.hiil.org)

Kessedjian, C. ,"International Jurisdiction and Foreign Judgments in Civil and Commercial Matters", October 1997, Hague Conference on Private International Law (http://www.hcch.net/upload/wop/jdgm_pd7.pdf)

Kobrin, S.J., "The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance, " *The Wharton School*, Working Paper Series, November 2002

Korff, D., "EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws", Cambridge, September 2002, (Study Contract ETD/2001/B5-3001/A/49)

Korff, D., "New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments" (January 15, 2010). European Commission DG Justice, Freedom and Security Report (http://ssrn.com/abstract=1638949)

Korff, D., New Challenges to Data Protection Study - Country Report: France (May 15, 2010). European Commission DG Justice, Freedom and Security Report (http://ssrn.com/abstract=1638955)

Kuner, C., "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, " *TILT Law & Technology Working Paper* No. 016/2010, October 2010, Version 1.0

Moerel, L., "Privacy without Borders", Het Financieele Dagblad (Dutch Financial Times) 3 April 2003

Moerel, E.M.L., "Transnational Private Regulation of Data Protection", 2009 HiiL Annual Conference on Transnational Private Regulation, June 2010, Dublin (www.privateregulation.eu)

"Verslag van het onderzoek naar gegevensverstrekking door banken aan de Amerikaanse autoriteiten", bijlage bij "Onderzoek naar directe gegevensverstrekking aan de VS en antwoorden op kamervragen inzake SWIFT", nader rapport 27-06- 2007" (www.rijksoverheid.nl)

Reidenberg, J.L., Workshop 4: International issues: international data transfers, applicable law and jurisdiction (European Commission Conference on the Implementation of Directive 95/46/EC, 2002), at 3-4

Vodafone, "Privacy – an evolving challenge", to be found at (http://www.vodafone.com/content/dam/vodafone/about/public_policy/future_ofprivacy/privacy_an_evolving_challenge_update.pdf)

Case Law

European Court of Justice

Case 76/77, *Auditeur du travail v Bernard Dufour, SA Creyf's Interim and SA Creyf's Industrial* [1977] ECR 02485

Case 33/78, *Somafar SA v. Saar-Ferngas AG* [1978] ECR 02183

Case 139/80, *Blanckaert & Willems PVBA v. Luise Trost* [1981] ECR 00819

Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415

Case 168/84 *Bergholz* [1985] ECR 2251

Case C-106/89, *Marleasing SA v. La Comercial Internacional de Alimentacion SA* [1990] ECR I-04135

Case C-64/95 *Konservenfabrik Lubella Friedrich Büker GmbH & Co. KG v, Hauptzollamt Cottbuss* [1996] ECR, I-05105.

Case 21/76 *Bier v. Mines de Potasse d'Alsace* [1976] ECR 1735

Case C-190/95 *ARO Lease v. Inspecteur der Belastingdienst Grote Ondernemingen Amsterdam* [1997] ECR I-4383

Case C-390/96 *Lease Plan Luxemburg v. Belgische Staat* [1998] ECR I-2553

Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971

Case C-281/02 *Owusu* [2005] ECR I-1383

BIBLIOGRAPHY PART II

Books

Ahern, J. and W. Binchy, *The Rome II Regulation on the Law Applicable to Non-contractual Obligations: a new international litigation regime*, Leiden: Koninklijke Brill 2009

Asser/Hartkamp & Sieburg 6-III, *Verbintenissenrecht: Algemeen overeenkomstenrecht*, Deventer: Kluwer 2009, no. 101

Ayres, I. and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford 1992

Baldwin, R. and M. Cave, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford: Oxford University Press 1999

Bennett, C.J. and C.D. Raab, *The Governance of Privacy*, Massachusetts: MIT Press 2006

Bergkamp,L., *European community Law for the New Economy*, Schoten: Intersentia 2003

Besselink, L., F. Pennings and A. Prechal (eds.), *The Eclipse of Legality*, Alphen aan den Rijn: Kluwer Law International 2010

Black, J., *Rules and Regulators*, Oxford: Clarendon Press 2007

Blagescu, M., L. de Las Casas and R. Lloyd, *Pathways to Accountability: The GAP Framework*, London: One World Trust 2005

Blok, P., *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, The Hague: Boom Juridische Uitgevers 2002

Bodiroga-Vukobrat, N., G. Sander and S. Baric (eds.), *Die Offene Methode der Koordinierung in der Europäischen Union (Open Method of Coordination in the European Union)*, Hamburg: Verlag Dr Kovač 2010

Bovens, M., D. Curtin and P. Hart (eds.), *The Real World of EU Accountability: What Deficit?*, Oxford University Press 2010

Bullesbach, A. et. al. (eds.), *Concise European IT Law*, Deventer: Kluwer 2006

Büthe, T. and W. Mattli, *The New Global Rulers:The Privatization of Regulation in the World Economy*, Princeton University Press 2011

Carruthers, J., J.J. Fawcett and P.M. North, *Cheshire, North and Fawcett: Private International Law*, Oxford: Oxford University Press 2008

Castendyk, O., E. Dommering, and A. Scheuer, *European Media Law*, Alphen aan den Rijn: Kluwer Law International 2008

Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Cherednychenko, O., "EU Fundamental Rights, EC Fundamental Freedoms and Private Law," (2006) 1 *European Review of Private Law*

Clapham, A., *Human Rights Obligations of Non-State Actors*, Oxford: Oxford University Press 2006

Conley, J.M. and C.A. Williams, *Global Banks as Global Sustainability regulators: the Equator Principles*, J.L. & Policy Review, forthcoming 2011.

Cuijpers, C.M.K.C., *Privacyrecht of privaatrecht. Een privaatrechtelijk alternatief voor de implementatie van de Europese Privacyrichtlijn (dissertation, University of Tilburg)*, Nijmegen: Wolf Legal Publishers 2004

Dammann, U. and S. Simitis, *EG-Datenschutzrichtlinie*, Berlin: Nomos 1997

De Vos, B.J., *Horizontale werking van grondrechten. Een kritiek*, E.M. Meijers-reeks, Apeldoorn: Maklu Uitgevers 2010

Eijsbouts, A.J.A.J. and J.M. de Jongh et. al., *Maatschappelijk Verantwoord Ondernemen en het Recht, Preadviezen NJV 2010-1*, Deventer: Kluwer 2010

Follesdal, A., R.A. Wessel and V. Wouters (eds.), *Multilevel regulation and the EU, The interplay between global, European and national normative processes*, Leiden: Martinus Neijhof Publishers 2008

Griller, S. and J. Ziller (eds.), *The Lisbon Treaty: EU Constitutionalism without a Constitutional Treaty?* Dordrecht: Springer 2008

Grundmann, S. (ed.), *Constitutional values and European contract law*, Wolters Kluwer 2008

Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights*, D.J. Harris et al.(eds.), Oxford University Press: 2009

Hillier, T., *Sourcebook on Public International Law*, London: Cavendish 1998

Kaczorowska, A., *Public International Law*, 4th ed., New York: Routledge 2010

Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Kuner, C., *European Data Protection Law: Corporate Compliance and Regulation*, Oxford: Oxford University Press 2007

Kuypers, P.H.L.M., *Forumkeuze in het Nederlands internationaal privaatrecht*, Deventer: Kluwer 2008

McBarnet, D., A. Voiculescu and T. Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Moerel, L., B. van Reeken et.al., *Outsourcing, een juridische gids voor de praktijk,* Deventer: Kluwer 2009

Morgan, B. and K. Yeung, *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press 2007

Newman, A.L., *Protectors of Privacy, Regulating Personal Data in the Global Economy*, New York: Cornell University Press 2008

Ottow, A.T., *De Markt Meester? De zoektocht naar nieuwe vormen van toezicht*, The Hague: Boom Juridische Uitgevers 2009

Parker, C., *The Open Corporation: Effective Self-regulation and Democracy*, New York: Cambridge University Press 2001

Plender, R.,*The European Contracts Convention, The Rome Convention on the Choice of Law for Contracts*, Sweet & Maxwell 1991

Prins, J.E.J., *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk*, Leiden: Stichting NJCM-Boekerij 2010

Prins, J.E.J., *Burgers en Hun Privacy: Over Verhouding En Houding Tot Een Ongemakkelijk Bezit*, Leiden: Stichting NJCM-Boekerij 2010

Purtova, N., *Property Rights in Personal Data: a European Perspective* (dissertation Tilburg University), Oisterwijk: BOXpress 2011

Reid, K., *A Practitioner's Guide to the European Convention on Human Rights*, Sweet&Maxwell 2007

Rule, J.B. and G.W. Greenleaf, *Global Privacy Protection: The First Generation*, Cheltenham: Edward Elgar Publishing 2009

Schulz, W. and T. Held, *Regulated self-regulation as a form of modern government. An analysis of case studies from media and telecommunications law*, Luton: University of Luton Press 2004

Schwartz, P.M. and J.R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection*, Charlottesville: MICHIE Law Publishers 1996

Simitis, S. (ed.), *Bundesdatengeschutzgesetz*, Berlin: Nomos 2006

Van Dam, C.C., *Onderneming en mensenrechten* (oratie Utrecht), [2008]

Van Genugten, W., K. Homan, N. Schrijver and P. de Waart, *The United Nations of the Future; Globalization with a Human Face*, Amsterdam: KIT Publishers 2006

Verhey, L. and T. Zwart, *Agencies in European and Comparative Perspective*, Antwerp-Oxford-New York: Intersentia 2003

Articles

Bamberger, K.A. and D.K. Mulligan, "Privacy on the Books and on the Ground," *Stanford Law Review*, Vol. 63, January 2011

Basedow, J., "Freedom to Contract in the European Union," (2008) *European Review of Private Law* 16

Bergelson, V., "It's personal but it is mine? Towards Property Rights in Personal Information" . (2003), *U.C. Davis L. Review*, 379

Bing, J., "Data protection, jurisdiction and the Choice of Law", (1999) *Privacy Law and Policy Reporter* (http://www.austlii.edu.au/au/journals/PLPR/1999/65.html)

Black, J., "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes," (2008) 2 *Regulation & Governance*, at 137-164

Black, J., "The Emergence of Risk Based Regulation and the New Public Management in the UK," (2005) *Public Law*, at 512-549

Black, J., "Forms and Paradoxes of Principles-based Regulation", (2008) 3 *Capital Markets Law Review*, 425-457

Blok, P.J., "Privacybescherming in alle staten" (Privacy protection; a problem everywhere), (2005) *Computerrecht*, at 297-304

Bomhoff, J. and A. Meuwese, "The Meta-Regulation of Transnational Private Regulation," *Journal of Law and Society*, Vol. 38, Number 1, March 2011

Bottomley, S. and A. Forsyth, "The New Corporate law: Employees' Interest," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Brown, D.H. and J.L. Blevins , "The Safe Harbor Agreement between the United States and Europe: A Missed Opportunity to balance the Interests of E-Commerce and Privacy On-Line," *Journal of Broadcasting and Electronic Media* 46, no. 4 (2002)

Brownsword, R., "Consent in Data protection Law," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Burk, D.L., "Comment on 'Should ICT Regulation Be Undertaken at an International Level?'" in: Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Bygrave, L.A. "International Agreements to Protect Personal Data" in: Rule, J.B. and G.W. Greenleaf, *Global Privacy Protection: The First Generation*, Cheltenham: Edward Elgar Publishing 2009

Bygrave, L.A. and D.W. Schartum, "Consent, Proportionality and Collective Power," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Cafaggi, F., "New Foundations of transnational private regulation," *Journal of Law and Society*, 38: 20–49, March 2011

Cafaggi, F., "Preface New Modes of Regulation in Europe: Critical Rethinking of the Recent European Paths", in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Cafaggi, F., "Rethinking Private Regulation," Chapter 1, in: in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Campbell, K. and D. Vick, "Disclosure law and the market for corporate social responsibility," in:
McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Campbell, K. L.A. Gordon, M.P. Loeb and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," (2003) 11 *Journal of Computer Security*, 431-448

Casey, D.K. and C.D. Scott, "The Crystallization of Regulatory Norms," (2011) 1, *Journal of Law and Society*, 76-95 (available at SSRN: http://ssrn.com/abstract=1772396 or doi:10.1111/j.1467-6478.2011.00535)

Chalmers, D., "The Government and Citizenship of Self-Regulation," in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Cuijpers, C., "A Private Law Approach to Privacy; Mandatory Law Obliged?", SCRIPT-ed, Vol. 4, No. 4, September 2007. Available at SSRN: http://ssrn.com/abstract=1090837

Curren, L. and J. Kaye, "Revoking consent: A 'blind spot' in data protection law?" 2010 *Computer Law & Security Review*, 26(3):273 – 283

Curtin, D. and L. Senden, "Public accountability of Transnational Private regulation," in: (2011) 38 *Journal of Law and Society*, 185-211

Daintith, T. and M. Sah, "Privatisation and the Economic neutrality of the Constitution," [1993] Public Law 465

De Hert, P. and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

De Terwangne, C. , 'Is a Global Data Protection Regulatory Model Possible?', in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

de Witte, B., "Legal Instruments and Law-Making in the Lisbon Treaty," in Griller, S. and J. Ziller (eds.), *The Lisbon Treaty: EU Constitutionalism without a Constitutional Treaty?* Dordrecht: Springer 2008

Dorbeck-Jung, B.A., "Challenges to the Legitimacy of international Regulation: The Case of Pharmaceuticals Standardisation," in: Follesdal, A., R.A. Wessel and V. Wouters (eds.),

Multilevel regulation and the EU, The interplay between global, European and national normative processes, Leiden: Martinus Neijhof Publishers 2008

Enneking, L.F.H., "Crossing the Atlantic, The Political and Legal Feasibility of European Foreign Direct Liability Cases," (2009) *The George Washington International Law Review*, vol. 40, at 907 – 910

Eijsbouts, A.J.A.J., "Maatschappelijk (verantwoord) ondernemen: naast, in of met recht", in: Eijsbouts, A.J.A.J. and J.M. de Jongh et. al., *Maatschappelijk Verantwoord Ondernemen en het Recht, Preadviezen NJV 2010-1*, Deventer: Kluwer 2010

Eijsbouts, A.J.A.J., "Elementaire beginselen van Maatschappelijk Verantwoord Ondernemen", in:
Eijsbouts, A.J.A.J. and J.M. de Jongh et. al., *Maatschappelijk Verantwoord Ondernemen en het Recht, Preadviezen NJV 2010-1*, Deventer: Kluwer 2010

Feldman, D. and F. Campbell, "Constitutional Limitations on Privatisation," in: J.W. Bridge (ed.), *Comparative Law facing the 21st century*, London: UKNCCL 2001

Ford, C.L., "New Governance, Compliance, and Principles-based Securities Regulation", (2008) 45 *American business Law Journal*, 1-60

Gilad, S., "It runs in the family: meta-regulation and its siblings", (2010) 4 *Regulation & Governance*, 485-506

Glinski, C., "Corporate codes of conduct: moral or legal obligation?" in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Hosein, G., "Challenges in Privacy Advocacy," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Hartkamp, A.S., "Fundamental Rights, Fundamental Freedoms, and Contract Law", in: Grundmann, S. (ed.), *Constitutional values and European contract law*, Wolters Kluwer 2008

Hustinx, P., "The Role of data Protection Authorities," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Jaya, "Globalization, Law, and the Transformation of Sovereignty: the Emergence of Global Regulatory Governance," (1999) 2 *Indiana Journal of Global Legal Studies*

Joustra, C.A., "Europese richtlijnen en Internationaal privaatrecht (European Directives and Private International Law)," (1999) *Weekblad voor Privaatrecht, Notariaat en Registratie* 6369 at 666

Kagan, R.A. and J.T. Scholz, "The Criminology of the Corporation and Regulatory Enforcement Strategies", in: Hawkins, K. and J. Thomas (eds.), *Enforcing Regulation*, Boston: Kluwer-Nijhoff 1984

Kobrin, S.J., "The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance," *The Wharton School*, Working Paper Series, November 2002

Koops, B.J., M. Lips, S. Nouwt, C. Prins and M. Schellekens, "Should Self-Regulation Be The Starting Point?" in: Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Korff, D., "EC Study on implementation of the Data Protection Directive, Comparative study of national laws," *Human Rights Centre University of Essex*, September 2002

Kotschy, W., "General Rules on the Lawfullness of the Processing of Personal Data," in: Bullesbach, A. et. al. (eds.), *Concise European IT Law*, Deventer: Kluwer 2006

Krawiec, K.D., "Cosmetic Compliance and the Failure of Negotiated Governance", (2003) 81 *Washington University Law Review*, 487 – 544

Kuner, C., "An International Legal Framework for Data Protection: Issues and Prospects," (2009) *Computer Law and Security Review*, 307-317

Kuner, C., "Data Protection Law and International Jurisdiction on the Internet (Part 1)," in (2010) *International Journal of Law and Information Technology*, 176-193

Kuner, C., "The New EU Standard Contractual Clauses For International Data Transfers to Data Processors," *Privacy & Security Law Report*, 19 April 2010

Kuner, C., "Developing an adequate legal framework for international data transfers," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Kuner C, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 176 (Available at SSRN: http://ssrn.com/abstract=1496847)

Kuner, C., "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)", (2010) 18 *International Journal of Law and Information Technology* (Available at SSRN: http://ssrn.com/abstract=1689495)

Lips, M., "Inventory of General ICT Regulatory Starting Points," in Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

McBarnet, D., "Corporate social responsibility beyond law, through law, for law: the new corporate accountability," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

McBarnet, D., and M. Kurkchiyan, "Corporate social responsibility through contractual control? Global supply chains and other regulation," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

McBarnet, D., and P. Schmidt, "Corporate accountability through creative enforcement: human rights, the Alien Torts Claims act and the limits of legal impunity," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

McHarg, A., "The Constitutional Dimension of Self-Regulation", in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Moerel, E.M.L., J. Koeter and N. Jansen, "U.S. Subpoenas and European Data Protection Legislation," in: *US Privacy & Data Security Law Journal*, July 2009, at 649-659

Moerel, E.M.L., "Back 2 Basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?," in: (2008) *Computerrecht*, 81 – 92

Moerel, E.M.L., "Back to basics: when does EU data protection law apply?", (2011) 2 *International Data Privacy Law*, 92-110

Moerel, E.M.L., "The country of origin principle in the E-commerce Directive: the expected 'one stop shop'?", (2001) *Computer Technology Law Report (CTLR)* at 84-90

Moerel, E.M.L., "The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", (2011) 1 *International Data Privacy Law*, 23-41

Muchlinski, P., "Corporate social responsibility and international law: the case of human rights and multinational enterprises," in: McBarnet, Voiculescu, Campbell, *The New*

Corporate Accountability, Corporate Social Responsibility and the Law, Cambridge: Cambridge University Press 2007

Gunningham, N., "Corporate environmental responsibility: the law and the limits of voluntarism," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Hosein, G., 'Challenges in Privacy Advocay', in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Hustinx, P., "The Role of Data Protection Authorities," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Nikoltchev, S., "A European Perspective of Self-Regulation in the Media", in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Nouwt, S., "Towards a Common Approach to Data protection," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Ottow, A. and S. Lavrijssen, "The legality of independent regulatory authorities", in: L. Besselink, F. Pennings & A. Prechal (eds.), *The Eclipse of Legality*, Alphen aan den Rijn: Kluwer Law International 2010

Parker, C., "Meta-regulation: legal accountability for corporate social responsibility," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Perez Asinari, M.V., 'International Aspects of Personal Data Protection: Quo Vadis EU?', M.V. Perez Asinari and P. Palazzi (eds.), *Challenges of Privacy and Data Protection Law* (31 Cahiers du CRID), Bruylant 2008, 381

Poullet, Y., "ICT and Co-Regulation: Towards a New Regulatory Approach?" in: Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Poullet, Y., "Selected comments on themes developed in this volume," in: Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Pounder, C., "Why the APEC Privacy Framework is unlikely to protect privacy," available at http://www.out-law.com/page-8550

Prins, C., "Should ICT Regulation Be Undertaken at an International Level?", in Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Prins, J.E.J., "Burgers in Hun Privacy: Over Verhouding En Houding Tot Een Ongemakklijke Bezit," in: Prins, J.E.J., *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk*, Leiden: Stichting NJCM-Boekerij 2010

Prins, J.E.J., "The Propertization of Personal Data and Identities," *Electronic Journal of Comparative Law*, Vol. 8(3), October 2004

Raab, C. and B.J. Koops, "Privacy Actors, Performances and the Future of privacy Protection," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Rank, W.A.K. and A.J. Haasjes, "Misbruik van de Wbp in civiele procedures tegen financiële instellingen", Tijdschrift voor Financieel Recht 2005-12, at 370-379

Reding, V., "The Upcoming Data Protection Reform for the European Union," *International Data protection and privacy law* (2001) 1 (1)

Retzer, Karin and Joanna Łopatowska, Dealing with Data Breaches in Europe and Beyond, *PLC Cross-border Data Protection Handbook 2011/12*.

Reidenberg, J.R., "Resolving Conflicting International Data Privacy Rules in Cyberspace", *Stanford Law Review* 52 1339-51 (2000)

Rodotà, S., "Data Protection as a Fundamental Right," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Rouvroy, A. and Y. Poullet, "The right to Informational Self-Determination and the Value of Self-Development. Reassessing the Importance of Privacy for Democracy," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

Rubinstein, I., "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes," *NYU School of Law*, Public Law Research Paper No. 10-16, 1 March 2010, available at SSRN: http://ssrn.com/abstract=1510275

Ruggie, J., "Protect, Respect and Remedy: a Framework for Business and Human Rights," *Report of the SRSG on the issue of human rights and transnational corporations and other business enterprises*, 7 April 2008, A/HRC/8/5

Sacconi, L., "Corporate Social Responsibility (CSR) as a Model of 'extended' Corporate Governance: an Explanation Based on the Economic Theories of Social Contract, Reputation,"

in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Schellekens, M., B.J. Koops and C. Prins, "Conclusion", in: Koops, B.J. et. al. (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: TCM Asser Press 2006

Scott, C.D., "Enforcing Consumer Protection Laws", in: Howells, G. et.al. (eds), *Handbook of International Consumer Law and Policy*. Cheltenham: Edward Elgar 2010

Senden, L., "The OMC and its Patch in the European regulatory and constitutional landscape," in: N. Bodiroga-Vukobrat, G. Sander, & S. Baric (Eds.), *Die Offene Methode der Koordinierung in der Europäischen Union (Open Method of Coordination in the European Union)*, 43-68

Senden, L., "Soft Law, Self-Regulation and Co-Regulation in European Law: Where do they meet", (2005) 9.1 *Electronic Journal of Comparative Law* (to be found at www.ejcl.org)

Sinden, A., "Addressing Corporate Environmental Wrongs," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Smith, L.M. and J.L. Smith, "Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?", at 12 (http://www.tamu.edu/)

Strikwerda, L., *Inleiding tot het Nederlands Internationaal privaatrecht*, Deventer: Kluwer 2008.

Suchman, M., "Managing Legitimacy: Strategic and Institutional Approaches", (1995) 3 *Academy of Management Review*, at 571- 610.

Sunstein. C., "Problems with Rules", (1995) 83 *California Law Review*, 953-1026

Swire, P., "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," (1998) 32 *International Lawyer* 991, 1007

Swire, P.P. "Elephants and Mice Revisited: law and Choice of Law on the Internet," (2005) 153 *University of Pensylvania Law Review*, 1975-2001

Teme, O., "For Privacy, The European Commission Must Be Innovative", Center for Democracy & Technology, 28 February 2011 (to be found at http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative)

Trudel, P., "Privacy Protection on the Internet," in: Gutwirth, S. et. al. (eds.), *Reinventing Data Protection?*, Dordrecht: Springer 2009

van Genugten, W., "Handhaving van Wereldrecht, een kritische inspectie van valkuilen en dilemma's," (2010) *Nederlands Juristenblad*, 85(1), 44-46

Van Heesen-Laclé, Z.D. and A.C.M. Meuwese, "The legal framework for self-regulation in the Netherlands", (2007) 2 *Utrecht Law Review* (to be found at http://ssrn.com/abstract=1083677)

Meerten , H. van and A. Ottow, "The proposals for the European Supervisory Authorities: the right (legal) way forward?", (2010) 1 *Tijdschrift voor Financieel Recht* (Available at SSRN: http://ssrn.com/abstract=1517371)

Van Ooik, R.H., "The Growing Importance of Agencies in the EU: Shifting Governance and the Institutional Balance", in Curtin, D.M. and R.A. Wessel (eds.), *Good governance and the European Union: Reflections on Concepts, Institutions and Substance*, Antwerp: Intersentia 2005

van den Bergen, A.J.E. "'De Wet bescherming persoonsgegevens in de financiële procespraktijk'", in: Tijdschrift voor Financieel Recht 2005-10, at 296- 306.

Viergever, L., "Privacy in the Clouds," (2010) *Tijdschrift voor Internetrecht*, 78–86

Voermans, W.J.M., "Is the European Legislator after Lisbon a Real Legislature?" (December 15, 2009), (2009) 50 *Legislacao Cadernos de Ciencia de Legislacao*, at 391-413 (available at SSRN: http://ssrn.com/abstract=1347959)

Vogel, D., "Private Global Business Regulation", (2008) 11 *Annu. Rev. Polit. Sci*, 261–82

Voiculescu, A., "Green paper to new uses of human rights instruments," in: McBarnet, Voiculescu, Campbell, *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge: Cambridge University Press 2007

Wessel, R. and J. Wouters, "The Phenomenon of Multilevel Regulation: Interactions between Global, EU and National Regulatory Spheres," in: Follesdal, A., R.A. Wessel and V. Wouters (eds.) *Multilevel regulation and the EU, The interplay between global, European and national normative processes*, Leiden: Martinus Neijhof Publishers 2008

Winter, J.W., "Geen regels maar best practices," in: Van Hassel, K.M. en M.P. Nieuwe Weme (eds.), *Willems' wegen, Opstellen aangeboden aan prof.mr. J.H.M. Willems*, Deventer: Kluwer 2010

Wugmeister, M., K. Retzer and C. Rich, "Global solution for cross-border data transfers: making the case for corporate privacy rules," (2007) *Georgetown Journal of International Law*, Vol. 38

Yilmaz, Y., "Private Regulation: a Real Alternative for Regulatory Reform," *CATO Policy Analysis* No. 303, 20 April 1998

Ziller, J., Constitutional Boundaries of Self-Regulation, in: Cavaggi, F. (ed.), *Reframing Self-Regulation in European Private Law*, Deventer: Kluwer Law International 2006

Papers/Reports/Other Publications

Black J., "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", LSE Law, Society and Economy Working Papers 2/2008 London School of Economics and Political Science Law Department (to be found at www.lse.ac.uk/collections/law/wps/wps.htmm)

Black, J., Legitimacy and the Competition for Regulatory Share, LSE Working Paper 14/2009 (2009)

Bradshaw, Simon, Millard, Christopher and Walden, Ian, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010
(available at SSRN: http://ssrn.com/abstract=1662374)

Cafaggi, F., "Private Regulation, Supply Chain and Contractual Networks: The case of Food Safety," EUI Working Papers RSCAS 2010/10

Centre for Information Policy Leadership, "Demonstrating and Measuring Accountability, A Discussion Document, Accountability Phase II – The Paris Project," October 2010 (to be found at www.information policy centre.com)

Comission Brouwer-Korf (2009) Gewoon Doen. Beschermen van veiligheid en persoonlijke levenssfeer, Rapport aan de ministers van justitie en Binnenlandse zaken, De Haag (tob e found at
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/01/22/rapport-gewoon-doen-beschermen-van-veiligheid-en-persoonlijke-levenssfeer.html)

Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework* (June 2004) (available at www.bis.org)

Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change, A

proposed Framework for Business and Policymakers", December 2010 (to be found at www.ftc.gov/os/2010/12/101201privacyreport.pdf)

"FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network. Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data", press release dated 30 March 2011 (to be found at http://ftc.gov/opa/2011/03/google.shtm)

Galway project and Centre for Information Policy leadership, "Data Protection Accountability: The essential Elements, A document for Discussion", 2009 (to be found at <www.hunton.com>)

Gellman, R., "Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete", March 2002 (available at www.epic.org/reports/dmfprivacy.html#2)

Giuliano, M., and P. Lagarde, Report on the Convention on the law applicable to contractual obligations, *Official Journal of the European Communities* C 282 31.10.1980 P.0001-0050

Hampton, P., Reducing Administrative Burdens, Effective Implementation and Enforcement (HM Treasury, 2004)

HiiL 2008, "The added value of private regulation in an international world? Towards a model of the legitimacy, effectiveness, enforcement and quality of private regulation," HiiL 2007 – 2008 (to be found at www.hiil.org)

Joerges, C., "Rethinking European Law's Supremacy," *EUI Working Papers* 2005/12 (2005)

Korff, D., "New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments" (January 15, 2010). European Commission DG Justice, Freedom and Security Report (http://ssrn.com/abstract=1638949)

Kuner, C., "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future," *TILT Law & Technology Working Paper* No. 016/2010, October 2010, Version 1.0

Kroes, N., "Towards a European Cloud Computing Strategy", speech for World Economic Forum Davos, 27 January 2011, available at http://europa.eu

Mandelkern Group on Better Regulation: Final Report, 13 November 2001 (available at http://ec.europa.eu/governance/better_regulation/documents/mandelkern_report.pdf)

Moerel, L., "Privacy without Borders", Het Financieele Dagblad (Dutch Financial Times) 3 April 2003

Pollman, E., Reconceiving Corporate Personhood (December 31, 2010) (available at SSRN: http://ssrn.com/abstract=1732910)

Privacy International, "European Privacy and Human Rights 2010", to be found at www.privacyinternational.org/ephr

Privacy International, "A race to the Bottom – Privacy Ranks of Internet Service Providers", to be found at www.privacy.international.org

Report i-Overheid of the Wetenschappelijk Raad vooor het Regeringsbeleid (March 2011) (available at http://www.binnenlandsbestuur.nl/Uploads/Files/Document/Ioverheid.pdf.)

The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe, Brussels, 4 November 2002 (to be found at http://ec.europa.eu/internal_market/company/modern/index_en.htm)

Ruggie, J., Protect, Respect and Remedy: a Framework for Business and Human Rights, 7 April 2008, A/HRC/8/5 (to be found at www.ohchr.org)

Scott, C.D., "Enforcing Consumer Protection Laws" (July 30, 2009). UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 15/2009 (http://ssrn.com/abstract=1441256)

Scott, C.D., "Regulatory Governance and the Challenge of Constitutionalism," EUI Working Paper RSCAS 2010/07

Case Law

European Court of Justice

Case 9/56, *Meroni & Co. Industrie Metallurgiche SpA v High Authority* [1958] ECR 133

Case 10/56 Meroni & Co., *Industrie Metallurgiche, S.A.S., v High Authority of the European Coal and Steel Community* [1958] ECR.

Case C-22/70 *Commission v Council* [1971] ECR 263

Case C-36/74, *Walrave v. Association Union Cycliste Internationale*, 1974 ECR 1405

Case C-150/77 *Bertrand* [1978] ECR 1431

Case C-201/82 *Gerling* [1983] ECR 2503

Case C-71/83 *Tilly Russ* [1984] ECR 2417

Case C-9/87 *Arcado* [1988] ECR 1988 01539

Joined Cases C-90/90 and C- 91/90 *Jean Neu v Sécrétaire d'Etat à l'Agriculture* [1991] ECR I-3617 142

Case C-26/91 *Handte* [1992] ECR I-3967

Case C-89/91 *Shearson Lehman Hutton* [1993] ECR I-139

Case C-269/95 *Benincasa* [1997] ECR I-3767

Case C-99/96 *Mietz* [1999] ECR I-2277

Case C-51/97 *Réunion européenne and Others* [1998] ECR I-6534

Case C-387/98 *Coreck Maritime* [2000] ECR I-9337

Case C-238/99 *Limburgse Vinyl Maatschappij (LVM) v Commission and Others* [2002] ECR I-8618

Case C-94/00 *Roquette Frères SA v. D-G de la concurrence, de la consommation et de la répression des frauds* [2002] ECR I-9039

Case C-96/00 *Gabriel* [2002] ECR I-6367

Case C-334/00 *Tacconi* [2002] ECR I- 7357

Joined Cases C-465/00, C-138, C-139/01 *Österreichischer Rundfunk/Neukomm* [2003] ECR I-04989

Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971

Case C-27/02 *Engler* [2005] ECR I-481

Case C-265/02 *Frahuil* [2004] ECR I-0000

Case C-281/02 *Owusu* [2005] ECR I-1383

Case C-180/06 *Ilsinger*, [2009] OJ C153/3

Case C-275/06 *Promusicae* [2008] ECR I-271

Case C-518/07 *Commission v. Germany* [2010] OJ C 113

International Court of Justice

France v Turkey (SS Lotus) 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7)

European Court of Human Rights

I v. Finland, Application no. 20511/03, ECHR 17 July 2008

Niemietz v. Germany, 72/1991/324/396, ECHR 16 December 1992

Société Colas Est v France, Application no. 37971/97, Reports of Judgments and Decisions 2002-III

Von Hannover v Germany Application no. 59320/00, ECHR 24 June 2004

X. and Y. v. The Netherlands, Application no. 8978/80, ECHR 26 March 1985

US Supreme Court

Santa Clara Co. v. Southern Pacific Railroad, 118 U.S. 394 (1886)

Federal Communications Commission v. AT&T Inc., 562 U.S.(2011)

Supreme Court of California

Marc Kasky v. Nike, et al, 2 Cal. Daily Op. Serv. 3790, 2002 Daily Journal D.A.R. 4757.