MANAGING INNOVATIVE COMPANY'S CAPITAL: THE CASE OF PERSONAL DATA TRANSFER

*Dr. sc. Danijela Vrbljanac**

UDK: 347.152::004
https://doi.org/10.30925/zpfsr.39.4.19
Ur.: 20. rujna 2018.
Pr.: 20. listopada 2018.
Prethodno priopćenje

Summary

Not many areas of European law proved themselves as controversial as data protection. The only case in which this issue could become more debatable is if personal data crosses EU borders. The transfer of personal data to third countries proved its disputed status when the CJEU invalidated the Safe Harbour Agreement, one of the frameworks for the transfer of personal data to the US and several more came under the CJEU's scrutiny, including the Safe Harbour Agreement's successor, the Privacy Shield Agreement. It has been suggested that some of these instruments for transfer need to be repealed or amended in order to be brought in conformity with the GDPR. The paper, after analysing each of the grounds for transfer which may be used by EU companies, argues that regardless of the recent entry into force of the GDPR, the data protection "revolution" is still not complete, at least as far the transborder data flows are concerned.

Keywords: *data protection; EU law; General Data Protection Regulation; privacy; transborder data flows; transfer of data.*

1. INTRODUCTION

In the wake of Snowden revelations in 2013 on mass surveillance and collection of data, the issue of privacy protection, particularly the transfer of personal data, was brought to the attention of the European legal public. 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

* Danijela Vrbljanac, Ph.D., Postdoctoral Fellow, University of Rijeka Faculty of Law; danijela.vrbljanac@pravri.hr.
This paper is written under 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".

Regulation, hereinafter: the GDPR)[1], effective from May 2018, maintained the rules of personal data transfer from its predecessor in most part. Regardless of the fact that GDPR interventions in data transfer rules were not as extensive as in certain other areas, this matter remains to be one of the most controversial ones in data protection. Grounds for the transfer of personal data to third countries enacted under the GDPR's predecessor are still in force, albeit their validity and compliance with the new regime has been brought into question. The aim of this paper is to analyse the grounds which may be invoked by EU companies to transfer data outside the EEA and outline the development of these instruments in recent years, especially after the GDPR entered into force; compare the transfer of personal data from EU companies to non-EEA companies with the transfer between EEA companies, as well as to pinpoint certain issues which might be problematic and still require the attention of the EU legislator and the CJEU.

2. INNOVATIVE COMPANIES AND DATA

The rapid development of information technology in the last two decades has significantly altered the way businesses operate. There is virtually no part of the business landscape that has not been affected by technological advancement in terms of browsing, collecting, and storing information, marketing, offering and acquiring goods and services, completing transactions, communicating and interacting etc. However, innovative companies are the ones which managed to take advantage of information progress for leveraging large amount of data into revenue and making data the foundation of their income, since data is considered to be the commodity of the 21st century.[2]

In such environment, data transfer becomes a part of daily activities of companies, especially innovative ones. To borrow economic terminology, data represents a nonrivalrous good, meaning that its "consumption" by one person does not prevent simultaneous consumption by another.[3] Data as a nonrivalrous good, sometimes

1 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, pp. 1-88; Corrigendum to 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) (OJ L 119, 4.5.2016), OJ L 127, 23.5.2018, pp. 2-5.

2 See Janal, R., Fishing for an Agreement: Data Access and the Notion of Contract, in: Lohsse, S./Schulze, R./Staudenmayer, D. (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, p. 283.

3 See Lohsse, S./Schulze, R./Staudenmayer, D., Trading Data in the Digital Economy: Legal Concepts and Tools, in: Lohsse, S./Schulze, R./Staudenmayer, D. (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, p. 15; Zimmer, D., Property Rights Regarding Data, in: Lohsse, S./Schulze, R./Staudenmayer, D. (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-

referred to as informational good, may be subdued to a binary information, which makes it, by its very nature, susceptible to being easily transferred. The described setting of large amount of data flowing from one subject to another facilitates and multiplies data abuses and privacy violations.

3. DATA TRANSFERS

The GDPR represents the principal, horizontal source of EU law on data protection effective from 25 May 2018, thus replacing its 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 DPD)[4]. The conditions under which EU companies may transfer data to third countries or international organisations will differ depending on whether that data is being transferred to the controllers and processors outside of the EEA or within the EEA. In both cases, only personal data of natural persons is protected.[5] That encompasses personal data of companies employees, as well.[6] The fact that information is connected to professional activity does not mean it will be stripped of protection as personal data. Such information encompasses for instance names and surnames of persons appearing in minutes from a meeting,[7] record of employees working time,[8] information on which expert is author of a particular comment made by external experts group,[9] names and surnames mentioned on a reserve list for an open competition and individual decisions concerning the appointment of officials,[10] surnames belonging to members of decision-making bodies who participated in the meetings of those bodies in connection with the exercise of their public duties which were published in the OJ or on the internet.[11]

3.1. Transfers of Data Outside the EEA

The transfer of personal data to third countries[12] and international organisations is regulated by Chapter V of the GDPR (previously Chapter IV of the DPD). The

Baden, Nomos, 2017, p. 105.

4 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, pp. 31-50.

5 Both the GDPR and the DPD protect only natural persons' personal data. See Art. 1(1) of the GDPR and Art. 1(1) of the DPD.

6 However, the notion of natural person's personal data does not necessarily cover personal data of a sole director of a company which is included in the company register. See judgment of 9 March 2017 in *Manni*, C-39/15, EU:C:2017:197.

7 Judgment of 29 June 2010, *Bavarian Lager*, C-28/08 P, EU:C:2010:378, paragraph 68-70.

8 Judgment of 30 May 2013, *Worten*, C-342/12, EU:C:2013:355, paragraph 19.

9 Judgment of 16 July 2015, *ClientEarth*, C-615/13 P, EU:C:2015:489, paragraphs 29-34.

10 Judgment of 7 July 2011, *Jordana*, T-161/04, EU:T:2011:337, paragraph 91.

11 Judgment of 11 June 2015, *McCullough*, T-496/13, EU:T:2015:374, paragraph 66.

12 The term third country refers to countries other than EU Member States, Norway, Liechtenstein and Iceland.

territorial scope of the GDPR is set rather broadly. It applies to data processed by an establishment of a controller[13] or a processor[14] in the EU regardless of whether the processing takes place on the territory of the EU. It also covers the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, if the processing activities are related to the offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the Union or to the monitoring of their behaviour as far as their behaviour takes place within the EU.[15] However, the ambit of chapter on transfer of personal data to third countries and international organisations concerns only data which is being exported from the EU to a third country or an international organisation. It does not cover the transfer of personal data of EU data subjects which are being transferred by non-EEA based controllers and processors to third country or international organisation.[16] Such limitation of the scope of provisions on cross-border data transfer leaves personal data of EU data subjects processed by non-EEA based controllers and processors out of reach from GDPR protection when it comes to the transfer of such data.

As a principle, the transfer of personal data to third countries and international organisations is forbidden.[17] However, there are three possible exceptions or grounds for the transfer of personal data to third countries and international organisations which were taken over from the DPD. Those are: adequacy decisions, appropriate safeguards and derogations. EU companies may transfer personal data to third countries or international organisations if one of those grounds exists in a particular case.

3.1.1. Adequacy decisions

Adequacy decisions are European Commission decisions that a third country, a

13 GDPR defines controller as a 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. Art. 4(7) of the GDPR. See also Art. 2(d) of the DPD. The definition of the controller was taken from the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data concluded in 1981 with a slightly different wording. Council of Europe, Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, Strasbourg, Art. 2(d), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (31.8.2018).

14 Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Art. 4(8) of the GDPR. See also Art. 2(e) of the DPD.

15 Art. 3(1) and (2) of the GDPR. By protecting EU data extraterritorially, EU data protection rules are considered to set the global standard of data protection. See Suda, Y., The Politics of Data Transfer, Transatlantic Conflict and Cooperation over Data Privacy, New York, London, Routledge, 2018, pp. 113-115; Bradford, A., The Brussels Effect, Northwestern University School of Law, Vol. 107, 1/2012, pp. 22-26. Compared to the GDPR, the DPD set the scope of application more narrowly. See Art. 3 of the DPD.

16 See the wording of Recital 101 of the GDPR Preamble.

17 Art. 44 of the GDPR. The same general principle was prescribed by Art. 25(1) od the DPD.

territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection.[18] If the European Commission reaches an adequacy decision, an EU company does not have to seek authorisation or fulfil additional conditions in order to transfer data to third country or international organisation. Currently in force are adequacy decisions with respect to eleven countries: Andorra,[19] Argentina,[20] Faroe Islands,[21] Guernsey,[22] Israel,[23] Isle of Man,[24] Jersey,[25] New Zealand,[26] Switzerland,[27] Uruguay[28] and the US.[29] With respect to Canada, the EU recognised that Personal Information Protection and Electronic Documents

18 Art. 45(1) of the GDPR. See also Art. 25(1) of the DPD.

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, pp. 27-29.

20 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, pp. 19-22.

21 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, pp. 17-19.

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, pp. 27-28.

23 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, pp. 39-42.

24 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, pp. 48-51.

25 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, pp. 21-23.

26 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, pp. 12-14.

27 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, pp. 1-3.

28 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, pp. 11-14.

29 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, pp. 1-112.

Act (PIPEDA) provides an adequate level of protection. Since PIPEDA is a federal law which concerns only private-sector organisations, Canada adequacy decision is limited to transfer of data solely to these companies.[30] European Commission is at the moment conducting negotiations for adequacy decisions with respect to South Korea and Japan.[31]

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) is an adequacy decision with respect to the US which replaced the previous adequacy decision, 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)[32] in July 2016. The Safe Harbour was invalidated by the CJEU in the proceeding brought by Mr. Schrems against Irish Data Protection Commissioner. In the light of the Snowden revelations in 2013, Mr. Schrems sought from Facebook Ireland, a subsidiary of Facebook Inc., to stop transferring his personal data to a server in the US. After the Data Protection Commissioner rejected his claim, Mr. Schrems instituted the proceedings before the Irish High Court which sought clarification from the CJEU. The CJEU established that Safe Harbour cannot prevent national supervisory authorities from calling into question the level of privacy protection in the US and established that its provisions do not contain sufficient finding according to which the level of protection in the US would be essentially equivalent to the one in the EU, especially taking into account the US intelligence services overreach in collecting and processing data.[33]

In addition to 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.[34]

30 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, pp. 13-16.

31 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 27.8.2018); Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, COM(2017) 7 final, European Commission, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=41157 (accessed 27.8.2018).

32 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, pp. 7-47.

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

34 Judgment *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650,

Both the Safe Habour Decision and the Privacy Shield are based on a mechanism according to which a US company which seeks to receive data collected in the EU has to self-certify[35] before the US Department of Commerce and both of them rely on seven principles (Notice, Choice, Onward Transfers, Access, Security, Data Integrity, and Enforcement).[36] The main improvements in the Privacy Shield concern the Notice Principle, Onward Transfer Principle and Recourse, Enforcement and Liability Principle. Notice principle requires companies to provide data subjects with greater quantity of information. Onward Transfer Principle prescribes the obligation for companies transferring data to third party controllers to conclude contracts with these third parties which will oblige them to ensure the same level of protection as the Privacy Shield Principles, as well as to process data only for limited and specified purposes. If the company processes data using a third party agent, a GDPR compliant agreement has to be concluded with the third party agent. Under Recourse, Enforcement and Liability Principle the position of data subjects has been strengthened. Data subjects may file complaints before independent dispute resolution bodies and supervisory authorities. The US Department of Commerce also has a role in resolving complaints. Data subjects have at their disposal binding arbitration by a "Privacy Shield Panel" of at least 20 arbitrators chosen by the US Department of Commerce and the European Commission.

The proceedings of rendering the adequacy decision has changed to some extent with the GDPR. First of all, GDPR prescribes with more scrutiny which elements should be taken into consideration. According to Art. 45(2) the Commission should particularly take into account three categories of elements. The first one is the rule of law, respect for human rights and fundamental freedoms, relevant general and sectoral legislation, including the one concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred. The second one is the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement

paragraphs 79-106.

35 On 18 September 2018, there are 3739 active companies certified under the Privacy Shield. See Privacy Shield Framework, available at: https://www.privacyshield.gov/list (18.9.2018).

36 The Privacy Shield was supplemented with 16 supplemental principles: 1. Sensitive Data, 2. Journalistic Exceptions, 3. Secondary Liability, 4. Performing Due Diligence and Conducting Audits, 5. The Role of the Data Protection Authorities, 6. Self-Certification, 7. Verification, 8. Access, 9. Human Resources Data, 10. Obligatory Contracts for Onward Transfers, 11. Dispute Resolution and Enforcement, 12. Choice – Timing of Opt-Out, 13. Travel Information, 14. Pharmaceutical and Medical Products, 15. Public Record and Publicly Available Information, 16. Access Requests by Public Authorities.

powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States. The third one are international commitments the third country or international organisation has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data. The DPD in Art. 25(2) mentioned the nature of the data, purpose and duration of the proposed processing operation or operations, country of origin and country of final destination, rules of law - both general and sectoral - in force in the third country in question and the professional rules and security measures which are complied with in that country.

Furthermore, the GDPR has introduced a mechanism for periodic review at least every four years of the level of privacy protection in the third country or international organisation with respect of which an adequacy decision was enacted.[37] All of the adequacy decisions were enacted under the DPD. Even though the GDPR does not contain the sunset clause concerning adequacy decisions brought under the previous DPD regime,[38] it has been argued that these decisions will have to be replaced or amended to be brought in conformity with the GDPR.

The validity of the Privacy Shield has been called into question before the General Court of the EU. Digital Rights Ireland, a non-profit organisation for protecting internet freedoms challenged the Privacy Shield by stating that it is contrary to the EU Charter of Fundamental Rights. However, the applicant did not have standing.[39] Another non-profit organisation from France, La Quadrature du Net instituted the proceedings challenging the Privacy Shield, which is still ongoing, claiming that the level of data protection in the US is not essentially equivalent to the level of protection in the EU.[40] Apart from being challenged before the CJEU, the Privacy Shield was justifiably criticised for not tackling some of the Safe Harbour major concerns. This primarily refers to the fact that Privacy Shield did not solve the matter of intelligence services collecting data indiscriminately, in bulk and without the data subject's knowledge.[41]

In *Schrems*, the CJEU explained that assessing adequacy of a third country means establishing whether data protection rules in third country are "essentially equivalent" to data protection in the EU where privacy and data protection are raised to the highest level of protected fundamental rights by Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union.[42] Essential equivalence thus requires

37 Art. 45(3) of the GDPR.

38 Art. 45(9) of the GDPR.

39 Judgment of 22 November 2011, *Digital Rights Ireland v Commission*, T-670/16, EU:T:2017:838.

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

41 See Kuner, C., Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal, Vol. 18, 4/2017, p. 912; Schrems, M., The Privacy Shield is a Soft Update of the Safe Harbor, Foreword, European Data Protection Law Review, 2/3016, p. 3; WP 238, Article 29 Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 13.4.2016, available at: https://www.pdpjournals.com/docs/88536.pdf (31.8.2018).

42 Charter of Fundamental Rights of the European Union, OJ C 202, 7 June 2016. See also Boehm, F., Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonised Data Protection Principles for Information Exchange at EU-level,

that a third state ensures a high level of protection of fundamental rights which is established based on the 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 data protection and privacy. Self-certification is not in itself contrary to essential equivalence. However, there has to be a mechanism for establishing and effective detection, supervision and punishment of infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data. Furthermore, essential equivalence has to be periodically checked by the Commission.[43] It is not entirely clear how the US, based on these conditions and extensive requirements from Art. 45(2) of the GDPR, can be assessed as a country ensuring an adequate level of data protection. The US has a completely different approach to protecting data compared to the EU. What is more, the US legal system does not provide for the horizontal protection of data, but rather a sectoral one and the enforcement of data protection is not as effective as the one in the EU, especially for non-US citizens.[44]

3.1.2. Appropriate Safeguards

If the EU company wants to transfer data to a third country or an international organisation which is not covered by the adequacy decisions, it may do so if it provides appropriate safeguards and under the condition that enforceable rights and effective

Cham, Springer, 2012, pp. 12-173; Boehm, F., Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes, European Data Protection Law Review, 2/2016, pp. 178-190; González Fuster, G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham, Springer, 2014.

43 Judgment *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650, paragraphs 73-89. For more on essential equivalence and adequacy see Kuner, C., op. cit., pp. 895-902; Roth, P., Adequate Level of Data Protection in Third Countries Post-*Schrems* and under the *General Data Protection Regulation*, Journal of Law, Information and Science, Vol. 25, 1/2017, pp. 49-67; Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and United States, Sidley Report, January 2016, available at: https://www.sidley.com/-/media/publications/essentially-equivalent---final.pdf?la=en (31.8.2018).
Besides the "essential equivalence", a standard developed by the CJEU, Art. 29 Working party established "European essential guarantees" standard which is to be differentiated from "essential equivalence" and provide guidance when assessing if an interference with a fundamental right can be justified and applied to all data processing operations. See WP 237, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Art. 29 WP, 13 April 2016, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf (31.8.2018.)

44 Coley, A., International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà vu' in Hasting Law Journal, Vol. 68, 2017, pp. 1118 -1129; On data protection in the US see also Milanovic, M., Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal, Vol. 56, 1/2015, pp. 88-89; Weber, R. H., Staiger, D., Transatlantic Data Protection in Practice, Cham, Springer, 2017, pp. 39-61.

legal remedies are available for data subjects.[45] Appropriate safeguards are binding corporate rules (hereinafter: the BCRs), contractual clauses, agreements between public authorities, approved codes of conduct and certification mechanisms.

3.1.2.1. Contractual Clauses

Contractual clauses may be standard contractual clauses or ad hoc clauses. Standard contractual clauses may be adopted by the European Commission in accordance with the examination procedure referred to in Art. 93(2) of the GDPR[46] or adopted by a national supervisory authority and approved by the European Commission under the same procedure[47]. Contractual clauses adopted by a national supervisory authority and approved by the European Commission were introduced as a ground for transfer with the GDPR. Ad hoc contractual clauses are authorised by the competent supervisory authority in accordance with the consistency mechanism[48]. Data transfers based on approved standard contractual clauses and approved ad hoc clauses do not require any further authorisation by supervisory authority.

Standard contractual clauses adopted by the Commission are the most commonly used ground for data transfer, not just among contractual clauses but in general. It has been suggested that standard contractual clauses offer the most efficient and reliable way for companies transferring data to and from the US.[49] Standard contractual clauses may be inserted into a wider contract and additional safeguards may be added provided that they do not contradict the provisions of standard contractual clauses.[50] European Commission has adopted four sets of standard contractual clauses decisions based on Art. 26(2) of the DPD, which are still valid until amended, repealed or replaced.[51] The first set adopted in Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC European Commission is intended for data transfers from EU data controller to non-EEA data controller (Set I controller-controller).[52] Decision 2001/497/EC 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 which introduced a new set of model clauses for transfers from EU controllers to non-EEA controllers (Set II controller-controller).[53] The two sets differ on matters of liability and

45 Art. 46(1) of the GDPR.
46 Art. 46(2)(c) of the GDPR
47 Art. 46(2)(d) of the GDPR
48 Art. 46(3) of the GDPR.
49 Weber, R. H., Staiger, D., op. cit., p. 35.
50 Recital 109 of the GDPR Preamble.
51 Art. 46(5) of the GDPR.
52 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, pp. 19-31.
53 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, pp. 74-84.

third-party beneficiary rights. The Set I controller-controller model clauses, prescribes that the data exporter and the data importer are jointly and severally liable for the damage suffered by the data subject as a consequence of a breach of data importer and data exporter's obligations. Under Set I controller-controller, data subjects who are third-party beneficiaries may enforce clauses prescribing obligations of the data exporter and importer. The liability regime in Set II controller-controller is 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. In exercising third-party beneficiary rights by data subjects, data exporters have a more active role. If the data subject alleges breach 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 do so within a reasonable period (which under normal circumstances would be one month), the data subject may enforce his rights against the data importer directly. The data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (*culpa in eligendo*) and the data subject can take action against the data exporter in this respect. EU companies which perform controller processing activities wishing to transfer data to non-EU controller may choose between the two sets. Set II seems to be less burdensome for EU companies wishing to transfer data outside of the EEA since it does not prescribe joint and several liability.[54]

The European Commission adopted two decisions intended for transfers of personal data from EU controller to non-EEA processor. Set I controller-processor 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[55] cannot be used any longer, but remains to be in force for transfers agreed prior to 15 May 2010. Set II controller-processor enacted with the Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC[56] of the European Parliament and of the Council replaced the previous set. Set I controller-processor prescribed primary liability of the data exporter, while the Set II controller-processor, similarly to Set II controller-controller, provides that the data exporter and the data importer are liable for their own breach. Set II controller-processor contains another crucial difference compared to Set I

54 For a similar reasoning see Kong, L., Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law, Vol. 21, 2/2010, p. 451; Kuan Hon, W., Data Localization Laws and Policy, The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens, Cheltenham, Northampton, Edward Elgar, 2017, p. 190.

55 Decision 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., pp. 52-62.

56 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, pp. 5-18.

controller-processor, i.e. the fact that it allows for sub-processing. Introducing the possibility of outsourcing by the processor of its processing activities (sub-processing) to other sub-processor or sub-processors while ensuring the protection of data subjects was, in fact, the main reason for introducing Set I controller-processor.[57] Pursuant to Set II controller-processor clauses, the data importer has to acquire prior written consent of the data exporter before subcontracting any of its processing operations performed on behalf of the data exporter under the provisions of the Decision 2010/87/EU. When the data importer subcontracts its obligations under the provisions of the Decision 2010/87/EU, it has to enter into 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 Decision 2010/87/EU. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer remains fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement. The prior written contract between the data importer and the sub-processor has to contain a third-party beneficiary clause for cases in which the data subject is not able to bring the claim for compensation against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and there is no successor entity assuming the entire legal obligations of the data exporter or data importer. Even though the Set II controller-processor clause presents an improvement taking into consideration the requirements of technological advancement and data economy, it was criticised for not being well adjusted to situations in which there are multiple data importers, since it proved to be cumbersome for companies in terms of paperwork and time requirements. Furthermore, Set II controller-processor cannot be used in the event EU controller transfers data to EU-processor which further transfers it to non EEA sub-processor.[58]

In the aftermath of the *Schrems* decision, the European Commission adopted the 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. Decision 2001/497/EC and Decision 2010/87/EU were amended since the CJEU's established in *Schrems* that rule according to which 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, along with other multinational technology companies,[59] started relying on Decision

57 Decision updating the standard contractual clauses for the transfer of personal data to processors established in non-EU countries, Press Release, Brussels, 5 February 2010, available at: http://europa.eu/rapid/press-release_MEMO-10-30_en.htm?locale=en (31.8.2018).

58 Wojtan, B., The new EU Model Clauses: One step forward, two steps back?, International Data Privacy Law, Vol. 1, 1/2011, available at: https://academic.oup.com/idpl/article/1/1/76/759672 (31.8.2018.).

59 Bu-Pasha, S., Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, Vol. 26, 3/2017, p. 221; Voss, G.

2010/87/EU for transfer of Facebook users' personal data to the US. As a result, Mr. Schrems reformulated his claim and sought from Irish Data Protection Commissioner to suspend data transfer under Decision 2010/87/EU without questioning the validity of the Decision. However, the Data Protection Commissioner decided to investigate the validity of all three sets of standard contractual clauses. The Irish High Court found that Commissioner's allegations that standard contractual clauses might be invalid are convincing. The Court found that standard contractual clauses do not ensure an adequate level of EU citizen's data protection nor have an effective remedy at their disposal in the US which is contrary to Art. 47 of the Charter.[60] In April 2018, it decided to refer a question for preliminary ruling to the CJEU.[61] The future of standard contractual clauses, as a ground for transfer frequently used by EU companies, including multinational internet technology companies, is thus in the hands of the CJEU.

3.1.2.2. Binding Corporate Rules

BCRs[62] are appropriate safeguards intended for companies forming a corporate group allowing them to transfer data to their non-EEA affiliates. Even though they were not expressly mentioned by the DPD as one of the appropriate safeguards, they were nonetheless accepted as one of the grounds for transborder data flows.[63] BCRs are suitable for various types of corporate groups which may vary in different EU Member States. However, they are considered to be most effective for multinational companies. Under the DPD, it was suggested that BCRs might not be the best option for loose conglomerates of diverse member companies due to their broad range of

V., The Future of Transatlantic Data Flows: Privacy Shield or Bust, Journal of Internet Law, Vol. 19, 11/2016, p. 10. The European Court of Justice to rule on the validity of standard contractual clauses, Linklaters, 30 May 2016, pp. 1-2, available at: https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/brussels/160530_alert_the_european_court_of_justice_to_rule_on-the_validity_of_standard_contractual_clauses.ashx (31.8.2018).
See, for instance, Google Cloud Platform, EU Model Contract Clauses, available at: https://cloud.google.com/terms/eu-model-contract-clause (18.9.2018); Facebook, What is a standard contractual clause?, available at: https://www.facebook.com/help/566994660333381?ref=dp&locale=en_GB (18.9.2018), https://www.facebook.com/about/privacy/update (18.9.2018); Microsoft Office, Frequently Asked Questions, available at: https://products.office.com/en-us/business/office-365-trust-center-eu-model-clauses-faq (18.9.2018).

60 High Court, *The Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, 3 October 2017 [2016 No. 4809 P.], available at: https://dataprotection.ie/docimages/documents/Judgement3Oct17.pdf (18.9.2018).

61 High Court, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, Request for a Preliminary Ruling,* 12 April 2018 [2016 No. 4809 P.], available at: http://www.europe-v-facebook.org/sh2/ref.pdf (18.9.2018).

62 Art. 47 of the GDPR.

63 See Kuner, C., op. cit., pp. 906-907. BCRs were acknowledged as an appropriate safeguard by WP 74, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Art. 29 WP, 3 June 2003, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (31.8.2018).

processing activities. In the latter cases, it was recommended to set up subgroups within loose conglomerats which will have separate BCRs.[64] However, the GDPR seems to have broadened the variety of undertakings which may use BCRs. Art. 47(1)(a) of the GDPR, besides group of undertakings, mentions group of enterprises engaged in a joint economic activity which suggests that BCRs may be used by groups of undertakings without formal structure, such as business partner companies. Although neither the GDPR, nor the DPD, formally set a hierarchy among appropriate safeguards, it has been argued that BCRs should be used as an additional tool for transborder data transfer when existing instrument for transfer prove to be problematic.[65]

In order to be a valid ground for data transfer, BCRs have to be legally binding and apply to and be enforced by every member concerned of the group of undertakings, or enterprises engaged in a joint economic activity, including their employees. Additionally, BCRs have to expressly confer enforceable rights on data subjects with regard to the processing of their personal data. The GDPR prescribes the minimum content of the BCRs.[66] The DPD did not contain equivalent provision, but the content of BCRs was prescribed by Art. 29 Working Party in several working papers.[67] It has been pointed out that the GDPR prescribes lesser requirements concerning the BCRs

64 WP 74, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Art. 29 WP, 3 June 2003, p. 9., available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (31.8.2018).

65 WP 74, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Art. 29 WP, 3 June 2003, p. 6., available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (31.8.2018).

66 Art. 47(2) of the GDPR. See also WP 256, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Art. 29 WP, 29 November 2017, available at: https://iapp.org/media/pdf/resource_center/wp256_BCR_11-2017.pdf (31.8.2018) and WP 257, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, Art. 29 WP, 29 November 2017, available at: https://iapp.org/media/pdf/resource_center/wp257_BCR-processor.pdf (31.8.2018).

67 Art. 29 WP indicated the content of the BCRs in their working papers. See, for instance WP 74, pp. 14-15; WP 108, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, Art. 29 WP, 14 April 2005, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf (31.8.2018); WP 153, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Art. 29 WP, 14 June 2008, available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf (31.8.2018); WP 154, Working Document Setting up a framework for the structure of Binding Corporate Rules, Art. 29 WP, 24 June 2008, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf; WP 195, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, Art. 29 WP, 6 June 2012, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (31.8.2018); WP 204 rev 1.0, Explanatory Document on the Processor Binding Corporate Rules, Art. 29 WP, 19 April 2013, last revised and adopted on 22 May 2015, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf (31.8.2018)

content.[68]

The BCRs have to be authorised by a supervisory authority in the relevant Member State in accordance with the consistency mechanism set out in Art. 63 of the GDPR, under which the European Data Protection Board (EDPB) will issue a non-binding opinion on the draft decision submitted by the competent supervisory authority.[69] Companies have to identify the leading supervisory authority based on elements suggested in WP 263 rev 1.0, the most important of which is the location of the group's European headquarters, to which they submit the BCRs draft which will manage the cooperation process with other relevant supervisory authorities, i.e. authorities of those Member States from which the data will be exported.[70] Once the BCRs are authorised under the described scheme, unlike under the DPD, no further specific authorisation will be required from the supervisory authority. By 24 May 2018, there were 130 companies using BCRs which were authorised under the DPD.[71] These BCRs, just as it is the case with adequacy decisions and standard contractual clauses, remain to be in force until they are amended, repealed or replaced.

3.1.2.3. Other appropriate safeguards

Both the GDPR[72] and the DPD[73] encourage drawing up codes of conduct.

68 Pateraki, A., EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?, Bloomberg BNA World Data Protection Report, Vol. 16, 3/2016, pp. 2-3, available at: https://www.huntonak.com/images/content/3/2/v3/3291/EU-Regulation-Binding-Corporate-Rules-Under-the-GDPR.pdf (31.8.2018).

69 Art. 64 of the GDPR.

70 WP 263 rev 1.0, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, Art. 29 WP, 11 April 2018, available at: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51031 (31.8.2018).
For a comparison with the previous authorization procedure under the DPD, see Pateraki, A., op. cit., pp. 3-5 and working papers: WP 108, WP 107, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", Art. 29 WP, 14 April 2005, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf (31.8.2018); WP 102, Model Checklist Application for approval of Binding Corporate Rules, Art. 29 WP, 25 November 2012, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp102_en.pdf (31.8.2018); WP 133, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, Art. 29 WP, 10 January 2007, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc (31.8.2018); WP 153; WP 195a, Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, Art. 29 WP, 17 September 2012, available at: http://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2012/wp195a_application_form_en.doc (31.8.2018).

71 Binding corporate rules, European Commission, available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en#listofcompanies (31.8.2018).

72 Art. 40 and 41 of the GDPR.

73 Art. 27 of the DPD.

However, under the GDPR they may be used for the transfer of personal data to third countries and international organisations if they provide for binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.[74] Under the same condition, certification mechanism may be used as a ground for the transfer of personal data to third countries, which is also a novelty introduced by the GDPR.[75]

The GDPR introduced appropriate safeguards which are of less importance for private companies: agreements between public bodies[76] and judgments of a court or tribunal and decisions of an administrative authority of a third country.[77]

3.1.3. Derogations

According to Article 29 Working Party layered approach to crossborder data transfers,[78] companies wanting to transfer personal data to third countries and international organisations should use an adequacy decision as a ground the for transfer if there is one. In the absence of the adequacy decision, they should resort to one of the appropriate safeguards and if this ground is also unavailable, the last option are grounds for transfer referred to as derogations. The majority of them were taken over from the DPD. Apart from conditions prescribed for each derogation in Art. 49 of the GDPR, the processing activity must comply with other relevant GDPR provisions, in particular with Art. 5 prescribing processing principles and Art. 6 laying down conditions for lawful processing. Therefore, a two-step test has to be applied.[79]

The first derogation mentioned in Art. 49(1)(a) is consent. Whereas the DPD[80] required the consent to be unambiguous, the GDPR prescribes that it has to be explicit, which is a more strict requirement. Prior to giving consent, the data subject has to be informed of possible risks. Furthermore, consent has to be specific, meaning that it

74 Art. 46(2)(e) of the GDPR.

75 Arts. 42, 42 and 46(2)(f) of the GDPR.

76 Public authorities or bodies may conclude legally binding enforceable agreements which do not require specific authorisation of a national supervisory authority (46(2)(a) of the GDPR) or administrative arrangements which include enforceable and effective data subject rights and which are not legally binding, such as memorandum of understanding, and have to be authorized by competent supervisory authority (Art. 46(3)(b) of the GDPR).

77 Such judgments and decisions requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable if they are based on an international agreement in force between the EU or an EU Member State and a third country, such as a mutual legal assistance treaty (Art. 48 of the GDPR).

78 WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Art. 29 WP, 25 November 2005, p. 9, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf (31.8.2018). See also Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018).

79 Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, p. 3, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018).

80 Art. 26(1)(a) of the DPD.

has to be given for a particular data transfer or set of transfers. Therefore, it will not always be possible to request prior consent of the data subject for a future data transfer at the time of collecting data.[81] Personal data transfer may take place if it is necessary for the 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 or if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.[82] Apart from being necessary, the transfer under these derogations has to be occasional.[83] Personal data may be transferred to a third country or international organisation if it is necessary for the important reason of public interest.[84] The respective derogation may only be applied if under EU law or the law of the Member State to which the controller is subject, data transfers at issue are allowed for important public interest reasons. Furthermore, it may be deduced from the wording of Recital 111 that data transfers based on public interest reasons may be non-occasional. Even though this derogation will be more frequently used by public entities, private companies are not excluded from its application.[85] Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent[86] refers to situations in which the risk of serious harm to the data subject outweighs data protection concerns, such as medical emergencies.[87] Transfer made from a public register[88] refers to registers which are either open to public or a person who can demonstrate a legitimate interest. Transfer necessary for establishment, exercise or defence of legal claims is a derogation which may only be used by public authorities.[89]

Finally, the EU companies acting as data exporters may benefit from another derogation the GDPR introduced as a last resort, for residual cases. Personal data may be transferred to a third country or international organisation 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

81 See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, pp. 6-8, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018).

82 Art. 49(1)(b) and (c) of the GDPR. See also Art. 26(1)(b) and (c) of the DPD.

83 Recital 111 of the GDPR Preamble.

84 Art. 49(1)(d) of the GDPR. See also Art. Art. 26(1)(d) of the DPD.

85 Recital 112 of the GDPR Preamble.

86 Art. 49(1)(f) of the GDPR. See also Art. 26(1)(e) of the DPD.

87 See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, pp. 12-13, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018).

88 Art. 49(1)(g) of the GDPR. See also Art. 49(1)(f) of the DPD.

89 Art. 49(1)(e) of the GDPR. See also Art. 26(1)(d) of the DPD.

the data subject of the transfer and on the compelling legitimate interests pursued.[90] The data exporter has to be able to demonstrate that it could not use appropriate safeguards or other derogations because, for instance, the data exporter is a small company so it is not reasonable to expect that it uses some of the appropriate safeguards or the data importer refuses to use standard contractual clauses or the data subject did not give his or her consent. Compelling interest should be interpreted restrictively, for instance in cases in which there is a risk of harm or penalty for the data exporter and should be balanced with the data subjects rights.[91]

3.2. Transfers of Data Within the EEA

The conditions for transferring personal data within the EEA will depend upon whether the data is being transferred from one controller to another controller or from controller to processor. It is not always apparent whether a particular company processes data as a controller or a processor. With respect to one set of data, a company may act as a processor, while with respect to other data it may be in the role of the controller.[92] Art. 29 Working Party suggested that the controller is a functional concept, intended to allocate responsibilities and thus the assessment should be based on factual rather than a formal analysis. The controller is the party which makes a decision to process, the one which initiates it.[93] Controllers choose which data will be collected and processed, for which purpose, who will have access to data, for how long will the data be processed etc.[94] Technical and organisational decisions such as which software will be used may be delegated to processor.[95] The

90 Art. 49(1) of the GDPR.

91 See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, pp. 14-15, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018).

92 See for instance the case of SWIFT, a Belgian worldwide financial messaging service which facilitates international money transfers which considered itself a data processor, but the Belgian data protection authority, concluded it had the role of data controller. See Decision of the Belgian data protection authority of 9 December 2008, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/swift_decision_09_12_2008.pdf (31.8.2018). See also WP 128, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Art. 29 WP, 22 November 2006, https://iapp.org/media/pdf/resource_center/wp128_SWIFT_10-2006.pdf (31.8.2018)

93 WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, p. 8, available at https://iapp.org/media/pdf/resource_center/wp169_concepts-of-controller-and-processor_02-2010.pdf (31.8.2018).

94 For in Google Spain, the CJEU clarified that the search engine when it performs the activity of finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference acts as a controller. Activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published. Judgment of 13 May 2014, *Google Spain*, C-131/12, EU:C:2014:317, paragraphs 33-41.

95 WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, p. 14, available at: https://iapp.org/media/pdf/resource_center/wp169_concepts-of-controller-

GDPR explicitly states that processor which infringed the GDPR determining the purposes and means of processing, i.e., makes its own decision instead of following the controller's instructions, will be considered to be a controller.[96] The criteria which might help differentiate the controllers from processors are for instance "freedom from instructions by the contracting entity that delegated the data processing to the processing entity in question; merging of the data received upon delegation with own databases; use of the data for own purposes that may have not been agreed upon with the contracting entity; processed data having been collected by way of a legal relationship between the processing entity and the data subjects; responsibility of the processing entity for the lawfulness and accuracy of the data processing."[97]

3.2.1. Transfer Controller – Processor

The transfer of personal data from the controller to processor is expressly regulated by the GDPR.[98] Controllers wishing to delegate processing to processors have to make sure that they choose processors providing sufficient guarantees to implement appropriate technical and organisational measures which will be in line with the GDPR and ensure sufficient protection of the data subject's rights. Processing by the processor has to be regulated by a contract or other legal act under EU or Member State law, binding for the processor. The contract or legal act has to regulate the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The DPD required that the binding agreement between the controller and the processor prescribes the obligation of the processor to act under the controller's instructions and ensure security of the processed data.[99] The GDPR prescribes several more obligations to be included into the binding agreement: persons processing data are under confidentiality obligations, acting in accordance with the rules regarding appointment of sub-processors, implementing technical and organisational measures so that controller complies with the rights of data subjects; deleting or returning the personal data after the end of provision of services unless EU or Member State law prescribes otherwise, assisting the controller in obtaining approval from DPAs where required; assisting the controller to comply with the obligations of security of data, notification of data breach to supervisory authority and data subject, impact assessment and prior consultation; and provide the controller all information necessary to demonstrate compliance with its obligations, allow and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.[100]

The processor may engage a sub-process only with a prior specific or general

and-processor_02-2010.pdf (31.8.2018).

96 Art. 28(10) of the GDPR.

97 Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR), A Practical Guide, Cham, Springer, 2017, p. 19.

98 Art. 28 of the GDPR.

99 Art. 17 (2) and (3) of the DPD.

100 Art. 28(1) and (3) of the GDPR.

written authorisation of the controller and in such case the sub-processor is bound by the same obligations as the processor by a contract or other legal act and liable to the controller.[101] Instead of relying on a contract or a legal act, the GDPR provides the possibility that a processor adheres to an approved code of conduct or an approved certification mechanism in order to demonstrate that it provides sufficient guarantees. The European Commission and national supervisory authorities may adopt standard contractual clauses in accordance with the examination procedure and consistency mechanism, respectively. In the latter case, the contract and the legal act may be based on standard contractual clauses.[102] No such codes of conduct, certification mechanisms or standard contractual clauses have been drafted so far. Under the GDPR, the processor has the obligation of immediately informing the controller if, in its opinion, acting in accordance with the controller's instructions infringes the GDPR or other EU or Member State data protection provisions.

3.2.2. Transfer Controller – Controller

The GDPR contains one provision on the transfer between controllers. It regulates the obligation of, the so-called, joint controllers. Joint controllers are controllers which jointly determine the purposes and means of processing. They have an obligation of concluding an agreement by which they will determine their respective responsibilities for compliance with the GDPR in a transparent manner, their roles and responsibilities, unless the respective responsibilities of the controllers are determined by EU or Member State law. Particularly, this obligation refers to exercising the rights of the data subject and their right to be informed on data obtained from data subject and data not obtained from the data subject. The arrangement may designate a contact point for data subjects. The summary of the agreement has to be made available to data subjects. Data subjects may exercise their rights against each of the controllers.

Not all transfers between controllers will fall into the category of joint controllers. It is possible that controllers act independently, without agreeing on processing means and purposes.[103] The GDPR does not contain provision on the transfer between such independent controllers. It may be concluded based on GDPR provisions that in these situations, processing by each controller is considered as separate processing which has to be justified by one of the legal bases for processing prescribed in Arts. 6 or 9 of the GDPR. A separate legal basis necessity would be in line with the purpose limitation principle from Art. 5(1)(b) of the GDPR according to which data may be collected for specified, explicit and legitimate purposes and not further processed in a manner

101 Art. 28(4) of the GDPR.

102 Art. 28 (5)-(8)of the GDPR.

103 Under Data Protection Act 1998, English law distinguished the category of controllers in common, which do not determine purpose and manner of data processing jointly but share a pool of personal data that they process independently of each other. See Data Protection Act 1998, Part I; Guide to data protection, Information Commissioner's Office, available at: http://webarchive.nationalarchives.gov.uk/20180524151709/https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (31.8.2018).

that is incompatible with those purposes, as well as accountability principle under which controller has to demonstrate compliance with data processing principles.[104] Wenderhorst indicated that if the separate legal basis necessity or principle of separate justification, as she refers to it, is accepted, the independent controller – controller transfer has to be justified on both ends, i.e. both the transfer from the initial controller and the receipt of data on the part of the receiving controller have to be separately justified by one of the GDPR legal bases. However, if EU controller-EEA controller transfer is subjected to separate legal basis necessity, in certain situations it might be more burdensome compared to EU controller-non-EEA controller transfer. Under Privacy Shield, Accountability for Onward Transfer principle, in order to transfer personal information to a third party acting as a controller, organisations must comply with the Notice and Choice Principles. Notice principle refers to information which have to be provided to the data subject, whereas Choice principle gives the option to data subject to opt out if they do not want their personal information to be disclosed to a third party or used for a purpose that is materially different from the purposes for which it was originally collected or subsequently authorised by the individuals. Therefore, no equivalent requirement to the legal basis from Art. 5 of the GDPR is prescribed under Privacy Shield. A similar situation is with the Set II controller-controller standard contractual clauses enacted with Decision 2004/915/EC. According to Clause II(i) the controller importing data may further disclose or transfer personal data to non-EEA controller (which does not processes the personal data Commission decision finding that a third country provides adequate protection and is not signatory to standard contractual clauses or another data transfer agreement approved by a competent authority in the EU), if it notifies the data exporter about the transfer, and data subjects have been given the opportunity to object after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or if sensitive data is at issue, data subjects have given their unambiguous consent to the onward transfer.[105]

Transfers between controllers within the EEA compared to transfers between EU-controller and non-EEA controller seem to be more burdensome from another aspect. In cases in which the joint controllers transfer data within EEA, the standard of liability is more burdensome compared to the transfer between EU-controller and non-EEA-controller which jointly determine the purpose of processing and use Set II controller-controller. While the standard of liability according to Set II controller-controller is fault-based, joint controllers which transfer data within EEA might be held jointly and severally liable pursuant to Art. 82(4) of the GDPR.[106]

104 Wenderhorst, C., How to Reconcile Data Protection and the Data Economy, in: Lohsse, S./Schulze, R./Staudenmayer, D. (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, pp. 334-336.

105 For a similar argument see ibid, pp. 337-338.

106 For a similar reasoning, see Van Alsenoy, B., Liability under EU Data Protection Law, from Directive 95/46 to the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 7, 2016, p. 287. See also Bukovac Puvača,

4. CONCLUSION

Data transfers pose a grave risk to privacy. Yet, European data economy, which is a part of the Digital Single Market strategy, requires that data crosses borders of the EU. Such dichotomy requires a careful balancing of protecting data and creating an environment in which the data can flow freely to and from the EU. With the aim of striking the right balance, the EU legislator has developed instruments based on which EU data may be transferred outside the EU, while prescribing safeguards with the aim of maintaining a sufficient level of protection. These instruments or grounds for transfer, namely adequacy decisions, appropriate safeguards and derogations were developed under the DPD regime and taken over by the GDPR. EU companies which act as data exporter will benefit from the fact that the GDPR has proliferated the variations within each of the grounds for transfer in comparison to the DPD. Even though efforts have been made to improve these instruments, even prior to the enactment of the GDPR, they still present some concerns, both for data subjects and companies acting as data exporters. Furthermore, transfers between companies within EEA, in contrast to transfers from EU companies to non-EEA companies, demonstrate some impracticalities given that the former impose more requirements on onward transfers than the latter.

LITERATURE

Books and Articles

1. Boehm, Franziska, 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, 2012
2. Bradford, Anu, The Brussels Effect, Northwestern University School of Law, Vol. 107, 1/2012, pp. 1-68
3. Bukovac Puvača, Maja, Nova EU Opća uredba o zaštiti osobnih podataka – pravo na naknadu štete i odgovornost zbog njenog kršenja (čl. 82. Uredbe), in: Mićović, Miodrag (ed.), Savremeni pravni promet i usluge, Kragujevac, Pravni fakultet Univerziteta u Kragujevcu, 2018, pp. 755-777
4. Bu-Pasha, Shakila, Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, Vol. 26, 3/2017, pp. 213-228
5. Coley, Alyssa, International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà vu' in Hasting Law Journal, Vol. 68, 2017, pp. 1111 -1134
6. Geppert, Nadine, 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?, pp. 1-44, available at SSRN: https://ssrn.com/abstract=2928064 (31.8.2018)
7. González Fuster, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham, Springer, 2014, pp. 163-212
8. Janal, Ruth, Fishing for an Agreement: Data Access and the Notion of Contract, in: Lohhse, Sebastian, Schulze, Reiner, Staudenmayer, Dirk (eds.), Trading Data in the

M., Nova EU Opća uredba o zaštiti osobnih podataka – pravo na naknadu štete i odgovornost zbog njenog kršenja (čl. 82. Uredbe), in: Mićović, M. (ed.), Savremeni pravni promet i usluge, Kragujevac, Pravni fakultet Univerziteta u Kragujevcu, 2018, p. 772-773.

Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, pp. 271-291
9. Kong, Lingjie, Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law, Vol. 21, 2/2010, pp. 441-456
10. Kuan Hon, W., Data Localization Laws and Policy, The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens, Cheltenham, Northampton, Edward Elgar, 2017
11. Kuner, Cristopher, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal, Vol. 18, 4/2017, pp. 881-918
12. Lohsse, Sebastian, Schulze, Reiner, Staudenmayer, Dirk, Trading Data in the Digital Economy: Legal Concepts and Tools, in: Lohsse, S./Schulze, R./Staudenmayer, D. (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, pp. 13-24.
13. Milanovic, Marko, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' in Harvard International Law Journal, Vol. 56, 1/2015, pp. 81-146
14. Pateraki, Anna, EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?, Bloomberg BNA World Data Protection Report, Vol. 16, 3/2016, pp. 1-5, available at: https://www.huntonak.com/images/content/3/2/v3/3291/EU-Regulation-Binding-Corporate-Rules-Under-the-GDPR.pdf (31.8.2018).
15. Roth, Paul, Adequate Level of Data Protection in Third Countries Post-*Schrems* and under the *General Data Protection Regulation*, Journal of Law, Information and Science, Vol. 25, 1/2017, pp. 49-67
16. Schrems, Max, The Privacy Shield is a Soft Update of the Safe Harbor, Foreword, European Data Protection Law Review, 2/3016, pp. 1-4
17. Suda, Yuko, The Politics of Data Transfer, Transatlantic Conflict and Cooperation over Data Privacy, New York, London, Routledge, 2018
18. Van Alsenoy, Brendan, Liability under EU Data Protection Law, from Directive 95/46 to the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 7, 2016, pp. 271-288
19. Voigt, Paul, von dem Bussche, Axel, The EU General Data Protection Regulation (GDPR), A Practical Guide, Cham, Springer, 2017
20. Voss, Gregory, V., The Future of Transatlantic Data Flows: Privacy Shield or Bust, Journal of Internet Law, Vol. 19, 11/2016, pp. 1, 9-18
21. Weber, Rolf H., Staiger, Dominic, Transatlantic Data Protection in Practice, Cham, Springer, 2017
22. Wenderhorst, Christiane, How to Reconcile Data Protection and the Data Economy, in: Lohsse, Sebastian, Schulze, Reiner, Staudenmayer, Dirk (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, pp. 327-355
23. Wojtan, Boris, The new EU Model Clauses: One step forward, two steps back?, International Data Privacy Law, Vol. 1, 1/2011, pp. 76-80 available at: https://academic.oup.com/idpl/article/1/1/76/759672 (31.8.2018.)
24. Zimmer, Daniel, Property Rights Regarding Data, in: Lohsse, Sebastian, Schulze, Reiner, Staudenmayer, Dirk (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos, 2017, pp. 101-107

Legal Acts:

1. Charter of Fundamental Rights of the European Union, OJ C 202, 7 June 2016
2. 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, pp. 7-47
3. Council of Europe, Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, Strasbourg, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (31.8.2018)
4. Corrigendum to 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) (OJ L 119, 4.5.2016), OJ L 127, 23.5.2018, pp. 2-5
5. Decision 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., pp. 52-62
6. 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, pp. 31-50
7. 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, pp. 1-88
8. UK, Data Protection Act 1998
9. 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, pp. 1-3
10. 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, pp. 19-31
11. 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, pp. 19-22
12. 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, pp. 27–28
13. 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, pp. 48-51
14. 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, pp. 74-84
15. 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, pp. 21-23
16. 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, pp. 17-19
17. 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, pp. 27-29

18. 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, pp. 5-18.
19. 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, pp. 39-42
20. 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, pp. 11-14
21. 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, pp. 12-14
22. 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, pp. 1-112
23. 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, pp. 13-16

Case Law:

1. Belgian data protection authority, SWIFT Decision of 9 December 2008, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/swift_decision_09_12_2008.pdf (31.8.2018)
2. CJEU, judgment of 11 June 2015, *McCullough*, T-496/13, EU:T:2015:374
3. CJEU, judgment of 13 May 2014, *Google Spain*, C-131/12, EU:C:2014:317
4. CJEU, judgment of 16 July 2015, *ClientEarth*, C-615/13 P, EU:C:2015:489
5. CJEU, judgment of 22 November 2011, *Digital Rights Ireland v Commission*, T-670/16, EU:T:2017:838
6. CJEU, judgment of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771
7. CJEU, judgment of 29 June 2010, *Bavarian Lager*, C-28/08 P, EU:C:2010:378
8. CJEU, judgment of 30 May 2013, *Worten*, C-342/12, EU:C:2013:355
9. CJEU, judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650.
10. CJEU, judgment of 7 July 2011, *Jordana*, T-161/04, EU:T:2011:337
11. CJEU, judgment of 9 March 2017, *Manni*, C-39/15, EU:C:2017:197
12. CJEU, order of 25 October 2016, La Quadrature du Net and Others v Commission, T-738/16.
13. Ireland, High Court, *The Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, 3 October 2017 [2016 No. 4809 P.], available at: https://dataprotection.ie/docimages/documents/Judgement3Oct17.pdf (18.9.2018).
14. Ireland, High Court, *The Data Protection Commissioner and Facebook Ireland and Maximilan Schrems, Request for a Preliminary Ruling,* 12 April 2018 [2016 No. 4809 P.], available at: http://www.europe-v-facebook.org/sh2/ref.pdf (18.9.2018)

Other Sources:

1. Binding corporate rules, European Commission, available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en#listofcompanies (31.8.2018)
2. Decision updating the standard contractual clauses for the transfer of personal data to processors established in non-EU countries, Press Release, Brussels, 5 February 2010, available at: http://europa.eu/rapid/press-release_MEMO-10-30_en.htm?locale=en (31.8.2018)
3. Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and United States, Sidley Report, January 2016, available at: https://www.sidley.com/-/media/publications/essentially-equivalent---final.pdf?la=en (31.8.2018)
4. Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, COM(2017) 7 final, European Commission, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=41157 (accessed 27.8.2018)
5. Facebook, What is a standard contractual clause?, available at: https://www.facebook.com/help/566994660333381?ref=dp&locale=en_GB (18.9.2018), https://www.facebook.com/about/privacy/update (18.9.2018)
6. Google Cloud Platform, EU Model Contract Clauses, available at: https://cloud.google.com/terms/eu-model-contract-clause (18.9.2018)
7. Guide to data protection, Information Commissioner's Office, available at: http://webarchive.nationalarchives.gov.uk/20180524151709/https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (31.8.2018).
8. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, EDPB, 25 May 2018, available at: https://iapp.org/media/pdf/resource_center/edpb_guidelines_2_2018_derogations_en.pdf (31.8.2018)
9. Microsoft Office, Frequently Asked Questions, available at: https://products.office.com/en-us/business/office-365-trust-center-eu-model-clauses-faq (18.9.2018)
10. See Privacy Shield Framework, available at: https://www.privacyshield.gov/list (18.9.2018.)
11. The European Court of Justice to rule on the validity of standard contractual clauses, Linklaters, 30 May 2016, pp. 1-2, available at: https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/brussels/160530_alert_the_european_court_of_justice_to_rule_on-the_validity_of_standard_contractual_clauses.ashx (31.8.2018)
12. 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 27.8.2018)
13. WP 102, Model Checklist Application for approval of Binding Corporate Rules, Art. 29 WP, 25 November 2012, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp102_en.pdf (31.8.2018)
14. WP 107, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", Art. 29 WP, 14 April 2005, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf (31.8.2018)
15. WP 108, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, Art. 29 WP, 14 April 2005, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf (31.8.2018)
16. WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Art. 29 WP, 25 November 2005, p. 9, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf (31.8.2018)

17. WP 128, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Art. 29 WP, 22 November 2006, https://iapp.org/media/pdf/resource_center/wp128_SWIFT_10-2006.pdf (31.8.2018)
18. WP 133, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, Art. 29 WP, 10 January 2007, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc (31.8.2018)
19. WP 153, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Art. 29 WP, 14 June 2008, available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf (31.8.2018)
20. WP 154, Working Document Setting up a framework for the structure of Binding Corporate Rules, Art. 29 WP, 24 June 2008, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf (31.8.2018)
21. WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, p. 8, https://iapp.org/media/pdf/resource_center/wp169_concepts-of-controller-and-processor_02-2010.pdf (31.8.2018)
22. WP 195, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, Art. 29 WP, 6 June 2012, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (31.8.2018)
23. WP 195a, Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, Art. 29 WP, 17 September 2012, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc (31.8.2018)
24. WP 204 rev 1.0, Explanatory Document on the Processor Binding Corporate Rules, Art. 29 WP, 19 April 2013, last revised and adopted on 22 May 2015, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf (31.8.2018)
25. See WP 237, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Art. 29 WP, 13 April 2016, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf (31.8.2018.)
26. WP 238, Article 29 Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 13.4.2016, available at: https://www.pdpjournals.com/docs/88536.pdf (31.8.2018)
27. WP 256, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Art. 29 WP, 29 November 2017, available at: https://iapp.org/media/pdf/resource_center/wp256_BCR_11-2017.pdf (31.8.2018)
28. WP 257, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, Art. 29 WP, 29 November 2017, available at: https://iapp.org/media/pdf/resource_center/wp257_BCR-processor.pdf (31.8.2018)
29. WP 263 rev 1.0, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, Art. 29 WP, 11 April 2018, available at: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51031 (31.8.2018)
30. WP 74, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Art. 29 WP, 3 June 2003, p. 6., available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (31.8.2018)

Danijela Vrbljanac*

Sažetak

UPRAVLJANJE INOVATIVNIM KAPITALOM TRGOVAČKOG DRUŠTVA: SLUČAJ PRIJENOSA OSOBNIH PODATAKA

Malobrojna su područja europskoga prava koja su se pokazala kontroverznima do mjere do koje je to zaštita osobnih podataka. Posebice se to odnosi na pitanje prijenosa osobnih podataka izvan Europske unije. Pitanje prijenosa osobnih podataka u treće zemlje aktualiziralo se posebice nakon što je Sud Europske unije proglasio je nevaljanim sporazum "Safe Harbour", jedan od mehanizama prijenosa osobnih podatka u SAD, a valjanost nekolicine ostalih je dovedena u pitanje, uključujući i sporazum "Privacy Shield", sljednik sporazuma "Safe Harbour". U pogledu dijela pravnih osnova za prijenos osobnih podataka u treće zemlje, istaknuto je da trebaju biti ukinute ili izmijenjene kako bi bile u skladu s Općom uredbom o zaštiti podataka. Nakon analize svake od pravnih osnova za prijenos osobnih podataka koje stoje na raspolaganju društvima iz EU-a, u radu se ističe da "revolucija" osobnih podataka koja je nastupila nedavnim stupanjem na snagu Opće uredbe o zaštiti podataka, nije završila, barem što se tiče prekograničnog prijenosa osobnih podataka.

Ključne riječi: *zaštita podataka; pravo EU-a; Opća uredba o zaštiti podataka; privatnost; prekogranični prijenos podataka; prijenos podataka.*

Zussamenfassung

KAPITALMANAGEMENT BEI INNOVATIVEN UNTERNEHMEN: ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Es gibt nicht viele Bereiche des Europäischen Rechts, welche so kontrovers wie Datenschutz sind. Nur beim grenzüberschreitenden Verkehr personenbezogener Daten könnte dieses Problem noch umstrittener werden. Der Status der Übermittlung personenbezogener Daten in Drittländer hat sich bei der Entkräftung der Sicheren-Häfen-Vereinbarung vom EuGH, einer der Rechtsrahmen für die Übermittlung personenbezogener Daten in die USA, als strittig erwiesen. Weitere Abkommen wurden vom EuGH geprüft, einschließlich des Datenschutzschilds, des Nachfolgers

* Dr. sc. Danijela Vrbljanac, poslijedoktorandica, Sveučilište u Rijeci, Pravni fakultet; danijela.vrbljanac@pravri.hr.

der Sicheren-Häfen-Vereinbarung. Es wurde vorgeschlagen, dass manche dieser Instrumente der Übermittlung aufgehoben oder geändert werden müssen, um mit der DSGVO im Einklang gebracht zu werden. Dieser Beitrag analysiert die Rechtsgrundlagen, welche die Unternehmen in der EU für die Übermittlung personenbezogener Daten anwenden. Es wird behauptet, dass, ungeachtet des Inkrafttretens der DSGVO, die "Revolution" des Datenschutzes noch nicht beendet ist, wenigstens was den grenzüberschreitenden Datenverkehr betrifft.

Schlüsselwörter: *Datenschutz; EU-Recht; Datenschutz-Grundverordnung; Privatsphäre; grenzüberschreitender Datenverkehr; Datenübermittlung.*

Riassunto

LA GESTIONE DEL CAPITALE DELLE SOCIETÀ INNOVATIVE: IL CASO DEL TRASFERIMENTO DI DATI PERSONALI

Pochi settori del diritto europeo risultano sì controversi come quello della protezione dei dati personali. L'unico caso in cui tale questione può diventare ancora più discutibile è quello in cui i dati personali valicano i confini dell'UE. Il trasferimento dei dati personali a stati terzi fece sorgere questioni giuridiche quando la Corte di Giustizia dell'UE annullò il Safe Harbour Agreement, e cioè uno dei quadri regolatori del trasferimento di dati personali verso gli USA, come pure in occasione dell'attento scrutinio della stessa Corte rispetto ad un successore del Safe Harbour Agreement, ossia il Privacy Shield Agreement. Venne infatti suggerito come alcuni di questi strumenti atti al trasferimento dei dati necessiti una rivisitazione e delle modifiche al fine di conformarsi al GDPR. Il contributo, dopo l'analisi di ciascuno dei fondamenti per il trasferimento dei dati che potrebbe venire utilizzato dalla compagnie europee, argomenta che nonostante la recente entrata in vigore del GDPR, la "rivoluzione" della protezione dei dati non sia ancora interamente compiuta, perlomeno per quanto concerne il flusso transfrontaliero dei dati.

Parole chiave: *protezione dei dati; diritto dell'UE; Regolamento generale per la protezione dei dati; privacy; flusso transfrontaliero di dati; trasferimento di dati.*