UNIO - *EU Law Jounal*. Vol. 1, No. 1, July 2015, pp 77-93.
®2015 Centre of Studies in European Union Law
School of Law – University of Minho

The Right to Data Protection and the Commissions' Adequacy Decision

Alexandra Maria Rodrigues Araújo *

ABSTRACT: *Data protection is a fundamental right protected by the EU as well as several international human rights instruments. However, an adequate relation of this right faces new challenges every day. A complicated area for the effectiveness of EU data protection law is the cross-border transfer of personal data. In European law, the main principle applicable to international data flows is the principle of adequate protection. This principle implies that a transfer to a third country/international organization is only permissible if an adequate level of protection of the personal data transferred is guaranteed. In this regard, this paper examines the application of this principle in the adequacy decisions adopted by the European Commission.*

KEYWORDS: *European Union law - data flows -principle of adequate protection - third countries - European Commission.*

* Integrated member of the Centre of Studies of European Union Law of University of Minho.

Introduction

Data protection is a fundamental right protected in the EU and several international human rights instruments. It is a manifestation of the dignity and individual freedom of every human being, expressed in the need to ensure adequate control of his or her personal information.[1] As Ferretti claims: "[…] democratic societies should not be turned into societies based on control, surveillance, actual or predictive profiling, classification, social sorting and discrimination".[2] Nonetheless, every day the full respect of this right has been facing new challenges through the dynamic mechanisms of information and communication technology. In addition, the ubiquitous character of processing personal data hampers a real perception of its compliance with law. A puzzling area for the effectiveness of EU data protection law is the international transfers of personal data to countries outside the European Economic Area (hereinafter "the EEA"). The importance of adequate regulation in terms of data flows to third countries is becoming essential for the protection of individuals' rights in a global and interconnected world. International data flows have exponentially increased in recent years. With regard to European law, the main principle applying to international data flows is the *principle of adequate protection*. It is a principle at the crux of EU data protection law concerning personal data flows and presupposes that a transfer to a third country/international organization is permissible if an adequate level of protection for the personal data transferred is assured.

This article aims to analyze the application of this principle in the adequacy decisions adopted by the European Commission as well as the content of the concept of appropriate level of protection used in the adequacy assessment. The paper has three parts; in the first one, an approach is made to the evolution in time of the data protection EU legal framework. The second part of the article focuses on the general framework of international transfers of personal data to third countries. The third part analyses the actual provisions concerning to the Commissions' Adequacy decisions and the related provisions contained in the proposed General Data Protection Regulation. The paper finishes with some brief reflections.

1. Evolution in Time of EU Data Protection Legal Framework: Key Aspects

The right to privacy emerged in international human rights instruments with Article 12 of the *Universal Declaration of Human Rights* (1948)[3] closely followed by

▪ This article was written in the context of the project "Transfer of personal data to third countries or international organizations: the adequate protection" funded by the Brazilian National Program PNPD/CAPES (Portaria nº 86/2013) and developed at the *Centro Universitario de Maringá* - UniCesumar.

[1] Cf. Peter Hustinx, "*EU Data Protection: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*" 15 September 2014, p. 2, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014.

[2] F. Ferretti, "*Data Protection and the legitimate Interest of Data Controllers: Much ado about nothing or the winter of rights*", Common Market Law Review 51 (2014): 849.

[3] Under the aegis of the United Nation see also: Article 17 of the *International Covenant on Civil and Political Rights. General Comment No. 16 on the respect of privacy, family, home, correspondence, protection of honor and reputation – Article 17. Guidelines for the Regulation of Computerized Files of Personal Data*, adopted by Resolution 45/95 of the UN General Assembly on 14 December 1990. Resolution 68/167 on the *Right to Privacy in the Digital* adopted by the UN General Assembly on18 December 2013. Under the framework of the OECD see the *Guidelines Governing the Protection of Privacy and*

Article 8 of the *European Convention on Human Rights* (1050). The Council of Europe adopted the *Convention for the Protection of Individuals with regard to Personal Data Automatic Processing* (hereinafter "the Convention 108") in 1981, aiming to protect individuals against abuses committed in the collection and use of personal data by the public and private sectors. This international instrument was the first legally binding provision in the field of data protection.[4] The Council of Europe subsequently adopted an *Additional Protocol* to the Convention 108, in 2001.[5] This Protocol regards to supervisory authorities and establishes the provisions on the transfer of personal data to countries not party to the Convention 108, in more detail.

All current 28 EU Member States have ratified the Convention 108.[6] Today, 45 of the 46 Contracting Parties to Convention 108 are States that belong to the Council of Europe. However, Convention 108 has an open character for accession by States outside the Council of Europe, including non-European states. The first non-European state to access the Convention was Uruguay in August 2013. Since 2010, there have been ongoing negotiations on a proposal for the modernization of the Convention 108.

Along with Convention 108, the distinction between the concept of *privacy* and *data protection* started being clarified. Article 2(a) Convention 108 defines personal data as the follows: "any information relating to an identified or identifiable person". Article 2(a) of Directive 95/46/EC[7] maintains the essence of this definition. Consequently, as defends Hustinx: "this means that 'data protection' is *broader* than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data *regardless of* their relationship with privacy, and at the same time *more limited* because it merely concerns to the processing of personal information, with other aspects of protections being disregarded".[8]

Directive 95/46/EC, in terms of individuals protection with regard to the processing of personal data and on the free movement of such data (hereinafter "the Directive" or "Directive 95/46/EC"), was adopted in order to strengthen and expand the principles of data protection contained in the Convention 108.[9] The main objectives of the Directive are twofold: to ensure free movement of personal data between Member States and protect the fundamental right to data protection.

The territorial scope of the Directive goes beyond the 28 Member States and includes the states, which are not EU members, forming part of the EEA. They are Iceland, Liechtenstein and Norway. The material scope of the Data Protection

Transborder Flows of Personal Data (as amended on 11 July 2013).

[4] The Convention 108 requires Contracting Parties to incorporate into their respective domestic laws the necessary measures to ensure respect for all individuals with regard to the processing of personal data. Nevertheless, it cannot be relied on by individuals to create legal rights.

[5] *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*, Strasbourg, 8 November 2001.

[6] Although the adoption of amendments to Convention 108 in 1999 in order to allow the European Communities to accede, the EU is not a party to the Convention 108. But it benefits, however, from observer status and actively participates in the work of the Council of Europe in the field of data protection.

[7] 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 L 281, 23.11.1995, p. 31.

[8] Peter Hustinx, "EU Data Protection Law – Current State and Future Perspectives" (speech presented at *High Level Conference: Ethical Dimensions of Data Protection and Privacy,* Tallinn, Estonia, 9 January 2013), p. 3.

[9] OJ L 281, 23.11.1995, p. 31.

Directive is limited to the single market. It does not apply, therefore, to the area of police and criminal justice. Consequently, the Council Framework Decision 2008/977/JHA completed the Directive on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[10] Moreover, as the Directive is addressed to the Member States, Regulation No 45/2001 was adopted to protect individuals with regard to the processing of personal data by the EU e institutions and bodies.[11]

With the entry into force of the Lisbon Treaty (2009), the expand of the right to data protection in the EU happened due to two main elements introduced in the Treaties: Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 6(1) of the Treaty on European Union (TEU).

Article 16 TFEU contains the new horizontal legal basis for laying down the rules on data protection. In paragraph 1 of Article 16 the right to the protection of personal data is acknowledged, and in its paragraph 2 the fact that the EU has a specific competence to legislate on the matter is recognized . As a principle, the processing of personal data in the public and private sector and in the context of law enforcement are included in the scope of Article 16. [12]

Article 6 of the TEU recognizes that the Charter of Fundamental Rights of the European Union (hereinafter "the Charter") has the same legal value as the Treaties. The Charter is now formally binding upon EU institutions and Member States when they are implementing EU law.[13] It is a primary document, which must be referenced when examining the legality of EU legislation. The Charter ensures the respect for private and family life in article 7. In addition, it explicitly recognizes the right of personal data protection to everyone in article 8. Article 8(2) identifies some of the key principles of data protection: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Paragraph 3 of Article 8 ensures that compliance with data protection rules shall be controlled by an independent authority. Nonetheless, the right to data protection is not absolute and its exercise can be limited in accordance with Article 52(1) of the Charter.[14] However, these limits should be interpreted restrictively.[15]

In summary, with the recognition provided by the Charter, the right to personal data protection evolved from the right to respect private life to an autonomous

[10] OJ L 350, 30.12.2008, p. 60. On the concrete topic of transfers of personal data to third countries or international organizations, these data should, in principle, benefit from an adequate level of protection. The criteria for the assessment of the level of protection are the same of Article 25 of Directive 95/45/CE.

[11] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individual with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 88, 12.1.2001). It was also necessary to detail apart some of the provisions covered by the Data Protection Directive such as those relating to personal data processing in the electronic communications sector.

[12] The foreign and security policy of the EU is only partially covered by the article. Cf. Article 16 (2) last subparagraph TFEU and Article 39 TEU.

[13] Cf. Article 51(1) Charter.

[14] Article 52(1) Charter: «Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others».

[15] Cf. Judgment of 8 April 2014 in Joined Cases C-293 and C-594/12, *Digital Rights Ireland and Seitlinger and Others.*

right, although closely connected to the latter. In accordance with Hustinx "Privacy and data protection - more precisely: the right to *respect* for private life and the right to the *protection* of personal data - have important connections. […] However, there are also crucial differences. The concept of 'data protection' was developed in order to provide structural legal protection to individuals against the inappropriate use of information technology for processing information relating to them, *regardless* of whether that processing would be within the scope of the right to respect for private life or not".[16]

Since 2012, there has been a discussion about the review of the legislative framework of data protection. The reform is based on two Commissions' legislative proposals: a Regulation establishing the general framework of the EU's data protection (replacing Directive 95/46/EC);[17]and a Directive that sets out the rules on the protection of personal data processed for the purposes of prevention, investigation, detection, prosecution of criminal offenses or the execution of criminal penalties (replacing Council Framework Decision 2008/977/JHA).[18]

2. Transfers of Personal Data to Third Countries

Before focusing on the adequacy decisions of the European Commission, the following pages are going to examine the notion of personal data transfer and the legal framework for international data flows.

2.1. Notion of Transfer of Personal Data

In EU law, the notion of *transfer of personal data* has not been defined yet. Nevertheless, there are some elements of it in European law. The notion includes data transfers, which contain "any information relating to an identified or identifiable natural person".[19] Article 25(1) of Directive 95/46/EC regulates "transfer of personal data to a third country, which are undergoing processing or are intended for processing after transfer [...]". In the Council of Europe instruments, Article 2(1) of the Additional Protocol to the Convention 108 regulates "transfer of personal data to a recipient who or which is subject to a foreign jurisdiction". Accordingly, for the European Data Protection Supervisor (hereinafter "the EDPS"), as a starting point, the term is used in EU law "in its

[16] Peter Hustinx, "*EU Data Protection: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*" p. 50.

[17] European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, Brussels, 25 January 2012.

[18] European Commission (2012) Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities. For the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM (2012) 10 final, Brussels, 25 January 2012. In this new proposed legal framework, it is clarified that transfers to third countries may take place only if the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (article 33). Article 34 lays down that transfers to a third country may take place when in relation to which the Commission has adopted an adequacy decision under the General Data Protection Regulation or specifically in the area of police co-operation and judicial co-operation in criminal matters. When adequacy decisions do not exist, a transfer can only happen based on appropriate safeguards (for example, an international agreement) or specified derogations.

[19] Article 2(a) Directive 95/46/CE.

natural meaning, i.e. that data 'move' or are allowed to 'move' between different users".[20] However, the scope of this notion can have tricky contours on a daily basis.

The Court of Justice of the European Union (hereinafter "the CJEU") brought its attention to this notion in the *Boldil Lindqvist* case[21]. In Article 25 of Directive 95/46/CE context, the Court of Justice maintained that there is no transfer of data to a third country: "where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State. Thereby making that data accessible to anyone who connects to the internet, including people in a third country".[22]

In order to fall within the scope of personal data transfers, the transfer needs to be directed at specific recipients.[23] Consequently, the information needs to be deliberately made available to recipients in a third country. Therefore, the term *transfer of personal data* may include the following elements: "communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject […] that the recipient(s) will have access to it".[24] Data flows can take place in physical or digital environment. The latter covers both forms of Internet-based communication *deliberate transfers* and *permitted transfers*.

2.2. Legal Framework for Transborder Data Flows outside the EEA:

The *principle of adequate protection* is the main principle applying to international data transfers subject to Directive 95/46/EC. This principle implies that data flows to third countries are only permissible if an adequate level of protection of the personal data transferred is guaranteed.[25] Accordingly, the general EU legal framework for transborder data flows outside the EEA are established in Articles 25 and 26 of the Directive. In this legal framework, data flows may take place under different legal bases. The most important distinction is that between the free data flows from the restricted data flows. There are free transfers of data to third countries with an adequate level of protection, or to third countries in the specific cases of Article 26 (derogations). There are restricted data flows to third countries when such transfers are made by proof that adequate data protection safeguards are in place, that is, through contractual clauses, binding corporate rules or special international agreements (the EU has been concluding special agreements for two types of data transfers: passenger name records and financial messaging data).

Directive 95/46/EC is addressed to Member States. Therefore, Regulation No 45/2001 (hereinafter, "the Regulation") was adopted in order to protect individuals with regard to the processing of personal data by the EU institutions

[20] EDPS, *The transfer of personal data to third countries or international organizations by EU institutions and bodies*, Brussels, 14 July 2014, p. 6.
[21] Judgment of 6 November 2003 in Case C-101/01, *Lindqvist.*
[22] Ibid. recital 71.
[23] Cf. FRA, CoE, *Handbook on European data protection law* (Luxembourg: Publications Office of the EU, 2.nd edition, 2014) p. 131.
[24] EDPS, *The transfer of personal data to third countries or international organizations by EU institutions and bodies*, p. 7.
[25] Cf. Article 25(1) of Directive 95/46/CE.

and bodies.[26] The most important article for data transfers to third countries is Article 9 of the Regulation which applies to data flows to recipients not subject to the Directive 95/46/EC. Consequently, the scope of Article 9 does not cover recipients established in the EEA countries unless the transfers occur in fields excluded by the directive.[27]

The *principle of adequate protection* is also the main principle applying to international data flows to third countries by EU institutions and bodies.[28] In the context of international transfers of personal data, Article 9 of the Regulation sets out the rules for these transfers in accordance with Articles 25 and 26 of Directive 95/46/EC. However, some notes need to be taken. Article 9(1), unlike Article 25 of the Directive, explicitly includes not only transfers to third countries but also transfers to international organizations.[29] On the other hand, the paragraph adds that the transfer should take place "solely to allow tasks covered by the competence of the controller". For the EDPS "this is a more restrictive approach than the directive, based on the specific nature of the public institutions and bodies covered by the Regulation, who are not permitted to act beyond their competences".[30]

Moreover, Article 9 of the Regulation also provides other different legal basis for data flows: specific mechanisms providing appropriate safeguards for the data flows adopted by the controllers (paragraph 7); and, specific derogations (paragraph 6).

3. The Transfer of Personal Data to Third Countries Accompanied by an Adequacy Decision Adopted by the European Commission

Regarding the free transfer of personal data to third countries accompanied by an adequacy decision, the evaluation of adequacy can be carried out at different levels. Currently, Directive 95/46/EC establishes that the assessment of an appropriate level can be accomplished either by the Member States or by the European Commission. Member States have been using different administrative procedures to comply with its obligations. Namely, by imposing a direct obligation on the controllers, developing a system of prior authorization or subsequent control by data protection authorities.

According to Article 25(6) of the Directive, the Commission is also responsible for the adequacy assessment of data protection in third countries. Commission adequacy decisions are published in the *Official Journal of the European Union* and are binding in all Member States of the EEA guaranteeing a free transfer of personal

[26] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individual with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 88, 12.1.2001).

[27] As such, Regulation No 45/2001 includes two other provisions related to data transfers in Articles 7 and 8. These provisions do not have parallel rules in the Directive 95/46/CE. Article 7 is applicable to data flows within or between EU institutions. Article 8 is applicable to transfers to recipients, other than EU institutions and bodies, subject to Directive 95/46/EC.

[28] The institutions and bodies subject to a specific legal regime for data protection are excluded from the scope of Article 9. For example, the Europol and Eurojust have they specific legal regime on the matter.

[29] Nonetheless, the Commissions' proposal for a General Data Protection Regulation already includes transfers to international organizations.

[30] EDPS, *The transfer of personal data to third countries or international organizations by EU institutions and bodies*, p. 9.

data to the third country concerned. So far, there are only a few number of countries beneficiated with an adequacy decision of the Commission under Article 25(6) of the Directive. These countries are Andorra, [31] Argentina, [32] Canada (private sector),[33] Switzerland,[34] Faroe Islands,[35] Guernsey,[36] State of Israel,[37] Isle of Man,[38] Jersey,[39] New Zealand,[40] the *International Safe Harbor Principles* of the US Department of Commerce (certain activities within the private sector)[41] and Uruguay.[42]

The Regulation No 45/2001 -as Directive 95/46/EC- also provides different possible actors for the assessment of the protection level: controllers, data protection authorities or the European Commission. Subsequently, in the absence of an adequacy decision of the Commission, the EU institutions and bodies as controllers needed to conduct a specific adequacy assessment prior a transfer of personal data to third countries or international organizations. Article 9(5) of the Regulation states that an adequacy decision adopted in the terms established in Article 2(4) and (6) of the Directive 95/46/EC also applies to EU institutions and bodies. There is a guarantee of personal data free transfer to the concrete third country. In this sense, the Institutions or bodies of the EU do not need to adopt any specific procedure or inform the EDPS.[43]

---

[31] Cf. Commission Decision of 19 October 2010 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (OJ L 277, 21.10.2010, p. 27).

[32] Cf. Commission Decision of 30 June 2003 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (C (2003) 1731 end of 30.6.2003).

[33] Cf. Commission Decision of December 20, 2001 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate level of protection provided by the Canadian Personal Information Protection and Electronic Documents (Personal Information and Electronic Documents Act) (OJ L 2, 4.1.2002, p 13).

[34] Cf. Commission Decision of 26 July 2000 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate level of protection of personal data in Switzerland (OJ L 215, 25.8.2000, p. 1).

[35] Cf. Commission decision of March 5, 2010 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate level of protection afforded by the Act on processing of personal data in the Faroe Islands (OJ L 58, 9.3. 2010, p. 17).

[36] Cf. Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (OJ L 308, 25.11.2003, p. 27).

[37] Cf. Commission Decision of 31 January 2011 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automatic processing of data (OJ L 27 1.2.2011, p. 39).

[38] Cf. Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man (OJ L 151/51, 30.4.2004, p. 51).

[39] Cf. Commission Decision of 8 May 2008 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (OJ L 138, 28.5.2008, p. 21).

[40] Cf. Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data from New Zealand (OJ L 28, 30.1.2013, p. 12).

[41] Cf. Commission Decision of 26 July 2000 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the protection afforded by the principles of "safe harbor" and related frequently asked questions (FAQs) issued by the Department of Commerce of the United States of America (OJ L 215, 25.8.2000, p. 7).

[42] Cf. Commission Implementing Decision of August 21, 2012 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay in relation to automated data processing (OJ L 215, 25.8.2000, p. 1).

[43] However, the EDPS might decide to request information from data controllers on a case-by-case basis. Cf. Article 9(5) of the Regulation.

3.1. The Notion of Adequacy

Article 25(6) clarifies some criteria for adequacy assessment: "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose, duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectorial, in force in the third country in question and the professional rules and security measures which are complied with in that country". This list is not considered exhaustive and other elements can be relevant in a concrete evaluation. Thereby, *adequacy* is understood as a functional concept that requires an evaluation of the intended processing activity itself, the rules applicable in the data destination and their effective application.[44]

Concerning Regulation No 45/2001, Article 9(2) establishes the same assessment elements of Article 25(2) of Directive 95/46/EC. Consequently, the elements considered in the assessment of adequacy based on Article 25(6) also apply to the notion of adequacy implicit in the Regulation.

3.2. The Article 29 Working Party and its Contribution to the Notion of Adequacy

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter "the Working Party" or 'the Group") is an advisory group that acts independently. It is composed by representatives of the supervisory authorities designed from each Member State and a representative of the authorities established for the EU institutions and bodies as well as by a representative of the Commission.[45] One of the commitments of the Working Party, it is to give to the Commission an opinion about the level of data protection in third countries.[46]

The Working Party acquired a prominent role in the adequacy evaluation process and contributed significantly to the interpretation of Articles 25 and 26 of the Directive. For the Group, there are two fundamental elements in any adequacy assessment: the content of the rules applicable to the data transferred and the system established to give effect to these rules.[47] Its reference document is the Working Document 12 "Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" of 24 July 1998.[48] In this document, the Group based on the Directive 95/46/EC and other international data protection texts expose a set of core substantive principles of data protection and procedural requirements considered as the minimum necessary for the existence of an adequate protection. Nevertheless, the Group clarifies that this list cannot be interpreted rigidly for all transfers. The degree of risk for the data subject is a fundamental element that helps to determine the specific requirements of data protection for each concrete case.

---

[44] Cf. EDPS, *The transfer of personal data to third countries or international organizations by EU institutions and bodies*, p. 10.

[45] Article 29 of the Directive.

[46] Article 30(1)(b) of the Directive.

[47] Working Party, *Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive*, p. 5.

[48] See, also, the Working Document 4, *First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy*, adopted by the Working Party on 26 June 1997.

In general, each of the Groups' Opinions about adequacy starts with the identification of the law on data protection in the country concerned. Firstly, it is identified and analysed the law considered hierarchically superior: the written Constitution or the law with constitutional relevance and the international agreements ratified by the country. Afterwards, the legislation on data protection is also identified to assess its grade of data protection. The material and territorial scope of the legislations are investigated followed by an analysis of its accordance with the principles considered fundamental for adequate data protection legislation. These principles are summed up in the next lines.

Essential principles that must be respected by the content of such law are: a) *The purpose limitation principle*- data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer; b) *The data quality and proportionality principle*- data should be accurate and updated. Data should be adequate, relevant and not excessive to the purposes for which they are transferred or processed. c) *The transparency principle*- individuals should be provided with the purpose, processing and identity information of the data controller in the third country. d) *The security principle*- the data controller needs to take appropriate technical and organizational security measures according to the risks presented by the processing. e) *The rights of access, rectification and opposition*- the person whose data were subjected to treatment has the right to obtain a copy of all data processed relating to him, as well as the right to rectification of those data where they are shown to be inaccurate. In certain circumstances, the person must also have the right to object to the processing of data relating to him. f) *Restrictions on onward transfers*- further transfers of personal data by the recipient of the initial transfer should be permitted only where the second recipient is also subject to rules affording an adequate level of protection.[49]

The Group established three main goals of any legal system for protection of personal data: a) *ensure a high level of compliance with its rules*- by the data controllers. Besides, the data subjects should be aware of their rights and the means of exercising them. The existence of effective and dissuasive sanctions is considered an important element. b) *provide support and help to individuals data subjects in the exercise of their rights*- the individual should be able to exercise his rights rapidly and effectively, without prohibitive cost. c) *provide appropriate redress*- to the injured party where rules are not complied with.[50]

3.3. The Commissions' Adequacy Decision in the Proposed General Data Protection Regulation

The proposed General Data Protection Regulation (hereinafter "the proposed Regulation")[51] presented by the European Commission in 2012 is being discussed in the framework of the ordinary legislative procedure. The first aspect to mention regarding the proposed Regulation is the changing of the type of legal instrument from directive to regulation. Its most direct consequence is the direct applicability of the General Data Protection Regulation, such as provided for in article 288 TFUE, allowing a single legal instrument in force across the EU.

[49] The Group also established additional principles that should be applied in cases involving certain types of data processing such as sensitive data, *direct marketing* and *automated individual decisions*.
[50] All the opinions of the Group previous the existing adequacy decision of the Commission can be found at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[51] COM (2012) 11 final, Brussels, 25 January 2012.

International dimension of data protection gains importance and space in the new legal framework. Article 3 extends the territorial scope of the proposed Regulation to situations when goods or services are offered on the EU market from an establishment in a third country, or the behavior of data subjects in the EU is monitored. In Article 45 the proposed Regulation encourages international cooperation through dialogue and negotiations with third countries and relevant international organizations.[52]

The provisions on transborder data flows are developed in Chapter V (Articles 40 to 45). The Chapter begins with a general principle establishing that any transfer of personal data to third countries or international organizations needs to respect the provisions of the Regulation. These rules apply to controllers, processors and additional recipients on the case of onward transfers.

The basic three legal tools for international transfer of personal data are maintained. Consequently, free transfer of data to third countries can be achieved when the country takes an adequate level of data protection or in the specific cases of the permitted derogations. There is a restricted data flow to third countries when such transfer is made by proof that adequate data protection safeguards are in place, namely, through contractual clauses, binding corporate rules or special international agreements. In the next lines, the article presents in some detail the proposals of the Commission, the European Parliament and the Council for the new precepts concerning adequacy decisions adopted by the European Commission.

Comparing the proposed Regulation with Directive 95/46/EC regarding the adequacy decision of the Commission; the proposed Regulation adds the possibility of a transfer to an international organization and the possibility of an assessment only on a territory or processing sector within a third country. The Commissions' proposal also states in more detail, the criteria, conditions and procedures for the adoption of the adequacy decision.

Article 41 of the proposal states the relevant criteria for the adequacy assessment. They are the following: "a) the rule of law; relevant legislation in force, both in general and sectorial, including concerning public security, defense, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organization, effective and enforceable rights including effective administrative and judicial redress for data subjects […];

"b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of the Member States";

"c) the international commitments the third country or international organization in question has entered into."

Thereby, the set of circumstances surrounding the transfer of data as stipulated in article 25(2) of the Directive ceases to be part of the evaluation criteria.

Article 41(3) and (4) establishes that the Commission shall do the assessment of adequacy through an implementing act in accordance with the examination

[52] For example, with the Council of Europe, the Organization for Economic Cooperation and Development, the United Nations, the European Committee for Standardization, the International Organization for Standardization, the World Wide Web Consortium or the Task Force Internet Engineering.

procedure. Article 41(5) allows the Commission to decide, by a non-adequacy decision, when the requirements of paragraph 2 are not present, in particular: "in cases where the relevant legislation […] does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred […]". In these cases, any transfer of personal data to the third country, a territory, processing sector within that third country or the international organization is prohibited (with exception of the cases where appropriate safeguards are made or derogations applied). Consequently, the Commission shall enter into consultations with the interested party in order to resolve the situation.[53] A list with the countries, territories or processing sectors within a third country and an international organization with an adequacy/inadequacy decision shall be published by the Commission in the *Official Journal of the European Union.*

The same article ensures in paragraph 8, that the decisions adopted by the Commission until the date shall remain in force, until amended replaced or repealed by the Commission. Furthermore, from the reading of Chapter V of the proposed Regulation, it is understood that, with the new reform, the adequacy decision is centralized in the European Commission and the Member States can no longer make this assessment.

3.3.1. The European Parliament and the Proposed Regulation

The European Parliament adopted a legislative resolution (first reading) on the proposed Regulation in March 2014.[54] On transfers of personal data with an adequacy decision, the main aspects of the Commission proposal are maintained. However, the Parliament position introduced several new elements highlighted below.

In paragraph 2(a) the European Parliament proposes an amendment of the relevant criteria for the adequacy assessment that includes "the implementation of this [data protection] legislation" and "jurisprudential precedents". In subparagraph b) it includes "sufficient sanctioning powers" as an element for the independent supervisory authority to ensure compliance with the data protection rules. In subparagraph c) it gives a particular mention to the international commitments to the protection of personal data.

However, the main changes are in the next paragraphs. The first of them is provided in Article 41(3) and (5) where the European Parliament amends the proposed text of the Commission to stipulate that an adequacy decision shall be adopted by a Commissions' delegated act instead of an implementing act. In the *Explanatory Statement* of the *I Report* this option is defended because it enables the Council and the Parliament to make use of their right of control.[55] The European Parliament amendment also adds that the adoption of an adequacy/non adequacy decision need to include an opinion of the European Data Protection Board.[56] To

[53] Article 41(6) and (7) of the proposed Regulation.

[54] MEPs voted on the Report of Jan Phillip Albrecht: *I Report on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with the regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Committee on Civil Liberties, Justice and Home Affairs, 21 November 2013; See, also, 2014-2015 Session of the European Parliament of 11 March 2014, pp. 418-442.

[55] Ibid. p. 203.

[56] The European Data Protection Board is the current Article 29 Working Party.

that end, the Commission shall provide the group with all the necessary documentation.[57]

A new paragraph (4)(a) is added to the initial text establishing that the Commission shall monitor developments in third countries and international organizations that could affect the relevant elements that are derived from a previous Commission adequacy assessment. It is also stipulated that previous Commission adequacy decisions shall remain in force until five years after the entry into force of the Regulation unless amended, replaced or repealed by the Commission before the end of this period (paragraph 8).

Another important decision of the European Parliament is the elimination of the possibility of an adequacy decision only for a sector of a third country. The explanation given is that "it would increase legal uncertainty and undermine the Union's goal of a harmonized coherent international data protection framework".[58]

3.3.2. The Council and the Proposed Regulation

There have been intense discussions about the reform of the data protection package in the Council, however, any formal position about the proposed General Data Protection Regulation was adopted. Nevertheless, some elements of the document have been debated in the Council meetings. Because of these discussions, a partial general approach on several international aspects of the draft Regulation was achieved in the Justice and Home Affairs Council Meeting on the 5th and 6th of June 2014. In concrete, on the provisions on the territorial scope; on the definition of *binding corporate rules* and *international organizations;* and, on the transfers of personal data to third countries or international organizations.[59]

In the subsequent lines, some of the main points of this partial general approach connected with the international transfers of personal data, will be outlined. In regards to this, the Council decided to maintain the same basic three legal channels that enable personal data to be transferred outside the EU borders.[60] However, to the text proposed by the Commission for Article 41(2), the Council introduces new criteria for the adequacy assessment: "the respect for human rights and fundamental freedoms", "data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organization […]". Besides, in article 41(2)(c), the Council adds to the international commitments other "obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data". The Council also supports the idea of a reference of the European Data Protection Board rule during the process of adequacy/non-adequacy[61] and a new Article 41(4)(a) with a similar content to that introduced by the European Parliament.

On the contrary, it seems that the Council does not agree with the change made by the European Parliament, that an adequacy decision shall be adopted by a delegated act of the Commission and maintains the adoption by an implementing act in accordance with the examination procedure.

In paragraph 5 the Council adds that, where necessary, the Commission may "repeal, amend or suspend such decision [of adequacy] without retro-active effect

[57] Article 41(6)(a).
[58] I Report, p. 203.
[59] However, this agreement does not exclude future changes being made by the Council to the text of Chapter V of the Draft Regulation.
[60] Council of the European Union, Interinstitutional File 2012/0011(COD) 10349/14, p. 4 (para.8).
[61] Cf. Article 41(2)(a).

[…]". A new subparagraph is introduced establishing that "the Commission shall enter into consultations with the third country or international organization with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5".

Lastly, the current position of the Council also supports the Commission Proposal that a specified sector can be object of an adequacy decision (contrary to the opinion of the European Parliament).

4. The Adequacy Findings: Between the Past and the Future

The EU Data Protection package increased the level of visibility and protection of personal data in Europe and in the world. However, it can also be observed that regarding the transfers of personal data outside the EEA, the current EU legal framework on data protection does not fully deal with its legal challenges. Consequently, it failed to prevent insecurity about their personal data in most European citizens.[62]

Thus, the 2003 Commissions' first report on the implementation of Directive 95/46/EC has already identified some shortcomings in the implementation of Articles 25 and 26 of the Directive. Thereon, divergences between Member States law were pointed as "very broad".[63] Concerning the adequacy findings were identified several shortcomings at both national and European level.

4.1. Adequacy Assessments at National Level

Regarding the adequacy findings, the Commissions' first report exposes that the implementation of the Directive originated different approaches in the assessment of adequacy at the Member States' level. In some Member States, the controller assesses adequacy with very limited control by the State or national supervisory authorities. Other Member States have decided to require an administrative authorization for all transfers to third countries including when the use is made of the Commissions' adequacy decisions.[64] A better scrutiny in this lack of harmonization is given in the technical analysis on the implementation of the Data Protection Directive provided with the Report. For example, this analysis clearly shows that in some Member States it is possible to assess an adequacy finding with general effects. In some cases, the responsibility for the assessment relies on the national supervisory authorities and in other cases either in the Minister of Justice or in the Government. On the contrary, in other Member States, these national authorities or governments only deal with specific transfers without general effects.[65]

The report also underlines the main risks of such opposite approaches: "An overly lax attitude in some Member States – in addition to being in contravention of the Directive – 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

[62] Cf. European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union* (Brussels: Opinion & Social, 2011), pp. 137-172.
[63] European Commission, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 final, Brussels, 15 May 2003, p. 18.
[64] Ibid. p. 18. Cf. also: European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, Brussels, 15 May 2003, p. 32; pp. 50-51.
[65] Ibid. p. 32.

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".[66] The report expressed the concern "that many unauthorized and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement actions by the supervisory authorities."[67]

By all said, if we look for the proposed Regulation, the centralization of adequacy findings in the European Commission seems correct in order to achieve a more coherent framework and prevents the development, by governments/data protection authorities of a multitude of different lists eventually in conflict with each other. It also eludes the difficulties inherent to financial and staff shortcomings faced by several national authorities/governments when they take these adequacy findings.[68] In fact, the complexities of the decision or commitment that the national authorities assume in these findings made this option sparsely used by them.[69]

4.2. The Commissions' Adequacy Assessment

Concerning the Commissions' adequacy decisions, demands have being made to increase the number of decisions adopted; in the necessity for a clarification of the criteria and requirements for assessing the appropriate level of data protection in third countries;[70] in more clear rules concerning the procedure leading to an adequacy decision;[71] and, in the need for stricter enforcement and implementation monitoring of the adequacy Commissions decisions.[72] Simultaneously it has also been a frequent request that these demands need to be equilibrated with a necessary flexibility and openness toward to the distinct legal traditions and cultures presented in different countries and regions.[73]

In recent years the efficacy of the Commissions' adequacy decisions in the protection of personal data has been questioned as a result of the scandal regarding the third country's mass surveillance of EU citizens for intelligence and national security purposes. In particular the protection proportionated by the Safe Harbour Principles of the US Department of Commerce has been severely questioned since the business companies identified in the media revelations to be involved in the massive surveillance of EU citizens are companies that had declared their adhesion to these principles. Other countries vised by adequacy

---

[66] European Commission, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, p. 19.
[67] Ibid.
[68] Cf. CRIDS, *Assessment of the application of Article 25 of Directive 95/46*, 27 July 2011, p. 5; Directorate-General for internal Policy, *Study: Reforming the Data Protection Package*, pp. 69-70.
[69] Cf. *Analysis and impact study on the Implementation of Directive 95/46 in Member States*, p. 32.
[70] Cf. European Parliament, *European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union* (2011/2025 (INI), Brussels, 6 July 2011, recital 46; A. Zinser, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, Tulane Journal of Technology and Intellectual Property 6 (2004): p. 172; P. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, Iowa Law Review 80 (1994-95): p. 473.
[71] Cf. Directorate-General for internal Policy, *Study: Reforming the Data Protection Package* (Brussels, 2012), p. 70;
[72] Cf. European Parliament. *European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union,* recital 46.
[73] Cf. C. Kuner, *the European Union and the Search for an International Data Protection Framework,* Groningen Journal of International Law 2 (2014): pp. 69-71.

decisions are also object of critics since -according to the information available- the national agencies of New Zealand, Canada and Australia have also been involved in the mass surveillance of the electronic communications of EU citizens. [74]

These recent revelations triggered an important and ongoing debate about the democratic oversight of intelligence services with clear legal consequences. From the EU data protection law perspective, the problematic needs to have in consideration several different aspects. According Article 4(2) TUE -in the relationship between the EU and the Member States- maintaining its national security remains the "sole responsibility" of each Member State.[75] In consequence, EU law -including Directive 95/46/CE and the Charter- does not apply to matters within the scope of the national security of Member States. In this sense, Article 3(2) of the Directive 95/46/CE is a specific expression of this general exemption.[76] On the subject, however, Member States remain bonded to other international/European human instruments protecting personal data.[77]

A distinguishable situation appears when personal data subject to EU data protection law is accessed by third countries invoking the national security of such third countries. In these cases, the exemption that the treaty offers is not applicable. However, if a Member State claims that a threat to the national security of a third country also forms part of its own national security, this interest should only be accepted if it is properly justified to the relevant authorities on a case-by-case basis. If the Member State fails to do so, Directive 95/46/EC is not precluded and such transfers of personal data need to be covered by one of the legal tools provided for in Articles 25 and 26. This means that companies with data of European citizens stored have the obligation to comply with EU data protection legislation even where they are subject to national security legislation of a third country. In a working paper clarifying the legal discussions concerning this subject, Article 29 Working Party concludes that "Massive, indiscriminate and secret access to personal data originally processed under EU jurisdiction and transferred from the EU to a third country where it is then able to be accessed for that third country's surveillance programmes does not fulfill the requirements of the data transfer provisions of Directive 95/46/EC".[78]

This concrete issue has been object of attention during the reform of the data protection package. In particular, the European Parliament included a new Article

---

[74] Cf. Committee on Civil Liberties, Justice and Home Affairs (European Parliament), *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,* Rapporteur: Claude Moraes, 21 February 2014, specially pp. 1-15.

[75] See also Declaration 20 annexed to the Treaty of Lisbon.

[76] Differently, Article 13(1) of Directive 95/46/EC applies when the national legislator impose restrictions to the scope of the obligations and rights provided on the Directive if such a restriction constitutes a necessary measures to safeguard (a) national security; (b) defense; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); or (g) the protection of the data subject or of the rights and freedoms of others.

[77] See note n. 3. At European level, Member States are legally bounded by the European Convention on Human Rights (especially Article 8 as interpreted by the ECtHR case law), the Convention 108 and Additional Protocol.

[78] Cf. Article 29 Working Part, *Working Document on surveillance of electronic communications for intelligence and national security purposes,* adopted on 5 December 2014, p. 44. Also: Article 29 Working Part, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes,* adopted on 10 April 2014.

43a to the proposed Regulation establishing that requests by public authorities or courts in third countries to personal data stored and processed in the EU should only be granted by the data protection authority after verifying that the transfer complies with the Regulation.

However, due to the complexity of the matter, international agreements with third countries/international organisations in order to grant adequate protection to EU citizens when intelligence activities are carried out seems desirable.

In conclusion, if we examine the proposed Regulation, Chapter V responds better to the actual challenges of data transfers outside the EU and in concrete on the challenges concerning the adequacy decisions. Some improvements are clearly perceived. With the shift of the legal instrument -from a directive to a regulation- the complexity and inconsistencies caused by different national laws transposing Directive 95/46/EC will disappear. A single instrument instead of 28 national laws has greater potential for the reduction of legal fragmentation with the yearned benefits of greater harmonization. The elimination of the "circumstances of the specific transfer" in the assessment criteria provided in the Article was also welcome.[79] At the same time, Chapter V maintains a certain margin of flexibility in order to adapt the adequacy assessment to other legal cultures.[80]

However, a bigger level of transparency in adequacy decision procedures as well as a more detailed monitoring of the developments based on adequacy decisions seem to be desirable. This legal tool will also benefit from a situation in which concepts such as "national security", "public security", "internal security", "transfers of personal data" are clarified. In a more general way, this legal tool only works if the "all package" works. In this sense, if derogations to the *principle of adequate protection* are the "rule" for transfers of personal data outside the EEA, it seems that the adequacy decisions lose a significant part of its potential for data protection.

Final Remarks

Dynamic mechanisms of information and communication technologies are opening amazing prospects for business, health, communications, transports, environment, etc. However, it is in this vibrant and still emergent reality of the digital economy that individuals have a fundamental right of their personal data protection. This new "industrial revolution" cannot be done without the respect of fundamental rights and the legislature need to find the way to do it. In this sense, an effective legal framework on behalf of cross-border flows of personal data is essential for the guarantee of data subjects. The Commission adequacy decisions' have a central place in the legal framework of international cross-border flows of personal data. In spite of the complexities of its process, this legal tool should be driven whenever possible. Because this legal instrument has a great potential to increase data protection and legal certainty in personal data transfers outside the EEA. Furthermore, it can also work as an important tool for dialogue between EU and the world in the common interest of global interoperability of data protection frameworks.

---

[79] Cf. Directorate-General for internal Policy, *Study: Reforming the Data Protection Package*, p. 69.

[80] As C. Kuner underlines: "Only this mixture of respect for fundamental rights and flexibility towards the variety of data protection systems that exist around the world can provide the conditions under which an international legal framework for data protection can eventually develop". C. Kuner, «*The European Union and the Search for an International Data Protection Framework*» *Groningen Journal of International Law* 2 (2014); p. 71.