Athens Journal of Law - Volume 4, Issue 4 – Pages 337-358

Personal Data Transfer to Third Countries – Disrupting the Even Flow?[1]

By Danijela Vrbljanac[*]

In the light of the Snowden revelations in 2013, Maximilian Schrems instituted the proceedings against the Irish Data Protection Commissioner which resulted with the invalidation of the Safe Harbour Agreement by the CJEU. The Safe Harbour Agreement, the framework under which EU citizens' personal data were being transferred to the US, was replaced by the EU-US Privacy Shield which put in place rules and procedures for more effective protection of personal data. Apart from the adequacy decisions such as Safe Harbour and Privacy Shield, the Data Protection Directive envisages adequate safeguards, such as contractual clauses, binding corporate rules and derogations as bases for transfer of personal data to third countries. Despite the fact that these bases are maintained in the General Data Protection Regulation, its entry into force in May 2018 brought some changes in this respect. It was already suggested that the EU-US Privacy Shield will have to be significantly amended. Furthermore, the validity of standard contractual clauses will be inspected by the CJEU since the Irish High Court decided to refer the question for the preliminary ruling on this matter in October 2017. This paper analyses the bases and conditions for transfer of personal data to third countries, novelties introduced by the new General Data Protection Regulation and pinpoints the matters which might present the greatest challenge for efficient data protection, the area of EU law surrounded by much controversy.

Keywords: *Data Protection; Data Transfer; EU law; GDPR; Privacy; Transborder Data Flow.*

Introduction

Information and communication technology has intrinsically transformed every aspect of how society operates. In such environment, data, due to its characteristic of being non-rivalrous[2] or non-material, easily crosses over borders. Such transborder data flows represent a crucial part of effective usage of technology for different private, social and business purposes, such as interacting and sharing content via social media, storing data on clouds, browsing for information, selling goods and providing services online, completing transactions, etc. Such setting poses a great risk for misuse of personal data and invasion of privacy. This paper therefore aims to illustrate regulation of transborder data flows

[*]PhD, Postdoctoral Fellow at the Department of International and European Private Law, University of Rijeka, Faculty of Law, Croatia. Email: dvrbljanac@pravri.hr.
[1]This paper has been written with the support of the Croatian Science Foundation project no. 9366 – Legal Aspects of Corporate Acquisitions and Knowledge Driven Companies' Restructuring and University of Rijeka project no. 13.08.1.2.01 – Protection of Beneficiary on the Croatian and European Financial Services Market.
[2]Murray (2013) at 12-13.

https://doi.org/10.30958/ajl.4-4-4 doi=10.30958/ajl.4-4-4

in the EU, its recent judicial and legislative development, particularly taking into account entry into force of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation, hereinafter: GDPR),[3] as well as indicate issues that remain to be problematic.

Determination of the Problem

In the era of rapid technological advancement, globalisation and internationalisation of business, the transfer of personal data from the EU Member States to third countries[4] and international organisations is becoming more and more frequent. Following Snowden revelations in 2013, as well as numerous subsequent data leaks such as Uber in 2017, FedEx, and the most recent ones like Cambridge Analytica and Facebook in 2018, the transfer of personal data has become one of the most controversial issues of data protection. The validity of various bases for data transfer to third countries and international organisations has been contested more than once before the CJEU. With regards some of these bases, the proceedings before the CJEU are still ongoing. Furthermore, it has been argued that with the beginning of application of the GDPR some of the bases for personal data transfer to third countries and international organisations enacted under the GDPR's predecessor, 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 (hereinafter: the Data Protection Directive, DPD)[5] will have to be amended. The literature on EU data protection is extensive. While there is a number of papers and monographs on data transfer according to DPD and transfer bases enacted pursuant to DPD,[6] the literature providing an analysis taking into account the novelties brought about with the GDPR is sparse since it predates the GDPR,[7] or is focused on a particular issue.[8] This paper therefore aims to fill this void by providing an overview of data transfer regulation and its recent developments.

[3]Regulation (EU) 2016/679.
[4]The term third country refers to countries other than EU Member States, Norway, Liechtenstein and Iceland.
[5]Directive 95/46/EC.
[6]Aldhouse (1999); Kuczerawy (2011); Patzak, Hilgard & Wybitul (2011); Kuner (2013).
[7]Kuner (2017); Bu-Pasha (2017); Voigt & von dem Bussche (2017). For a brief overview of transfer of personal data to third countries and international organisations under the GDPR, see also Weber & Staiger (2017).
[8]Coley (2017); Report "Essentially Equivalent"; Geppert (2016); Byrne Sedgewick (2017); Voss (2016); Boehm (2016); Corcoran (2016); Corcoran (2017); Fahey (2018); Gonzalez Fuster (2016); Colonna (2016); Mouzakiti (2015); Suda (2018); Whitaker (2017); Cole, Fabbrini & Schulhofer (2017).

Grounds for Transfer

As of 25 May 2018, the GDPR, as an EU law source that horizontally regulates data protection law, started applying and replaced its predecessor, the DPD.[9] The transfer of data to third countries and international organisations is governed by Chapter V of the GDPR (previously Chapter IV of the DPD). The GDPR follows the same general principle as the DPD which generally prohibits the transfer of personal data to third countries and international organisation.[10] There are three possible grounds for exceptions based on which personal data may be transferred to third countries in the DPD which have been maintained in the GDPR: adequacy decisions, adequate or appropriate safeguards and derogations.

Adequacy Decisions

Adequacy decisions are European Commission decisions by which the Commission decides that a third country or an international organisation ensures an adequate level of protection, based on which personal data may be transferred to that third country or international organisation.[11] The GDPR is more elaborate with respect to the elements which have to be taken into consideration when reaching a decision on existence of the adequate level of protection than the DPD. Art. 45 of the GDPR enlists and further elaborates three categories of elements: legal rules, existence and effective functioning of one or more independent supervisory authority and international commitments of the third country or international organisation. Art. 25(2) of the DPD prescribed that adequacy should be assessed in the light of all circumstances, particularly nature of the data, the purpose and duration of processing, the country of origin and country of final destination, the rules of law, both general and sectoral, and the professional rules and security measures which are complied with in that country. Furthermore, the GDPR, unlike the DPD, prescribes that European Commission should implement a mechanism for periodic review, at least every four years of developments in third country of international organisation.

Article 29 Working Party[12] in its 1998 Working Document 12 established that analysis of adequacy should rely on two main factors, namely content of rules applicable to personal data transferred to a third country, and the system of ensuring the effectiveness of such rules. As a means of implementing such

[9]Apart from this horizontal legal acts, there are also sectoral ones such as Directive (EU) 2016/680 which had to be transposed into Member States legislations by 6 May 2018 and Regulation (EC) No 45/2001.

[10]See Art. 44 of the GDPR and Art. 25(1) of the DPD.

[11]See Art. 45 of the GDPR and Art. 25 of the DPD.

[12]Working Party on the Protection of Individuals with regard to the Processing of Personal Data or Article 29 Working Party was an advisory and independent body established by Art. 29 of the DPD which consisted of representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the EU institutions and bodies, and of a representative of the Commission. With the entry in force of the GDPR, it was replaced by the European Data Protection Board, which is an EU body with legal personality (Art. 68 of the GDPR).

analysis, Article 29 Working Party established content and enforcement principles[13] which are similar to the principles set down in 1981 Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[14] or the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files.[15]

From Safe Harbour to Privacy Shield

Adequate level of protection has been a subject of discussion before the CJEU in *Schrems*. The case concerned the adequacy decision by which the personal data was being transferred to the EU, i.e. Commission Decision 2000/520 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 (hereinafter: the Safe Harbour)[16]. Along with Edward Snowden revelations in 2013, this case raised the issue of data transfer to third countries to the level of one of the most polemical issues in EU law and policy.

In the light of information revealed by Edward Snowden, Maximilian Schrems, Austrian national and user of Facebook made a complaint to the Irish Data Protection Commissioner. Since every Facebook user from the EU had to enter into a contract with Facebook Ireland, a subsidiary of Facebook Inc. established in the USA, personal data belonging to those users were being transferred to Facebook Inc.'s servers located in the US for processing. Data was being transferred based on Safe Harbour Decision under which US companies could undergo a self-certification procedure in order to be able to process personal data collected in the EU. Schrems sought from the Irish Data Protection Commissioner to stop transferring his personal data to the US. The Commissioner rejected Schrems' complaint as unfounded since the European Commission found that the US ensures an adequate level of protection in Safe Harbour Agreement and there was no evidence that personal data belonging to Schrems was accessed by the US National Security Agency (hereinafter: the NSA). Schrems then challenged the Commissioner's decision before the Irish High Court. High Court found that Snowden revelations demonstrated that there is a "significant over-reach" on the part of the NSA and other federal agencies regarding surveillance and interception of personal data which is carried out in secret so that the EU

[13]Content principles are: the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and opposition and restrictions on onward transfers. Additional content principles which should be applied in case of specific types of processing are: sensitive data, direct marketing and automated individual decision. Enforcement principles are: good level of compliance, support and help to individual data subjects and appropriate redress. See Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12, 24.7.1998.

[14]OECD Guidelines were subsequently amended in 2013.

[15]For more on adequacy see Aldhouse (1999).

[16]Commission Decision 2000/520.

citizens do not have the right to be heard and is contrary to the principle of proportionality.[17]

In these circumstances the High Court decided to refer questions for the preliminary ruling to the CJEU by which it wanted to ascertain whether and to what extent, a national supervisory authority is bound by the Safe Harbour in examining whether the law and practices of the third country to which personal data is being transferred to do not guarantee an adequate level of protection contrary to the respect for private and family life, protection of personal data and the right to an effective remedy and to a fair trial enshrined in the Charter of Fundamental Rights of the European Union.

The CJEU responded that even when the Commission has adopted decisions such as the Safe Harbour, national supervisory authorities are not prevented from examining the claim of person, whose personal data has been transferred from the Member State to the third country, that laws and practices in that country do not ensure an adequate level of protection.[18] As the CJEU explained, Art. 28 of the DPD, which prescribes that national supervisory authorities hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data, does not provide for any exception when such transfer has been regulated by the Commission decision based on Art. 25(6) of the DPD. Otherwise, persons whose personal data were transferred to the third country would not be able to lodge a claim before the national supervisory authority with the intention of protecting their rights.[19]

When a person whose personal data has been transferred to the third country lodges a claim with the national supervisory authority, that authority must examine the claim with due diligence. If a national supervisory authority considers the claims are unfounded, the person must have access to the judicial remedy which enables him or her to challenge that decision before national courts. If the national supervisory authority finds the claim well founded, it must be able to engage in legal proceedings. Even though the national courts are entitled to consider the validity of an EU act, such as the Commission decision adopted pursuant to Art. 25(6) of the DPD, they do not have the power to declare it invalid. This power lies only with the CJEU. Therefore, national courts which doubt as to validity of the Commission decision must refer questions for the preliminary ruling to the CJEU.[20]

In *Schrems*, the CJEU invalidated the Safe Harbour, since it established that Art. 1 of the Safe Harbour is contrary to Art. 25(6) of the DPD because it does not contain sufficient findings that the US ensures an adequate level of protection based on its domestic law and international agreements. As the CJEU elaborated, the level of protection in third countries does not have to be identical as the one in the EU, but essentially equivalent to the one guaranteed in the EU based on the

[17]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 30-35.
[18]*Maximillian Schrems v Data Protection Commissioner*, paragraph 66.
[19]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 57-58.
[20]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 61-65.

DPD and the Charter.[21] Essential equivalence, first of all, includes high level of protection of fundamental rights in third state which derives from content of the applicable rules in that country resulting from its domestic law or international commitments and practice, as well as effective means of protecting fundamental rights. Reasons of national security, public interest, or law enforcement requirements should not have primacy over these fundamental rights.[22] Furthermore, essential equivalence has to be periodically checked by Commission. Self-certification is not itself contrary to the essential equivalence requirement as long as it provides for the detection and supervision mechanism which enable identifying and punishing violations of rules, especially ones protecting private life and data.

Apart from Art. 1 of the Safe Harbour, Art. 3 was found problematic since it prevented national supervisory authorities from examining claims of persons calling into question the level of protection in the third country to which the Commission decision refers to. Given that Arts. 2 and 4 of the Safe Harbour are inseparable from Arts. 1 and 3, the entire decision was invalidated.[23]

Safe Harbour Decision was replaced by the Commission Implementing Decision (EU) 2016/1250 of 12 July 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-U.S. Privacy Shield (hereinafter: the Privacy Shield)[24] which was adopted on 12 July 2016. Similarly to the Safe Harbour, it allows to US companies to self-certify to the Department of Commerce so that they can process personal data collected from the EU and Switzerland. Currently 3485 active companies take part in the Privacy Shield framework.[25] Privacy Shield Decision took over seven principles from the Safe Harbour Decision (Notice, Choice, Onward Transfers, Access, Security, Data Integrity, and Enforcement). The crucial differences exist with regards to the Onward Transfer Principle in the sense that the requirement for transferring data to third parties is stricter. Companies certified under the Privacy Shield Decision have to conclude contracts with third party controllers to which they transfer data. The level of protection provided by these third parties must accord to Privacy Shield Principles, and they may only process data for limited and specified purposes. Apart from that, Privacy Shield has enabled persons to file complaints before independent dispute resolution bodies and European Data Protection authorities. US Department of Commerce will

[21]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 73-74; Opinion of Advocate General Bot in *Maximillian Schrems v Data Protection Commissioner*, paragraph 141. The understanding of data protection as a right guaranteed by Art. 8 of the EU Charter is linked to the understanding of a right to private life guaranteed by Art. 8 of the ECHR, Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector. See Boehm (2012) at 4. 19-173. See also González Fuster (2014) at 75-107. See also Art. 52(3) of the EU Charter.

[22]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 73-89. For more on essential equivalence see Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and United States, Sidley Report, January 2016.

[23]*Maximillian Schrems v Data Protection Commissioner*, paragraphs 79-106.

[24]Commission Implementing Decision (EU) 2016/1250.

[25]Information retrieved on 11 August 2018 from Privacy Shield Framework website.

resolve complaints about a company non-compliance with the Privacy Shield Principles, and as a last resort, persons will have at their disposal binding arbitration by a "Privacy Shield Panel" of at least 20 arbitrators designated by the US Department of Commerce and the European Commission.[26]

Validity of Privacy Shield

Soon after its entry into force, Privacy Shield was challenged. Article 29 Working Party published Opinion 2/2016[27] in which it raised its concerns as to the Privacy Shield. It indicated that major concerns are the fact that Privacy Shield does not regulate the deletion of data and time limits for keeping data, the fact that US administration collects massive and indiscriminate data, insufficient powers of the Ombudsperson necessary for its effective functioning and lack of clarity in defining certain notions such as onward transfer principle. Article 29 Working Party thus suggested that Privacy Shield, as well as other adequacy decisions[28] should be amended in a way more consistent with the GDPR.

On 16 September 2016, Digital Rights Ireland, an Irish non-profit dedicated to protecting individual internet freedoms commenced the action contesting the Privacy Shield claiming that it is contrary to Art. 25(6) of the DPD, it violates the right to privacy guaranteed by the Charter of Fundamental Rights and that Privacy Shield does not adequately ensure that the EU citizens' rights under EU law are fully provided for where their data is transferred to the US. The EU General Court concluded that the applicant does not have standing and that the action is inadmissible.[29] Digital Rights Ireland claimed that it possesses a mobile phone and a computer which means that its personal data may be transferred to the US pursuant to Privacy Shield. The EU General Court responded to this claim by stating that the applicant, as a legal person, cannot possess personal data. Furthermore, if the applicant is observed from the perspective of a controller of its supporters' personal data, Privacy Shield does not impose obligation to European controllers. It imposes obligations to American controllers and processors, whereas European controllers are merely authorised to transfer personal data to American organisations. Digital Rights Ireland, as the EU General Court indicated, did not demonstrate that it was empowered to bring action in the name and on behalf of its supporters. With respect to the applicant's argument that Art. 80(2) of the GDPR allows Member States to provide that anybody, organisation or association to lodge a complaint with the national supervisory authority if the data subject's right have been infringed as a result of processing, the EU General Court simply responded that the GDPR does not enter into force until 25 May 2018.

Privacy Shield was again challenged on 25 October 2016 when La Quadrature du Net and others sought from the EU General Court to declare that it is contrary to provisions of Charter of Fundamental Rights of the EU. The

[26]For more on Privacy Shield see also Geppert (2016).
[27]Article 29 Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13.4.2016.
[28]See infra chapter *Other adequacy decisions and similar arrangements.*
[29]*Digital Rights Ireland v Commission*.

applicants alleged that level of privacy protection in the US is not essentially equivalent to the EU level and that there is no effective remedy in the US regulatory regime.[30] Since in the previous Digital Rights Ireland case, the EU General Court did not have the opportunity to go into the merits of the case, it will be interesting to see the developments in *La Quadrature du Net* case.

Other Adequacy Decisions and Similar Arrangements

The number of countries which were assessed as adequate is limited. Besides the US in the realms of the Privacy Shield, the European Commission has reached adequacy decisions in respect of the following countries: Andorra,[31] Argentina,[32] Faroe Islands,[33] Guernsey,[34] Israel,[35] Isle of Man,[36] Jersey,[37] New Zealand,[38] Switzerland,[39] Uruguay.[40] With respect to Canada, the Commission decision refers to transfer of personal data to recipients subject to the Personal Information Protection and Electronic Documents Act, which are private-sector organisations.[41] After Schrems, these adequacy decisions were all amended by replacing their provisions under which national supervisory authorities has limited powers similar to Art. 3(1) of the Safe Harbour Decision and by introducing the obligation of monitoring periodically developments in these countries.[42] Currently, negotiations are ongoing with respect to Japan and South Korea.[43]

Appropriate (Adequate) Safeguards

According to Art. 46 of the GDPR, in the absence of the adequacy decision, personal data may be transferred to the third country or an international organisation if the data controller or processor has provided appropriate safeguards or adequate safeguards as Art. 26(2) of the DPD referred to them.

Appropriate safeguards encompass agreements between public authorities, binding corporate rules, contractual clauses, and approved codes of conduct and certification mechanisms. Agreements between public authorities (Art. 46(2)(a) of the GDPR) is an appropriate safeguard which has not been envisaged in the DPD.

[30] *La Quadrature du Net and Others v Commission*.
[31] Decision 2010/625/EU.
[32] Decision 2003/490/EC.
[33] Decision 2010/146.
[34] Decision 2003/821/EC.
[35] Decision 2011/61/EU.
[36] Decision 2004/411/EC.
[37] Decision 2008/393/EC.
[38] Decision 2013/65/EU.
[39] Decision 2000/518/EC.
[40] Decision 2012/484/EU.
[41] Decision 2002/2/EC.
[42] Commission Implementing Decision (EU) 2016/2295.
[43] The European Union and Japan agreed to create the world's largest area of safe data flows, 17 July 2018, European Commission; Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, COM(2017) 7 final, European Commission.

Biding Corporate Rules

Biding corporate rules or BCR's (Art. 46(2)(b) and 47 of the GDPR) are appropriate safeguards which may be used for data transfer within a corporate group. They allow companies to transfer personal data to their non-EEA affiliates. The DPD did not expressly mention binding corporate rules as appropriate safeguards, but they were nonetheless allowed as a ground for transfer of personal data to third countries or international organisations.[44] Biding corporate rules have to be approved by the national supervisory authority and are subject to two conditions, namely that they are legally binding, applied and enforced by every member concerned of the group of undertakings or enterprises including employees, and that they expressly confer enforceable rights on data subjects. The GDPR sets the minimum requirements for content of the BCR's. It has been indicated that biding corporate rules represent an efficient level of data protection in corporate structures, as well as a good marketing instrument. However, the costs of setting up and maintaining such framework are high.[45] A number of companies is using approved biding corporate rules.[46] Biding corporate rules have not been affected by *Schrems* or challenged before the CJEU.

Contractual Clauses

Contractual clauses as one of adequate safeguards were envisaged by the DPD (Art. 26(2) of the DPD). Contractual clauses may be standard contractual clauses or ad hoc clauses. Standard contractual clauses are one of the most effective grounds for personal data transfer for corporations to and from the US.[47] They may be adopted by the European Commission (Art. 46(2)(c) of the GDPR) or adopted by national supervisory authority and approved by European Commission (Art. 46(2)(d) of the GDPR). Under the GDPR, standard contractual clauses adopted by the Commission no longer have to be approved by national supervisory authorities. Clauses adopted by national supervisory authority and approved by European Commission are a novelty introduced by the GDPR. Ad hoc contractual clauses are authorised by the competent supervisory authority (Art. 46(3) of the GDPR). Even though ad hoc clauses could have been used as a basis for transfer of personal data to third countries and international organisations under DPD, GDPR introduced the obligation of national supervisory authorities to subject their approval to consistency mechanism (Art. 63 of the GDPR) which will ensure consistent approach throughout the EU.

European Commission has adopted four standard contractual clauses decisions under the DPD. By the first one, Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries,

[44]See Kuner (2017).
[45]Weber & Staiger (2017).
[46]European Commission, Binding corporate rules, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en.
[47]Weber & Staiger (2017) at 35-36.

under Directive 95/46/EC[48] European Commission has approved Set I of model clauses which may be used when the EU data controller transfers personal data to non-EEA data controller (Set I controller-controller).[49] The latter Decision was amended by Decision 2004/915/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.[50] By Decision 2004/915/EC European Commission has approved a new set of model clauses for transfers from EU controllers to non-EEA controllers (Set II controller-controller). Under the Set I controller-controller model clauses, the data exporter and the data importer are jointly and severally liable for the damage suffered by the data subject as a consequence of violation[51] and data subjects who are third-party beneficiaries may enforce clauses prescribing obligations of the data exporter and importer.[52] On the other hand, Set II controller-controller introduced liability regime based on due diligence obligations under which the data exporter and the data importer are liable towards the data subjects for their breach of contractual obligations. The data exporter is also liable for not using reasonable efforts in determining whether the data importer is able to fulfil legal obligations prescribed by clauses (*culpa in eligendo*) and may be sued by the data subject in this respect.[53] In terms of exercise of third-party beneficiary rights by data subjects, data exporters have a more active role. If the data subject alleges the violation by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer. If the data exporter does not take such action within a reasonable period (under normal circumstances one month), the data subject may enforce his rights against the data importer directly. A data subject may commence action against data exporter that has failed to use reasonable efforts to determine that the data importer is able to fulfil its legal obligations and the data exporter has the burden to prove otherwise.[54]

Remaining two European Commission Decisions regulate the transfer of personal data from the EU controller to non-EEA processor.[55] Standard contractual clauses from Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC[56] (Set I controller-processor) cannot be used any longer, but remain in force for transfers agreed prior to 15 May 2010. The fourth decision, Decision 2010/87/EU of 5 February 2010 on standard

[48]Decision 2001/497/EC.

[49]Art. 4(7) of the GDPR and Art. 2(d) of the DPD define controller as natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[50]Decision 2004/915/EC, 74-84.

[51]See Clause 6 of Set I controller-controller.

[52]See Clause 3 of Set I controller-controller.

[53]See Recital 5 of the Decision 2004/915 and Clause I(b) of Set II controller-controller.

[54]See Recital 6 of the Decision 2004/915 and Clause III of the Set II controller-controller.

[55]Art. 4(8) of the GDPR and Art. 2(e) of the DPD define processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[56]Decision 2002/16/EC.

contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council,[57] (Set II controller-processor) replaced the Decision 2002/16/EC. The reason for repealing Decision 2002/16/EC and replacing it by Decision 2010/87/EC was the necessity of modifying standard contractual clauses taking into consideration "expansion of processing activities and new business models for international processing of personal data".[58] In particular, this encompasses sub-processing. According to Set II controller-processor clauses data importer may subcontract processing operations if data exporter gave its consent and by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the clauses. If sub-processor fails to fulfil its contractual obligation, the data importer is fully liable to the data exporter for the performance of the sub-processor's obligations. According to Set II controller-processor clauses, the written agreement between the data importer and sub-processor has to contain a third-party beneficiary clause allowing the data subject to enforce his or her rights against the sub-processor if the claim can no longer be brought against data exporter or importer.[59]

In the aftermath of the *Schrems* decision, European Commission adopted Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC.[60] Decision 2001/497/EC and Decision 2010/87/EU were amended since the CJEU's decision from *Schrems* that national supervisory authorities remain competent to oversee the transfer of personal data to third country should *mutatis mutandis* apply to European Commission decisions which envisaged limited powers of national supervisory authorities in this respect.

Following the decision in *Schrems* which invalidated Safe Harbour, Facebook started relying on Decision 2010/87/EU for transfer of Facebook users' personal data to the US. As a result, Mr. Schrems decided to reformulate his complaint against Facebook before Irish Data Protection Commissioner. In her investigation, the Data Protection Commissioner raised concerns as to validity of all three sets of standard contractual clauses. After investigating the regime of protecting personal data in the US, she concluded that it does not provide for an effective legal remedy at disposal for EU citizens whose personal data is being transferred to the US. The Irish High Court in a 152-page judgment, often referred to *Schrems II,* decided to refer the issue of standard contractual clauses validity to the CJEU. The Court found that standard contractual clauses do not ensure an adequate level of data

[57]Decision 2010/87/EU.

[58]Safer standards for European citizens' data transfers to processors in third countries. See also Commission Staff Working Document on the Implementation of the Commissions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries.

[59]See Clause 11 of the Set II controller-processor. As stated in the Article 29 Working Party WP 176, 00070/2010/EN, 12 July 2010, whereas it is not possible under Decision 2010/87/EU to transfer personal data from the EU controller to EU processor and then to non-EU sub-processor, it is not clear whether it is possible to transfer personal data from the EU controller to non-EU processor and then to non-EU sub-processor.

[60]Commission Implementing Decision (EU) 2016/2297.

protection pointing out that national supervisory authorities under Art. 4 of Decision 2001/87/EC and Art. 28 of the DPD are authorised to prohibit or suspend data flows to third countries with the aim of protecting individuals with regard to the processing of their personal data.[61] Facebook attempted to stay the referral to the CJEU, but the Irish Court denied the request for stay.[62]

Other Appropriate (adequate) Safeguards

Unlike the DPD, GDPR provides for the possibility that public authorities or bodies conclude agreements which are legally binding enforceable instruments as a basis for the transfer of personal data without the need of specific authorisation of a national supervisory authority (46(2)(a) of the GDPR). If public authorities and bodies make administrative arrangements which include enforceable and effective data subject rights and which are not legally binding, such as memorandum of understanding, the competent supervisory authority has to authorise them (Art. 46(3)(b) of the GDPR).

GDPR envisages codes of conduct as a basis for the transfer of personal data to third countries and international organisations (Art. 46(2)(e) of the GDPR). Codes of conduct have to be approved in accordance with the procedure envisaged by Art. 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. Even though the DPD encouraged drawing up codes of conduct with the aim of contributing implementation of the national provisions adopted by the Member States (Art. 27 of the DPD), codes of conduct were not envisaged as a basis for the transfer of personal data to third countries.

GDPR introduced approved certification mechanism pursuant to Art. 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Art. 46(2) of the GDPR). Another GDPR ground for transfer, not previously envisaged by the DPD is a judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data which may only be recognised or enforceable if is based on an international agreement in force between the EU or a EU Member State and a third country, such as a mutual legal assistance treaty (Art. 48 of the GDPR).

Derogations

In the absence of previously mentioned bases for the transfer of personal data to third countries and international organisations, the GDPR provides for a number of derogations, majority of which were recognised under the DPD.

The transfer may take place based on the explicit consent of the data subject who was informed of the possible risks of transfers for the data subject due to the

[61] *The Data Protection Commissioner v Facebook Ireland Ltd*. 3 October 2017.
[62] *The Data Protection Commissioner v Facebook Ireland Ltd*, 2 May 2018.

absence of an adequacy decision and appropriate safeguards (Art. 49(1)(a) of the GDPR). The DPD, which contained the same derogation (Art. 26(1)(a) of the DPD), used the term unambiguous consent. The difference in wording should not create much difference in practical application of the provision. However, under GDPR, the data exporter will have to prove providing information on possible risk, which under the DPD was not a requirement.

Performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request and conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person are derogations which remained unchanged (Art. 49(1)(b) and (c) of the GDPR and Art. 26(1)(b) and (c) of the DPD), as well as establishment, exercise or defence of legal claims and transfer of data from public registers (Art. 49(1)(e) and (g) of the GDPR and Art. 26(1)(d) and (f) of the DPD). With respect to the public interest (Art. 49(1)(d) of the GDPR), GDPR unlike the DPD (Art. 26(1)(d)) clarifies that it should be recognised in Union law or in the law of the Member State (Art. 49(4)). Compared to the DPD, the GDPR extended the scope of the data subject's vital interests basis to cover third persons (Art. 49(1)(f) of the GDPR and Art. 26(1)(e) of the DPD).

Finally, if the transfer of personal data to a third country or an international organisation could not be performed on the basis of adequacy decisions, appropriate safeguards or mentioned derogations, there is still one remaining option, introduced by the GDPR. Namely, the transfer may take place if the following conditions are fulfilled: it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has accordingly provided suitable safeguards with regard to the protection of personal data. The controller has to inform the supervisory authority of the transfer and inform the data subject of the transfer and on the compelling legitimate interests pursued (Art. 49(1) of the GDPR).

A Greater Level of Protection of Personal Data?

For years now, one of the main aims of the European Area of Freedom, Security and Justice is stronger data protection.[63] EU Council, in The Stockholm Programme, the EU policy framework established in the light of entry into force of Lisbon Treaty, indicated EU citizen's data protection in information society as one of the goals for the five-year period it was established.[64] One of the most tangible results of these EU law and policymakers, the GDPR, states in its recital that its purpose is to build a "stronger and more coherent data protection framework".[65]

[63]De Hert & Riehle (2010).
[64]The Stockholm Programme, p. 18.
[65]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, p. 2.; Recital 7 of the GDPR.

However, it is questionable if the legislative and judicial developments in the last couple of years in the field of data protection managed to ensure a higher level of protection, at least when it comes to the issue of personal data transfer to the third countries and international organisations. When making an assessment as to the current level of protection, both quantity of data transfer grounds and quality of protection guaranteed within each ground have to be taken into consideration

First of all, compared to the DPD, GDPR increased the number of grounds based on which personal data transfer may be transferred to third countries. Even though the three main exceptions or grounds, namely adequacy decisions, appropriate (adequate) safeguards and derogations were maintained, the varieties within two of these grounds have proliferated. When it comes to appropriate (adequate) safeguards, the GDPR introduced the standard contractual clauses adopted by national supervisory authorities and approved by European Commission, legally binding and enforceable agreements between public authorities, administrative agreements between public authorities, codes of conduct, certification mechanisms, judgments of a court or tribunal and decisions of administrative authorities. Furthermore, an additional derogation was added, i.e. transfer which may take place based on compelling legitimate interests under certain conditions.

Secondly, the qualitative level of protection within each of the data transfer grounds does not necessarily rise. This especially refers to the standard of "adequacy" and "essential equivalence". Regarding adequacy decisions, the advantages that the GDPR introduced are an obligation of its periodical assessment at least every four years and more comprehensively defined the elements which have to be taken into consideration when making an adequacy assessment. However, it is not reassuring that more scrupulous procedure will result with more protection, especially taking into account the fact that European Commission has internal guidelines for assessing countries' adequacy which are not publicly available,[66] as well as the fact that making the comparison of levels of protection across various jurisdictions may be burdensome, time-consuming and sometimes even objectively questionable due to the variety of factors to be taken into consideration. In *Schrems*, the CJEU clarified that the required threshold is "essential equivalence" of third country data protection with the protection guaranteed by the EU Charter.[67] It is not clear how could, following that standard, Privacy Shield be enacted since the US has a completely different approach to protecting personal data than EU,[68] which is characterised by non-horizontal, sectoral approach to data protection, and legal remedies in case of personal data breach which are far less effective compared to the EU, especially for non-US citizens.[69] Furthermore, Privacy Shield cannot ensure greater protection to data subjects from invasions of their privacy by intelligence services, compared to Safe

[66]Kuner (2017) at 900-901.
[67]See supra chapter *From Safe Harbour to Privacy Shield.*
[68]On comparison of the EU and US approach to See Coley (2017).
[69]On relevant data protection laws and judicial protection in the US, see *The Data Protection Commissioner v Facebook Ireland Ltd*, 2 May 2018. See also Milanovic, M. (2015) at 88-89; Weber & Staiger (2017) at 39-61.

Harbour, since these violations occur without data subject's knowledge. Another concern with respect to the adequacy decisions is the fact that two countries covered by adequacy decisions, namely Canada and New Zealand, participate in Five Eyes intelligence alliance[70].

When standard contractual clauses are concerned, their development shows liberalisation towards transfer of data. Set I controller-controller from Decision 2001/497/EC prescribes joint and several liability of the data exporter and data importer. Since such liability is burdensome for the data exporter, the Set II controller-controller from Decision 2004/915/EC set up a liability regime based on due diligence of data exporter and importer for the breach of their obligations.[71] Set I controller-processor from Decision 2002/16/EC was replaced with Set II controller-processor from Decision 21010/97/EU in order to allow sub-processing. The validity of EU Commission's standard contractual clauses was brought into question on the grounds of adequacy, as well. The future of both Privacy Shield, other adequacy decisions as well as EC Commission standard contractual clauses is now dependent on CJEU's decisions.

As far as binding corporate rules, other appropriate safeguards and derogations are concerned, they have not proven to be as controversial as adequacy decisions and standard contractual clauses. Compared to the DPD, the GDPR contains stricter provisions on binding corporate rules prescribing their minimal content. Another ground for transfer in which the GDPR raised the level of protection by stating that if personal data is being transferred based on data subject's consent, the data subject has to be informed to data transfer risks.

It has been argued that the EU rules in certain areas have a global impact and impose "Brussels effect", i.e. unilateral regulatory standard. One of such areas is privacy protection in which the EU is perceived to set the stricter standard than other countries,[72] especially the US.[73] While the corpus of rules on data protection may create an image of a very high level of privacy protection, the implementation of these rules, at least in the area of transborder data transfer paints a different picture.[74] It seems as though the EU uses overregulation and formalism to mask the fact that it adjusts the level of protection to the level accepted in countries where relevant global stakeholders are located. The outlined development seems to further demonstrate that individuals and associations protecting internet privacy rights generate stronger impetus for data protection in the area of transborder data transfer than the EU legislator.

[70]An alliance of five English speaking countries, US, UK, Canada, New Zealand, Australia on haring intelligence. For more on Five Eyes Intelligence alliance see Nyst & Crowe (2014).
[71]Kong (2010) at 451.
[72]Leenes, van Brakel, Gutwirth & De Hert (2017).
[73]Bradford (2012) at 22-26.
[74]Kuner suggest that EU maintains "exalting illusion" that it may set data protection standards on a global level. Kuner (2017) at 910.

Conclusion

With the occurrence and the rapid development of internet, the data transfer became frequent and unavoidable. However, data transfers pose a great risk for privacy violations. In the EU, the transfer of personal data to third countries and international organisations is generally forbidden. The GDPR prescribes for three exceptions to this rule, i.e. grounds for transfer, namely adequacy decisions, appropriate safeguards and derogations. Even though the same rule, as well as the same grounds, were prescribed by the DPD, the number of variations within these ground has increased with the GDPR. Besides this quantitative proliferation in variations within grounds for transfer, the development concerning certain grounds such as standard contractual clauses, even prior to the GDPR, did not necessarily advance towards greater protection of privacy. Adequacy decisions and standard contractual clauses currently in force were all enacted under the DPD and are currently under the CJEU's scrutiny. It was suggested that they will most likely have to be replaced or amended in order to be brought into conformity with the GDPR regime. Such circumstances provide an opportunity for strengthening protection of data being transferred outside of the EU.

List of References

Aldhouse, F. (1999). 'The Transfer of Personal Data to Third Countries under EU Directive 95/46/EU' in *International Review of Law, Computers and Technology* 13(1):75-79.

Boehm, F. (2016). 'Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes' in *European Data Protection Law Review* 2:178-190.

Boehm, F. (2012). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Cham: Springer.

Bradford, A. (2012). 'The Brussels Effect' in *Northwestern University School of Law* 107(1):1-68.

Bu-Pasha, S. (2017). 'Cross-border issues under EU data protection law with regards to personal data protection' in *Information & Communications Technology Law* 26(3):213-228.

Byrne Sedgewick, M. (2017). 'Transborder Data Privacy as Trade' in *California Law Review* 105:1513-1542.

Cole, D. D., Fabbrini, F. & S. Schulhofer (2017). *Surveillance, Privacy and Trans-Atlantic Relations*. Oregon: Hart Publishing.

Coley, A. (2017). 'International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà vu' in *Hasting Law Journal* 68:1111-1134

Colonna, L. (2016). 'Europe Versus Facebook: An Imbroglio of EU Data Protection Issues' in: Gutwirth, S., Leenes, R., De Hert, P. (eds.), *Data Protection on the Move, Current Developments in ICT and Privacy/Data Protection*, 25-50. Cham: Springer.

Corcoran, D. D. (2016). 'Safe Harbor to Privacy Shield: A view from the USA – Part 1' in *Journal of Data Protection & Privacy* 1(1):89-102

Corcoran, D. D. (2017). 'Safe Harbor to Privacy Shield: A view from the USA – Part 2' in *Journal of Data Protection & Privacy* 1(2):160-172

De Hert, P. & C. Riehle (2010). Data protection in the area of freedom, security and justice, ERA Forum, 11: 59-167, available at: http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_363_restricted.pdf (13.7.2018)

Fahey, E. (ed.) (2018). *Institutionalisation beyond the Nation State Transatlantic Relations: Data, Privacy and Trade Law*. Cham: Springer

Geppert, N. (2016). 'Could the 'EU-US Privacy Shield' Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries?' available at SSRN: https://ssrn.com/abstract=2928 064 (13.7.2018) 1-44

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer

González Fuster, G. (2016). 'Un-Mapping Personal Data Transfers' in *European Data Protection Law Review* 2:160-168

Kong, L. (2010). 'Data Protection and Transborder Data Flow in the European and Global Context' in *The European Journal of International Law* 21(2): 441-456

Kuczerawy, A. (2011) 'Facebook and its EU users – Applicability of the EU data protection law to US based SNS'. In: M. Bezzi et al. (eds.), *Privacy and Identity*, IFIP AICT 320, 75–85, Cham: Springer, available at SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605013 (2.7.2018)

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press

Kuner, C. (2017). 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' *in German Law Journal* 18(4):881-918

Leenes, R., van Brakel, R., Gutwirth, S. & P., De Hert (2017). *Data Protection and Privacy: (In)visibilities and Infrastructure*, 11. Cham: Springer.

Milanovic, M. (2015). 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' in *Harvard International Law Journal* 56(1):81-146

Mouzakiti, F. (2015). 'Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive' in *European Data Protection Law Review* 1:39-51

Murray A. (2013). *Information Technology Law*. 2nd ed. Oxford: Oxford University Press

Nyst, C. & A. Crowe (2014). 'Unmasking the Five Eyes' global surveillance practices' in *Privacy International*, available at:
https://www.giswatch.org/sites/default/files/unmasking_the_five_eyes.pdf (13.7.2018)

Patzak, A., Hilgard, M. C. & T. Wybitul (2011). 'European and German Privacy Laws and Cross-Border Data Transfer in US Discovery Procedures' in *Dispute Resolution International* 5(2):127-139

Suda, Y. (2018). *The Politics of Data Transfer, Transatlantic Conflict and Cooperation over Data Privacy*. New York, London: Routledge

Voigt, P. & A. von dem Bussche (2017). *The EU General Data Protection Regulation (GDPR)*, A Practical Guide. Cham: Springer

Voss, G. W. (2016). 'The Future of Transatlantic Data Flows: Privacy Shield or Bust' in *Journal of Internet Law* 19(11):1, 9-18

Weber, R. H. & D. Staiger (2017). *Transatlantic Data Protection in Practice*. Cham: Springer

Whitaker, P. (2017). 'Bring on the Privacy Shield' in *Journal of Data Protection & Privacy* 1(3):306-311

Legislative Acts

Charter of Fundamental Rights of the European Union, OJ C 202, 7 June 2016.

Commission Decision 2000/520 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, notified under document number C(2000) 2441, OJ L 215, 25.8.2000, at 7-47.

Commission Implementing Decision (EU) 2016/1250 of 12 July 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-U.S. Privacy Shield (notified under document C(2016) 4176), C/2016/4176, OJ L 207, 1.8.2016, at. 1-112.

Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8353) (Text with EEA relevance), C/2016/8353, OJ L 344, 17.12.2016, at. 83–91.

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8471), C/2016/8471, OJ L 344, 17.12.2016, at 100-101.

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, at 31-50

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/ JHA (the Data Protection Directive for the police and criminal justice sector) OJ L 119, 4.5.2016, at 89-131.

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), Brussels, 25.1.2012, COM(2012) 11 final 2012/0011 (COD).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, OJ L 119, 4.5.2016, at 1-88.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, at 1-22.

1981 Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C (2000) 2304) (Text with EEA relevance.), OJ L 215, 25.8.2000, at 1–3.

2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document number C(2001) 1539), OJ L 181, 4.7.2001, at 19-31.

2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), OJ L 2, 4.1.2002, at 13-16.

2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 4540), OJ L 6, 10.1.2002., at 52-62.

2003/490/EC: 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 (Text with EEA relevance), OJ L 168, 5.7.2003, at 19-22

2003/821/EC: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Text with EEA relevance) (notified under document number C(2003) 4309), OJ L 308, 25.11.2003, at 27–28

2004/411/EC: Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.4.2004, at 48-51

2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271), OJ L 385, 29.12.2004, at 74-84.

2008/393/EC: 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 (notified under document number C(2008) 1746) (Text with EEA relevance), OJ L 138, 28.5.2008, at 21-23

2010/87/EU: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), OJ L 39, 12.2.2010, at 5-18

2010/146/: Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (notified under document C(2010) 1130) (Text with EEA relevance), OJ L 58, 9.3.2010, at 17-19

2010/625/EU: 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 (notified under document C(2010) 7084) Text with EEA relevance, OJ L 277, 21.10.2010, at 27-29

2011/61/EU: 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 automated processing of personal data (notified under document C(2011) 332) Text with EEA relevance, OJ L 27, 1.2.2011, at 39-42

2012/484/EU: Commission Implementing Decision of 21 August 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 with regard to automated processing of personal data (notified under document C(2012) 5704) Text with EEA relevance, OJ L 227, 23.8.2012, at 11–14

2013/65/EU: 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 by New Zealand (notified under document C(2012) 9557) Text with EEA relevance, OJ L 28, 30.1.2013, at 12–14..

Cases

(The) Data Protection Commissioner v Facebook Ireland Ltd, 3 October 2017 [2016 No. 4809 P.] (High Court).

(The) Data Protection Commissioner v Facebook Ireland Ltd, 2 May 2018 [2016 No.4809P.] (High Court).

Digital Rights Ireland v Commission, T-670/16, EU:T:2017:838. Judgment of 22 November 2016.

Maximillian Schrems v Data Protection Commissioner, Judgment of 6 October 2015, C-362/14, EU:C:2015:650.

Opinion of Advocate General Bot of 23 September 2015 in *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:627

Order of 25 October 2016, *La Quadrature du Net and Others v Commission*, T-738/16.

Other Sources

Article 29 Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13.4.2016

Article 29 Working Party WP 176, 00070/2010/EN, 12 July 2010

Commission Staff Working Document on the Implementation of the Commissions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, SEC (2006) 95, 20 January 2006

European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en

Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, COM (2017) 7 final, European Commission, available: https://ec.europa.eu/newsroom/document.cfm?doc_id=41157 (accessed 11.8.2018)

Privacy Shield Framework, available at https://www.privacyshield.gov/list (accessed 11.8.2018)

Report "Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and United States", Sidley January 2016

Safer standards for European citizens' data transfers to processors in third countries, IP/10/130, 5 February 2010, Brussels, SEC(2006)95, 20.1.2006 http://ec.europa.eu/justice_home/fsj/privacy/docs/modelcontracts/sec_2006_95_en.pdf (8.6.2018)

The European Union and Japan agreed to create the world's largest area of safe data flows, 17 July 2018, European Commission, available at http://europa.eu/rapid/press-release_IP-18-4501_en.htm (accessed 11.8.2018)

The Stockholm Programme - An open and secure Europe serving and protecting the citizen, Brussels, 2 December 2009, 17024/09, p. 18. Available at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/the_stockholm_programme_-_an_open_and_secure_europe_en_1.pdf (13.7.2018)

Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12, 24.7.1998.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (2.7.2018)

1990 UN Guidelines for the Regulation of Computerized Personal Data Files, available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/un-guidelines (2.7.2018)