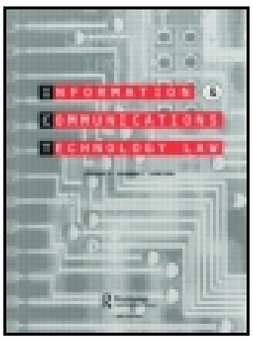

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: http://www.tandfonline.com/loi/cict20

Cross-border issues under EU data protection law with regards to personal data protection

Shakila Bu-Pasha

To cite this article: Shakila Bu-Pasha (2017): Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, DOI: 10.1080/13600834.2017.1330740

To link to this article: http://dx.doi.org/10.1080/13600834.2017.1330740

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 24 May 2017.

Submit your article to this journal

Article views: 349

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=cict20

Download by: [University of Helsinki] **Date:** 01 September 2017, At: 03:39

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 2017
https://doi.org/10.1080/13600834.2017.1330740

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Cross-border issues under EU data protection law with regards to personal data protection

Shakila Bu-Pasha

Faculty of Law, University of Helsinki, Helsinki, Finland

ABSTRACT

We are living in an inter-connected, global digital society where the services of different operating systems are universal in nature, but many Internet activities are still being tackled by national laws and regulations. A long-existing question is which law is applicable in cases of Internet activities because the online world does not have any physical boundaries. How the European Union (EU) approaches this duality has become a concern for data protection laws. By analysing some recent Court of Justice of the European Union case laws, this article seeks to discover how the EU data protection law tackles disputes involving transnational issues online, which includes its extra-territorial application and cross-border data transfers. The article also indicates that there is an enormous gap between legislation and practice.

KEYWORDS

EU data protection law; GDPR; extra-territorial jurisdiction; data transfer; EU-US Privacy Shield

Downloaded by [University of Helsinki] at 03:39 01 September 2017

1. Introduction

Much like cyberspace, communication is nowadays of cross-border nature. The Internet, including well-known websites and social media platforms such as Facebook, Twitter, Wikipedia and YouTube, is the prime medium for communication among people around the world. It is difficult to find any undoubtedly accepted international legal instrument to safeguard privacy and data protection of Internet users across the world although this area of law has become crucial for worldwide communication.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (CETS No.: 108) is regarded as the first and only legally binding international instrument that, along with the European Union (EU) Member States, is accessible by non-European as well as non-member countries of the Council of Europe that explicitly deals with data protection, information privacy and personal data considering gradual technological development.[1] Provisions on cross-border personal data flows to and from non-Member States were introduced by the Additional Protocol to Convention 108 that was adopted in 2001, which encourages the fair and legitimate collection, processing and use of personal data. In reality, all contracting parties to the Convention except

CONTACT Shakila Bu-Pasha shakila.bu-pasha@helsinki.fi
All websites were accessed on 15 March 2017.
[1]Jaap Zevenbergen, 'European Privacy Law and Its Effect on Location Information' (Location Privacy Workshop, 5–7 August 2004) <http://goo.gl/D2Rihm>.

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

Uruguay are members of the Council of Europe, turning it far from 'international' in practice.[2]

The Organisation for Economic Co-operation and Development (OECD) Privacy Framework states in its point 16: 'A data controller remains accountable for personal data under its control without regard to the location of the data'.[3] But this framework is a non-binding instrument.[4]

The Data Protection Directive (DPD) of 1995[5] is claimed to be the first and only effective international data protection legal instrument through which national laws are authorised to be applied in particular cases of data processing.[6] Scholars in the related field are expecting that the latest EU data protection legislation– the General Data Protection Regulation[7] (GDPR) is going to be the most influential regional legal instrument in data protection law with universal proximity that will encounter more international acceptance.

Because of the diffusive and universal nature of the Internet,[8] the general privacy policies and end-user license agreements of different websites, mobile applications and operating systems are also the same across borders. At the same time, aside from a very few international and regional legal instruments, data protection laws are mostly determined by national parliaments.

Under the general principle of territoriality, state jurisdiction to enforce a law includes the territory upon which the state can exercise sovereign power. The extra-territorial application of national law is possible only if any international law permits this where the country in question is a Member State of that particular international law.[9] With regard to data protection law, now it is quite challenging to adjust present extra-territorial issues online against traditional principles of territoriality.

Transnational data flow has become inevitable with the expansion of the Internet. Provisions of the DPD were outlined in order to protect the personal data of EU residents prescribing the limits of activities of the EU-based controllers. Transferring data from the EU to third countries means that a data controller within the EU first collects and then transfers data to the controller or processor of the third country. Thus, the legal aspects of transferring data to third countries involve some practical complexities that require two different actors in both sides as data controller and controller or processor.[10] The first controller is undoubtedly bound to follow the provisions of the EU data protection law, but disputes can arise regarding the applicable law for the latter controller and/or processor.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

[2]Council of Europe/European Court of Human Rights, European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (2014) 16, 17; Chart of Signatures and Ratifications of Treaty 108 <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=BOL2XLFM>.

[3]OECD, *The OECD Privacy Framework* (2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[4]Elena Perotti, 'The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation' (2015) 29 <http://www.academia.edu/19648451/The_European_Ruling_on_the_Right_to_be_Forgotten_and_its_extra-EU_implementation>.

[5]Directive 95/46/EC of the European Parliament and of 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, OJ L281/31.

[6]Lee A. Bygrave, 'Data Privacy Law: An International Perspective' (Oxford University Press, 2014), 63.

[7]Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016) OJ L119/1.

[8]Anabela Susana De Sousa Gonçalves, 'The Extraterritorial Application of the EU Directive on Data Protection' Spanish Yearbook of International Law (2015) 195.

[9]Perotti (n 4) 26.

[10]Aleksandra Kuczerawy, 'Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS', 2014, 80 <https://hal.inria.fr/hal-01061136/document>.

However, the GDPR attempts to govern both actors with some improved obligations when a connection to the EU exists.

A general principle is that the law of the country from which the data are collected is applicable to the controller until the actual transfer takes place. Thus, it is the legal obligation of the regional branches within the EU of any parent company to follow the EU data protection law.[11] For example, the social networking platform Facebook was originated and based in the United States, but now is popular worldwide. Normally, large amounts of users' personal (including location) data are processed via social networking websites/applications such as Facebook used in smart devices.[12] A big concern is how the EU data protection law would be applied in cases of data processing by Facebook. As per the definition under Article 2(e) DPD and Article 4(8) GDPR, by processing individual personal data, Facebook becomes the 'data processor'. Because technical decisions are taken in the head office, including 'the purposes and means' of the data processing, it can be said that EU nationals' data are processed by a US-based data controller [under Article 2(d) DPD and Article 4(7) GDPR].[13]

In this connection, it is relevant to mention that Facebook attempted to escape EU national laws by reference to Irish law only terming Facebook Ireland as data controller by fulfilling the 'establishment' test under Article 4(1)(a) DPD. But the High Court of Berlin disagreed with this argument in 2014.[14] Facebook continued the same argument that because Facebook's European headquarters is located in Dublin, Ireland, Facebook is only bound to comply with the national laws of Ireland.[15] The President of the Brussels Court of First Instance on November 2015 adopted the recommendation made by the Privacy Commission of Belgium on May 2015 and held that Facebook, Inc. is the data controller, and Facebook Ireland is not the data controller because it is not competent and independent to determine 'the purposes and means of the processing of personal data'.[16] Thus, Facebook Ireland and Facebook Belgium are only subsidiaries of Facebook, Inc.[17]

The head offices of many multinational technology companies are situated in the United States, and many of those do not have any regional offices within the EU. In these cases, it is technically possible that the US-based companies can directly obtain data from their worldwide users. In the absence of any intermediary or controller in the EU, complexities may arise to define 'data transfer'. In other words, when EU users send their personal data to the United States without a transferring authority, and the US-based technology companies process those data, whether the issue falls within the ambit of international application of the EU data protection law has become a crucial

[11]Kuczerawy (n 10) 80; European Commission, *Protection of Personal Data* <http://ec.europa.eu/justice/data-protection/>.
[12]Jeroen van den Hoven and others, 'Privacy and Information Technology' in Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2016 Edition) <https://plato.stanford.edu/archives/spr2016/entries/it-privacy/>.
[13]Kuczerawy (n 10) 78, 79.
[14]Tim Van Canneyt, 'The Belgian Facebook Recommendation: How the Nomination of a Single EU Data Controller Is Under Fire' *Privacy, Security and Information Law* (20 May 2015) <http://privacylawblog.fieldfisher.com/2015/the-belgian-facebook-recommendation-how-the-nomination-of-a-single-eu-data-controller-is-under-fire>.
[15]Columbia University, Global Freedom of Expression, *Belgian Privacy Commission v. Facebook* <https://globalfreedomofexpression.columbia.edu/cases/belgian-privacy-commission-v-facebook/>.
[16]*Belgian Privacy Commission v. Facebook*, Recommendation no. 04/2015 of 13 May 2015, Date of Decision: 9 November 2015; Columbia University (n 15).
[17]Canneyt (n 14); Marcus Evans and Jay Modrall, 'Belgian Court Orders Facebook to Stop Tracking Non-members, Rejects FB's Assertion of Lack of Jurisdiction', Data Protection Report (23 November 2015) <http://www.dataprotectionreport.com/2015/11/belgian-court-orders-facebook-to-stop-tracking-non-members-rejects-fbs-assertion-of-lack-of-jurisdiction/>.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

question. Multinational technology companies have become so powerful that they are capable enough to collect, transfer, and then process personal data from the online activities of Internet users worldwide. Whether or not an actual 'transfer' takes place within the meaning of the provisions of the DPD and GDPR, the result is the same (i.e. the US company processes the personal data of EU users).[18] However, it was expressed in the Lindqvist case[19] that merely uploading personal data to the Internet would not constitute a 'transfer', although that data could be accessed from any part of the world.[20]

Taking into account these dimensions, this article discusses cross-border issues by including two aspects: (1) extra-territorial application of the EU data protection law and (2) data transfers from the EU to the outside. The judgement of the renowned Google Spain case[21] strengthens the scope of applicability of the EU data protection law concerning extra-territorial jurisdiction and the Schrems case[22] ensures both the extra-territorial applicability and lawful transfers of personal data under the EU data protection law. Both cases have fostered subsequent developments in the EU data protection law with regards to personal data protection. Because of some unforeseen consequences of the digital environment with the passage of time, it appeared from these judgements that the provisions under the EU data protection law may be interpreted taking into account the consequences and realities of data processing. Although the GDPR is eager to apply from May 2018 [Art. 99(2) GDPR] repealing the DPD, discussing the DPD is inevitable because the judgements of the two cases were based on the provisions of the DPD. Without analysing them, the present developments (GDPR, Privacy Shield) would be incomplete.

Therefore, the next chapters of the paper are arranged as follows. Alongside an analysis of the related provisions of the DPD, Chapter II consists of discussions on Google Spain and subsequent development in the GDPR. In a similar order the Schrems case is discussed in Chapter III, followed by an analysis of the EU-US Privacy Shield in Chapter IV. For further clarification, Chapter II is relevant before the transfer of personal data outside the EU region, Chapter III discusses aspects both before and after the transfer happens, and Chapter IV is particularly focused on post-transfer concerns.

2. Extra-territorial jurisdiction

Article 4 of the DPD provides legal basis against 'conflict of laws'[23] that clarifies which national law of the Member States applies 'in the context of the activities of an establishment' [Art. 4(1)(a)], or if an equipment is used [Art. 4(1)(c)] within the territory of the said Member State in order to process personal data, provided that national laws are not arranged in conflict with the DPD. This provision is particularly relevant in processing data before it is transferred to third countries, irrespective of an establishment located within the EU or use of equipment within the EU by some association situated outside

[18]Kuczerawy (n 10) 80, 81.
[19]*Bodil Lindqvist v Åklagarkammaren i Jönköping* (CJEU, 6 November 2003) C-101/01, ECLI:EU:C:2002:513.
[20]Mark Watts, *The Bodil Lindqvist Case: ECJ Rules on Publishing Personal Data on the Internet* (Bristows, 17 November 2003) <http://www.bristows.com/news-and-publications/articles/the-bodil-lindqvist-case-ecj-rules-on-publishing-personal-data-on-the-internet/#nogo>.
[21]*Google Spain et al. v AEPD, Costeja Gonzales*, C-131/12 (CJEU, 13 May 2014) ECLI:EU:C:2014:317.
[22]*Maximillian Schrems v Data Protection Commissioner, Ireland*, C-362/14 (CJEU, 6 October 2015) ECLI:EU:C:2015:650.
[23]Conflict of laws arises where different jurisdictions provide different provisions on a same subject matter, and it becomes essential to determine the applicable law <http://www.lectlaw.com/def/c278.htm>.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

of the EU.[24] Article 4, in connection to territorial applicability and enforceability of the DPD, is somewhat complex and keeps scope for several interpretations, especially in determining an equipment under Article 4(1)(c) of the DPD.[25]

2.1. Google Spain case

Spanish citizen and lawyer Mario Costeja González filed a complaint with the national Data Protection Agency of Spain (AEPD) against the Spanish newspaper *La Vanguardia* and Google Spain and Google Inc. in March 2010.[26] He alleged that his right to privacy as well as 'right to be forgotten' was infringed by making searchable on Google the news published in *La Vanguardia* regarding an already resolved issue of judicial proceeding endured by him about 12 years ago concerning recovery of debt by forced sale of property, which he claimed 'entirely irrelevant'.[27] The complainant requested the defendants to remove or make inaccessible his personal information with offending contents.[28]

The AEPD did not find the *La Vanguardia* guilty because it published the news lawfully in accordance with a government order.[29] However, Google Spain and Google Inc. were held liable for processing personal data and were requested to remove such data from search results. By prohibiting access to particular data, Internet search engines are thereby held subject to the EU data protection laws.[30] Google appealed against the decision to the National High Court of Spain, which referred it to the Court of Justice of the European Union (CJEU). The CJEU issued its judgement in May 2014, finding Google as 'controller' under Article 2(d), and its activities were classified as 'processing of personal data' under Article 2(b) of the DPD.[31]

By finding Google Spain as an 'establishment' of Google Inc. under Article 4(1)(a) and within the meaning of Recital 19 of the DPD, the CJEU found them 'inextricably linked' and thereby permitted interpretation of the DPD with extra-territorial jurisdiction.[32] Personal data processing was carried out 'in the context of an establishment of the controller' in the EU where a branch or subsidiary promoting and selling advertising space was targeting the inhabitants of a Member State (ruling, point 2).

2.2. Influence of the case and subsequent developments

The most important finding for the topic in this judgement concerns the territorial scope of the DPD and reach of national laws of the EU Member States outside national boundaries. It is now established that Article 4(1)(a) can be applied with extra-territorial

[24]Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision* (13 April 2016) 12.
[25]Kuczerawy (n 10) 84.
[26]Perotti (n 4) 4.
[27]Perotti (n 4) 4.
[28]European Commission, *Factsheet on the 'Right to be Forgotten' Ruling (C-131/12)* <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.
[29]Columbia University, Global Freedom of Expression, *Google Spain SL v. Agencia Española de Protección de Datos* <https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>.
[30]Ibid; *Google Spain SL v Agencia Española de Protección de Datos* (*5RB: Media and Entertainment Law*, 20 February 2017) <http://www.5rb.com/case/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/>.
[31]Perotti (n 4) 6.
[32]Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the EU's "Right to be Forgotten"' (Working Paper No. 152, March 2015) 8, 9.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

jurisdiction. Accordingly, provisions of the EU data protection law will apply in the case of search engine operations through a branch or a divisional office within any Member State of the EU, even if the main company originated and is based outside of the EU.[33] Hence, in practical terms, the DPD (and nowadays the GDPR) can be interpreted as not only a regional but also an international data protection law.[34]

Thus, the territorial scope of the EU data protection law is described broadly in the *Google Spain* case. Through this judgement, national legislation and its jurisdiction to the extra-European activity has been extended in practice.[35] Perhaps the court took this broad approach considering the tremendous and boundless spread of the virtual world and to fit that spread in the existing data protection law, which was adopted in the 1990s when the legislators could not foresee the probable influence of the Internet in the future.[36]

In last several years, modern technologies have evolved drastically. With the borderless nature and wide-spread use of the Internet, the GDPR has been developed to embrace the consequences brought by the new digital environment and for the protection of fundamental rights within such an environment. The most important change that the GDPR brings with regulatory landscape is regarding the personal data protection of EU residents, which binds all companies or operating systems that process EU residents' personal data, irrespective of the location of the company or operating system in question. The GDPR extends, modernises and clarifies the jurisdictional scope of the EU data protection law.[37] With the phrase 'offering goods or services' stated in different provisions of the GDPR, it binds the companies operating from outside the EU that provide services for the consumers in the EU and process EU data subjects' data.[38]

Article 3 and Recital 22 of the GDPR clarify the territorial scope so that when controllers or processors process personal data with any of their establishments in the EU, the GDPR will be applicable 'regardless of whether the processing itself takes place within the Union' or not. It is a change in the data protection law that, with the GDPR, the relevance of the location of the equipment is replaced by a focus on people in the EU. The GDPR applies to processing in connection with the activities of an establishment in the EU regardless of where the processing happens (e.g. cloud storage abroad).[39]

The enforcement of Article 4(1)(c) of the DPD is not very easy in practice because of the ambiguity in determining what constitutes 'equipment'. Article 29 Data Protection Working Party (A29WP) suggested to apply Article 4(1)(c) in concrete cases for example, only when it is reasonable and necessary.[40] The philosophy behind such an approach may be that the users can get the feeling of personal data protection and privacy under their own national legislation in reasonable circumstances. On the other hand, it may not be wise to expect

[33] *Factsheet on the 'Right to be Forgotten Ruling'* (n 28).
[34] Article 29 Data Protection Working Party, *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* (30 May 2002) 3–12.
[35] Perotti (n 4) 14.
[36] Perotti (n 4) 35.
[37] 'GDPR Key Changes: An Overview of the Main Changes Under GPDR and How They Differ from the Previous Directive' (*EU GDPR Portal*) <http://www.eugdpr.org/key-changes.html>.
[38] Allen and Overy, 'The EU General Data Protection Regulation' (2016) 3 <http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>.
[39] Eduardo Ustaran (eds), 'Future-proofing Privacy: A Guide to Preparing for the EU Data Protection Regulation' (Hogan Lovells, June 2015) 8, 9.
[40] A29WP (*Non-EU Based Web Sites*) (n 34) p. 9.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

legal treatment from a third country except with a concrete ground. In case of contradiction between national law of EU Member States and other international laws that are not only concerned about the EU but also the whole world, a matter of big debate is how the territoriality principle would be applied and whether to prefer national law over international law would be undermining for the international law.[41]

Overcoming such ambiguity is attempted with a new and simple test introduced by the GDPR. The GDPR will be applicable to the activities of the data controller or processor not established within the EU territory, if goods or services are offered to data subjects or their behaviour is monitored within the EU [Art. 3 (2), Recital 23 GDPR]. In such a case, if the controllers or processors are established outside the EU region, they are required to appoint representatives in the Union or more specifically, in the concerned Member State (Art. 27, Recital 80).[42]

Downloaded by [University of Helsinki] at 03:39 01 September 2017

3. Cross-border data transfers

Article 25(1) of the DPD states that Member States permit transfer of personal data for the purpose of data processing only if 'an adequate level of protection' is ensured by the third country. According to Article 25(2), there is no exact standard to assess such adequacy, but it could be assessed considering the facts and circumstances related to the data transfer operation/s, including the nature, purpose and duration of data processing; the concerned countries to and from where the data would be transferred; and existing legal systems of those countries.

Article 26(1) of the DPD provides some specific circumstances of derogations from the requirement of adequate protection of data under Article 25. Those circumstances are sketched in a way where the threat to privacy rights of the data subject is comparatively low or in order to safeguard other interests or public interests that are more important than the right to privacy of the data subject.[43] If a data subject gives unambiguous consent, the transfer of personal data without ensuring the adequate protection may take place [Art. 26(1)(a)]. For the performance of a contract between the data subject and controller [Art. 26(1)(b)] or between controller and third party for the interest of the data subject [Art. 26(1)(c)], on the ground of public interest or legal requirements [Art. 26(1)(d)] or for the protection of the data subject's vital interest [Art. 26(1)(e)], the adequacy requirement can be exempted. The scope of these exemptions may seem wide, but to apply them the 'necessity test' is required in order to limit the scope.[44]

The requirement of ensuring an adequate level of protection might be exempted under Article 26(2) of the DPD by virtue of which Member States are authorised to transfer data to third countries where 'adequate safeguards' are offered by the controller for the protection of individuals' privacy and fundamental rights, particularly resulting from contractual clauses. It should be noted that when a general principle permits derogations, that should be applied restrictively.[45]

[41]Kuczerawy (n 10) 84.
[42]Hunton & Williams, 'The EU General Data Protection Regulation: A Guide for In-house Lawyers' (Hunton & Williams, October 2016) 10.
[43]Article 29 Data Protection Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (24 July 1998) 24.
[44]A29WP, *Transfers of Personal Data* (n 43) 24.
[45]A29WP, *Transfers of Personal Data* (n 43) 15.

In this context, discussing the Safe Harbour Agreement[46] and related dispute is extremely important. The Safe Harbour Agreement, which allowed EU citizens' data transfer from EU to the United States, was declared invalid by the CJEU in *Maximillian Schrems v Data Protection Commissioner* for a number of reasons, as discussed below.[47]

3.1. The Schrems case

Austrian national Maximillian Schrems has used Facebook since 2008. He brought a complaint to the Data Protection Commissioner of Ireland that Facebook transferred his data from Facebook's Irish servers to the United States, based on the disclosures by Edward Snowden in 2013 of the surveillance actions by the US intelligence agency. Thereby Schrems claimed that the requirement to ensure adequate data protection under EU law failed.[48] The Irish Data Protection Agency dismissed the claim, stating that adequate protection was ensured under the Safe Harbour Agreement.[49]

The case was then submitted to the High Court of Ireland and its evaluation was subsequently accepted by the CJEU.[50] However, the CJEU declared the Safe Harbour Decision invalid and delivered some important findings along with the cross-border issues.

It was expressed that the Safe Harbour Agreement was not meant to reduce, interfere or eliminate the authority of national data protection agencies under the DPD or Charter of Fundamental Rights (CFR) of the EU.[51] The adequacy of data protection in third countries under Article 25(1) could not be ensured if any kind of prejudice occurred to the EU Member States' national laws framed 'pursuant to' the provisions of the DPD. The CJEU held that before determining such adequacy, the European Commission was supposed to be confirmed that the domestic law of the third country (i.e. US domestic law) or its international commitments protect the right to the protection of personal data which should be 'essentially equivalent' to that as guaranteed under the DPD and CFR.[52] But the Commission with its Decision of 2000,[53] did not explore such legal background and only explored the Safe Harbour scheme.[54]

The court found that the US public authorities were kept immune from the applicability of the Safe Harbour scheme; rather, the scheme was meant to apply to the US-owned undertakings.[55] The court ruled:

[46]Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC 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 (OJ 2000 L215).
[47]Samuel Gibbs, 'What Is 'safe harbour' and Why Did the EUCJ Just Declare It Invalid?' *The Guardian* (6 October 2015) <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>.
[48]Court of Justice of the European Union, Press Release No. 117/15 (Luxembourg, 6 October 2015).
[49]Martin A. Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research Service, 19 May 2016) 6.
[50]Thomas Claburn, 'Safe Harbor Fails, European Court Rules' *InformationWeek* (19 May 2016) <http://www.informationweek.com/government/cybersecurity/safe-harbor-fails-european-court-rules/d/d-id/1322509>.
[51]Weiss and Archick (n 49) 7.
[52]Sidley, 'Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States' (January 2016) 9, 10 <http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf>; Weiss and Archick (n 49) 7.
[53]Commission Decision 2000/520/EC (n 46).
[54]Press Release No. 117/15 (n 48).
[55]Press Release No. 117/15 (n 48).

Downloaded by [University of Helsinki] at 03:39 01 September 2017

> Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.[56]

Thus, the US law enforcement requirements, including assurance of national security and public interest, received preference over the Safe Harbour frame, and in case of any conflict between them, the US public authorities would prevail, allowing the US undertakings to ignore the Safe Harbour principles.[57] Thereby, through the Safe Harbour Agreement, the US authority became capable of interfering with the personal data that had been transferred from the EU to the United States. US law does not provide any provision to limit such interference and, thereby, could cause interference in the right to respect for one's private life.[58]

The court also found that with the Safe Harbour project, the power of national courts in the EU was somehow narrowed to decide on the fundamental right to privacy upon an individual's petition, which the European Commission is not authorised to do. As a result of this judgement, the supervisory authority of Ireland becomes competent to decide on the complaint of Maximillian Schrems.[59]

3.2. Consequence of the judgement on cross-border issues

The Schrems case is very important to ensure protection of personal data when the matter involves cross-border issues in connection to the EU data protection law. The judgement of this case provides strong grounds to interpret the EU data protection law in the EU users' favour to protect personal data and privacy even outside EU the region.

Even before this judgement A29WP expressed that, Article 4 of the DPD should not be affected by the Safe Harbour programme.[60] This implies that the purpose of the Safe Harbour principles was not to replace the applicable national laws drawn in accordance with the DPD.[61]

US-based giant multinational technology companies, including Google, Facebook, Apple and Microsoft, are no longer allowed lawfully to transfer users' data automatically. In doing so, they need to adopt 'model contract clauses' for each incident of data transfer from the EU to the United States complying with the EU regulations.[62] Accordingly, after this judgement, numerous companies started to adopt model/standard contractual clauses for the continuation of transferring data in accordance with the European Commission decisions on contractual clauses.[63] Adoption of such clauses could be a temporary

[56]Claburn (n 50).
[57]Weiss and Archick (n 49) 7.
[58]Weiss and Archick (n 49) 7.
[59]Press Release No. 117/15 (n 48).
[60]Article 29 Data Protection Working Party, *Opinion 4/2000 on the Level of Protection Provided by the 'Safe Harbor Principles'* (16 May 2000) 3.
[61]Kuczerawy (n 10) 81.
[62]Gibbs (n 47).
[63]European Commission, Justice, *Model Contracts for the Transfer of Personal Data to Third Countries* <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>; Tanguy Van Overstraeten and Alexandre Entraygues, *The European Court of Justice to Rule on the Validity of Standard Contractual Clauses* (Linklaters, 30 May 2016) 1, 2. <file://atkk/home/b/bupasha/Desktop/Extra%20territorial/standard_contractual_clauses.pdf>.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

solution, but in the long run it may not seem effective being unable to prevent generalised surveillance measures by US government agencies.[64]

It has been a matter of apprehension whether this judgement would result in giant technology companies only theoretically or really bringing effective changes in practice in case of processing EU citizens' personal data, though many of those companies have started to build some data centres within the EU territory in order to manage EU citizens' personal data.[65] Thus, the judgement provides improved data protection by limiting unauthorised access, transfer and processing of data and mass surveillance measures over personal activities online by those companies and law enforcement agencies in the United States.[66]

3.3. Transnational data transfers under GDPR

Data transfer to third countries is allowed under the GDPR if the European Commission considers the legal system of those countries as providing an 'adequate' level of personal data protection (Recital 103). Chapter V (Arts. 44–49) of the GDPR describes cross-border data transfers including some important improvements in relation to the DPD.[67]

Like the DPD, the GDPR requires adequacy determinations with the additional possibility of data transfer. Transfer by way of model clauses would not require any prior notification or specific authorisation from supervisory authorities (Arts. 44, 45, 46 GDPR).[68]

The GDPR not only facilitates transnational data transfers with improved mechanisms but also provides procedures, conditions and restrictions for personal data transfers outside the EU, to third countries or to 'a territory or specified sector within a third country, or an international organisation' upon the European Commission's adequacy decision (Recitals 103–107, 169, Art. 45).[69]

It is interesting that the requirement of 'essential equivalence', as expressed in Schrems case, is reflected in Recital 104 of the GDPR. In order to determine the adequacy, the European Commission takes into account a number of factors, such as the existing legal system, criminal law and access to justice in the country in question; individual processing activities; and international human rights requirements. The Commission is supposed to conduct periodic review and may recognise inadequacy in the level of data protection and prohibit further transfer of personal data in consultation with related appropriate bodies (Recitals 106, 107).[70]

Article 46(1) of the GDPR allows transfer of personal data if the receiver country or organisation as the controller or processor provides 'appropriate safeguards' with data subjects' enforceable rights and effective legal remedies. The procedure, probable contents and providing authorities of such safeguards is described in Recitals 108–110, 114 and Article 46 of the GDPR.

[64]Overstraeten and Entraygues (n 63) 2.
[65]Gibbs (n 47).
[66]Gibbs (n 47).
[67]Anna Myers, 'Top 10 Operational Impacts of the GDPR: Part 4 – Cross-border Data Transfers' (19 January 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/>.
[68]Hunton & Williams (n 42) 32, 33.
[69]ICO (Information Commission's Office), 'Transfers of Personal Data to Third Countries or International Organisations' <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/>.
[70]Myers (n 67).

Downloaded by [University of Helsinki] at 03:39 01 September 2017

In addition, the GDPR provides extended possibilities for the lawful transfer of personal data. Thus, in particular circumstances, for example, by using standard contractual clauses (Art. 46), approved code of conduct (Art. 40) or binding corporate rules (Art. 47), the adequate safeguards might be insured, and accordingly, data might be transferred to non-EU countries under the GDPR even without an adequacy requirement.[71] In addition, Article 42 introduces a new arrangement for transfers by way of certifications, on condition of controllers' or processors' binding and enforceable commitments in applying the appropriate safeguards.[72]

Article 48 and Recital 115 introduce a new provision to the GDPR in relation to the DPD. It describes if a court, tribunal or administrative body of a third country has ordered transfer of personal data that is not otherwise authorised by the GDPR. Such transfer may be recognised or enforced only if there exists 'an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State', without prejudicing other provisions relating to data transfer in the GDPR. Such a provision undoubtedly provides additional protection of personal data to EU residents by limiting particular circumstances of data transfer. However, because the DPD did not have such a provision, the application and interpretation of Article 48 is still quite uncertain and challenging.[73]

The GDPR continues the same derogations as in the DPD and, at the same time, permits transfer to meet the controller's legitimate interests only in limited circumstances.[74] Derogations from adequacy decisions and appropriate safeguards are permitted, for example, with the data subject's explicit consent, for the performance of contract and, for public interest, legal claims or controller's legitimate interest, as described in Article 49 and Recitals 111, 112 and 113.

A significant improvement in the GDPR in relation to the DPD is, as per Article 83(5), a heavy monetary fine of up to 20 million euros, or 4% of the annual worldwide turnover (whichever is higher) that might be imposed for transfers of personal data in violation of the provisions in Articles 44–49.[75] Multinational technology companies should employ an independent data protection officer (Arts. 37–39) while operating their services within the EU.[76]

4. The EU-US Privacy Shield: an updated instrument to face recent technical developments and its interface with GDPR

After the Safe Harbour judgement, both the EU and US authorities drafted an improved new agreement in order to protect personal data and ensure cross-border data flows in co-operation with the national authorities,[77] which also includes commercial aspects of personal data exchange between transatlantic regions.[78]

[71]Tracey Stretton and Lauren Grest, 'How Will the New EU-US Privacy Shield Fit with the Upcoming General Data Protection Regulation?' (22 April 2016) <http://www.scmagazineuk.com/how-will-the-new-eu-us-privacy-shield-fit-with-the-upcoming-general-data-protection-regulation/article/486513/>.
[72]Myers (n 67).
[73]David J. Kessler, Jamie Nowak, and Sumera Khan, 'The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States' (2016) 17(2) The Sedona Conference Journal 577.
[74]Hunton & Williams (n 42) 32, 33.
[75]Stretton and Grest (n 71).
[76]Stretton and Grest (n 71).
[77]Weiss and Archick (n 49) 8.
[78]A29WP Opinion 01/2016 (n 24) 2.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

Because the Safe Harbour Agreement lacked data protection standards and was arranged long before the current expansion of the Internet, it was not welcomed by many European data protection advocates. The expansion of new technologies during the last several years has opened a multifarious medium of collection and processing of personal data; therefore, the Safe Harbour Agreement was bound to be revised because in many respects it appeared as not current enough to tackle situations arising as a result of the latest technologies.[79]

The Safe Harbour Agreement was criticised for separate allegations against the US intelligence agency and the US-based technology companies taking part in unauthorised surveillance activities as well as some aligned interference activities by both were presumed by many European data protection scholars and EU officials. For the sake of economy and business relations in this era of globalisation, the issue was overlooked many years.[80]

Starting before the Safe Harbour judgement and continuing until early 2016 was a discussion about a better document to replace the Safe Harbour. Taking into account the previous concerns about Safe Harbour, a draft version of a new agreement named the EU-US Privacy Shield was released on 29 February 2016 by the EU and US authorities.[81] The European Commission adopted its decision of the EU-US Privacy Shield[82] and the annexes to the decision[83] on 12 July 2016. The Privacy Shield principles become relevant only when the data are transferred from the EU to the United States.[84]

By reviewing the draft agreement, A29WP has published its opinion on the EU-US Privacy Shield, which is non-binding but very relevant to explain the EU approach on cross-boundary data flow.[85] In doing so, the A29WP took into account the business aspects, fundamental rights to privacy and data protection and power of national authorities.[86]

The European Data Protection Supervisor and A29WP found the Privacy Shield as a development and significantly improved over the Safe Harbour Decision, and the 13 recommendations outlined by the European Commission were responded to by the Privacy Shield.[87] It is very important that the level of protection in third countries is equally maintained as it is meant in the EU when protecting fundamental rights to privacy and data protection under the DPD (nowadays in GDPR) and CFR.[88] The Privacy Shield imposes improved commitments for US organisations to protect personal data transferred from the EU, which includes the obligation to provide notice in a comprehensive way, a

[79]A29WP Opinion 01/2016 (n 24) 2.
[80]Weiss and Archick (n 49) 9.
[81]Weiss and Archick (n 49) 9.
[82]Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>.
[83]Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield <http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf>.
[84]A29WP Opinion 01/2016 (n 24) 12.
[85]A29WP Opinion 01/2016 (n 24) 2.
[86]A29WP Opinion 01/2016 (n 24) 2.
[87]Sidley, 'Privacy Shield: Essentially Equivalent' (July 2016) <http://www.sidley.com/~/media/publications/privacy-shield-essentially-equivalent.pdf> 3; Shara Monteleone and Laura Puccio, *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules* (European Parliament, January 2017) 18, 19.
[88]A29WP Opinion 01/2016 (n 24) 10, 11; Sidley (n 87) 8.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

better enforcement system maintaining an enhanced transparency, effective redress mechanisms and more safeguards from the surveillance measures.[89]

The Privacy Shield not only followed the mandates under DPD but also has taken into account the provisions of the GDPR, although some important principles of EU data protection law are not substantially reflected.[90] There are some practical complexities as well that need to be solved efficiently.

It is a matter of concern that the Privacy Shield authorises the US authorities to transfer the data received from the EU to other third countries. Because the state systems of other third countries may vary from one to another, it is not possible to predict those from a specific point of time. If, for example, data are transferred to a country having dictatorship with an arbitrary surveillance system on electronic media and communication, then the EU data will fall under threat. In such circumstances, Chapter V of the GDPR (or Arts. 25 and 26 DPD) should bind the third countries for the intra-group data transfers, which unfortunately are not ensured in the Privacy Shield.[91] However, it is expected that the Privacy Shield would take into account this issue soon.[92]

Some principles of the Privacy Shield are already criticised, such as the 'self-certification' provision, the Ombudsman position bearing doubtful independence[93] and the 45-days notification requirement for data breaches.[94] The language and arrangement of the Privacy Shield are argued to be a bit ambiguous, inconsistent, unclear and difficult to understand in some respects. Because many terms are interpreted differently in the EU and the United States, and some terminologies are different but mean the same matter in those two territories, it is very important to explain every confusing term with clear definitions.[95] For example, privacy on the Internet or right to erasure are understood differently in the EU and the United States.[96]

It is important to remember that, by processing personal data, a data controller may also be a data processor. The term 'data processor' [Art. 4(8) GDPR] does not necessarily mean 'data controller' [Art. 4(7) GDPR] because 'the purposes and means of the processing of personal data' are determined by the controller, and the data processor will not enjoy that power while it becomes a separate entity (only processor).[97] To determine and regulate the activities of such data processors for example, organisations, companies or agents receiving data from the EU to the United States for the purpose of processing, some specific and clear provisions are required in the Privacy Shield, which is still absent.[98] Limiting data retention is a basic feature of the European data protection law [Art. 6(1)(e) DPD and Recital 39, Art. 5(1)(e) GDPR]. Such a provision within the meaning of keeping data 'no longer than is necessary' is absent in the Privacy Shield.[99]

Downloaded by [University of Helsinki] at 03:39 01 September 2017

[89]Weiss and Archick (n 49) 10.
[90]For example, point 6(146) and footnotes 16 and 208 of the Commission Implementing Decision.
[91]A29WP Opinion 01/2016 (n 24) 20–22.
[92]Monteleone and Puccio (n 87) 35.
[93]Monteleone and Puccio (n 87) 32.
[94]'Get Privacy Shield Wrong and It Will Have to be Renegotiated in 2018 Warns Data Protection Lawyer' (March 2016) <http://technewsrss.com/get-privacy-shield-wrong-and-it-will-have-to-be-renegotiated-in-2018-warns-data-protection-lawyer/>.
[95]A29WP Opinion 01/2016 (n 24) 12–14.
[96]Stretton and Grest (n 71).
[97]Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "Processor"* (16 February 2010).
[98]A29WP Opinion 01/2016 (n 24) 16.
[99]A29WP Opinion 01/2016 (n 24) 17.

There are some exceptions to the Privacy Shield principles under which legal obligation of data protection could be limited on the grounds of 'national security, public interest, or law enforcement requirements; by statute, government regulation or case law that creates conflicting obligations or explicit authorizations'.[100] From the EU side, such provision also keeps scope of ambiguity to determine the exact extent of exemption from legal obligation. For that purpose, the EU authorities need to be cognisant about the US law.[101]

Because the future impacts of the GDPR are still unforeseen, the Privacy Shield should be subject to review and amendment considering the application and acceptance of the GDPR.[102] However, the Privacy Shield keeps the flexibility of annual review and joint dispute resolutions to be updated with time and for solving probable complexities. As a paradox, the very flexible nature of an agreement may turn it difficult for concerned legal activists to rely on and investigate properly the related practicalities.[103] The joint review mechanism, as prescribed in the Privacy Shield, is a good initiative, though the provision needs more clarification. Some regional contact point in the EU is required for an effective resolution mechanism.[104]

With the emergence of the GDPR and now the EU-US Privacy Shield in a contemporary time period, a new era in data protection regime is about to begin.[105] It is a time of concern and uncertainty whether the GDPR and Privacy Shield will proceed in harmony or some conflict will arise.[106] The EU authorities sketched the GDPR targeting personal data and privacy protection of EU residents in the changing digital environment. At the same time, with strengthening the harmonised 'one-stop-shop' principle, the GDPR facilitates business aspects of the EU Member States in connection with personal data protection both inside and outside the EU.[107] On the other hand, the Privacy Shield is an attempt to simplify business between the EU and the United States in a digitalised environment. Unavoidably, it has to take into consideration both the EU and US legislations.

It is important to remember that the Privacy Shield is not a legislation but an agreement. Normally, the US-based giant multinational technology companies are not bound to implement this decision unless they subscribe to it.[108] But the universal spread of IT business services necessitates the subscription to the Privacy Shield in order to deal with the cross-border data flows between the EU and the United States. Under such circumstances, subscriptions of hundreds of US-based multinational companies (including Facebook, Google and Microsoft) to the present Privacy Shield decision implies that they care for the EU data protection law in case of transatlantic data transfer.[109]

After the failure of the Safe Harbour Agreement, in spite of both the visible advantages and limitations of the Privacy Shield at this point in time, how the transnational data flow

[100]Annex II.I.5 of the Annexes to the Commission Implementing Decision.
[101]A29WP Opinion 01/2016 (n 24) 17.
[102]A29WP Opinion 01/2016 (n 24) 15; Sidley (n 87) 6.
[103]Stretton and Grest (n 71).
[104]A29WP Opinion 01/2016 (n 24) 3, 4.
[105]Stretton and Grest (n 71).
[106]Stretton and Grest (n 71).
[107]Stretton and Grest (n 71).
[108]Sidley (n 87) 3.
[109]Kevin Townsend, 'Google Signs Up For EU/U.S. Privacy Shield' *Security Week* (6 September 2016) <http://www.securityweek.com/google-signs-euus-privacy-shield>; James Titcomb, 'Facebook Signs Up to Privacy Shield Data Treaty' *The Telegraph* (15 October 2016) <http://www.telegraph.co.uk/technology/2016/10/15/facebook-signs-up-to-privacy-shield-data-treaty/>.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

between the EU and the United States would be tackled, and how the GDPR will interface with Privacy Shield is still uncertain and complex. The most challenging task may currently be to hold a practical and business-oriented look at implementing the Privacy Shield.

5. Conclusion

If people receive suggestions from Google, Facebook, etc. based on their previous online and, very surprisingly, even offline activities, then the total system seems very vague, having a lack of openness, transparency and accountability under a process of surveillance. Under such vagueness and overreaching dominance of the giant technology companies, it is possible to process personal data by operating from any part of the world and targeting users in any part of the world. Even it is not always easy to know when or who processes data, for what purpose and the exact amount and nature of the processing.

An improved legal basis is sought to be established with the introduction of updated provisions in the GDPR, which is expected to be effective in jurisdictional scope and cross-border data transfer issues, especially, for introducing clear and modernised provisions. The EU data protection law's international application in EU data subjects' personal data processing and cross-border data transfer is secured with strong and unambiguous provisions through GDPR.

It is now clear that the EU authorities tried their best to frame EU data protection measures in line with the technological expansion in practice.[110] If a website or application becomes available in any part of the EU, it may be brought under the ambit of the EU data protection law, irrespective of the web or app developers' place of origin when processing EU users' personal data, thereby making a link to the EU. With the GDPR, the regulatory landscape is extended by benefiting businesses and recommending protection of personal data by both the EU- and non-EU-based companies and both inside and outside the EU in the Digital Single Market.[111]

With regards to international data transfer, although the GDPR updates legal obligations with some new concepts, it has not brought massive changes over the existing provisions in the DPD.[112] The same applies for the Privacy Shield, which many believe is an upgrade to the Safe Harbour Agreement.[113]

However, the advancements in information and communication law have just started. In the coming years, it is probable to face new situations and technologies that demand new interpretation of laws and produce numerous case laws.[114]

From the EU users' points of view, the EU data protection law provides efficient protection of privacy against unlawful personal data processing. However, if we explain from

[110]Thompson Hine, 'European Union Imposes Extraterritorial Privacy Obligations on U.S. Businesses' (16 May 2014) <file://atkk/home/b/bupasha/Desktop/Extra%20territorial/Internet%20material/EU-extraterritorial%20privacy%20obligations%20on%20U.S.%20businesses%20-%20Lexology.html>.

[111]Pietro Franzina, 'The EU General Data Protection Regulation: A Look at the Provisions that Deal Specifically with Cross-border Situations' *Conflict of Laws.net* (10 May 2016) < http://conflictoflaws.net/2016/the-eu-general-data-protection-regulation-a-look-at-the-provisions-that-deal-specifically-with-cross-border-situations/>.

[112]Tobias Bräutigam, 'The Land of Confusion: International Data Transfers Between Schrems and the GDPR' in Tobias Bräutigam and Samuli Miettinen (eds) *Data Protection, Privacy and European Regulation in the Digital Age* (FORUM IURIS, Faculty of Law, University of Helsinki, 2016) 168, 169.

[113]Natasha Lomas, 'EU-US Privacy Shield Now Officially Adopted but Criticisms Linger' (12 July 2016) <https://techcrunch.com/2016/07/12/eu-us-privacy-shield-now-officially-adopted-but-criticisms-linger/>.

[114]Bräutigam (n 112) 169.

Downloaded by [University of Helsinki] at 03:39 01 September 2017

non-EU-based, for example, US-based online platforms' standpoints when their services are used within the territory of the EU, it may become complicated for them to define their legal obligation in processing personal data. Ultimately and theoretically they are bound to comply with both the EU and US data protection laws, including the data protection laws of all the respective Member States in question.[115]

In the absence of any universally accepted international data protection law in spite of the worldwide reach of the Internet, the EU data protection law holds the leading position globally when personal data processing of EU nationals/residents are concerned. Ironically, this EU-focused approach of the EU data protection law can be described as a limitation to be 'international' for the people in all parts of the world in the sense that it does not provide redress for non-EU citizens and GDPR only protects data subjects in the EU.[116]

Acknowledgements

The author would like to thank Professor Päivi Korpisaari for her contributions to and assistance in revising initial drafts of this article, as well as Post-Doctoral Researcher Anette Alén-Savikko for commenting on the draft before submission for publication.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

The work is supported jointly by the MyGeoTrust project funded by Tekes– the Finnish Funding Agency for Innovation [grant number 462070] and the Emil Aaltosen Säätiö-funded project *Henkilötietojen suoja digitalisoituvassa yhteiskunnassa* [grant number 4703244].

Downloaded by [University of Helsinki] at 03:39 01 September 2017

[115]Kuczerawy (n 10) 82.
[116]Perotti (n 4) 38, 39.