ISSN 2601-8683 (Print)
ISSN 2601-8675 (Online)
European Journal of
Formal Sciences and Engineering
January - June 2023
Volume 6, Issue 1

Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice

Emanuela Furramani

Ph.D. Lecturer, University "Luigj Gurakuqi", Shkodër, Albania

Abstract

The focus of this study is the transfer of personal data to third countries or international organizations according to EU Regulation No. 679/2016 (GDPR) on the protection of personal data. The primary goal of this Regulation concerning data transfer to third countries is to ensure that the subject's rights and freedoms are safeguarded at the same level as provided by GDPR. According to GDPR, before any transfer to a third country or international organization, it must first be ascertained whether the European Commission has established that a third country ensures an adequate level of protection. Regarding personal data protection in the third state, the Court of Justice of the European Union has intervened on different occasions. In the last decision, in 2020, the Court declared invalid the European Commission's Decision No. 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield (CJEU, Schrems II, 2020, July 16) because it does not provide effective and enforceable rights for personal data subjects in cases of interference. According to the Court of Justice of the European Union, the US does not guarantee an "essentially equivalent" level of protection to that provided by the European Union under Article 45(1) GDPR, read in conjunction with Articles 7, 8, and 47 of the European Union's Charter of Fundamental Rights, which guarantee respect for private and family life, personal data protection, and the right to effective judicial protection.

Keywords: GDPR, personal data, transfer, third country, Privacy Shield.

Introduction

The rapid evolution of the digital economy and the considerable changes in international trade have brought new challenges regarding personal data protection. One of the challenges the European Union faces today is data transfer from European Union or Exclusive Economic Area countries to other countries or international organizations outside this area (Kirschen, 2019, p. 262). The European Union Regulation No. 679/2016 (General Data Protection Regulation, hereafter GDPR)

provides that the transfer of personal data outside the European Union or the Economic Exclusive Area is generally prohibited unless the state in question offers the appropriate safeguards (GPDP, 2019; EDPB, 2018). The principal purpose of this provision is to protect personal data and preserve the security provided by EU legislation (Regulation (EU) 2016/679, Recital 6; EDPB, 2018). From this perspective, the transfer of personal data to third countries or international organizations should be accompanied by the protection established for personal data in the European Union (CJEU, Schrems II, 2020, July 16). In this regard, on July 16, 2020, the Court of Justice of the European Union found that the United States does not provide an "*essentially equivalent*" level of protection to that provided by the European Union, invalidating the European Commission's adequacy decision No. 2016/1250.

Methodology

This paper focuses on the transfer of personal data from the European Union or Exclusive Economic Area to countries or international organizations outside this area according to European Union Regulation No. 679/2016.

This research uses qualitative research methods to analyze the transfer of personal data outside the European Union and the guarantees provided for personal data protection. The paper is divided into three sections, where the first part refers to the concept of personal data and the transfer of personal data according to the EU Regulation. The second section of the paper examines the provisions of the EU Regulation governing the transfer of personal data to third countries and all of the criteria that must be satisfied if a transfer occurs. The third part of this paper refers to the jurisprudence of the Court of Justice of the European Union, which has intervened, highlighting the importance of the "equivalent level" of personal data protection in the case of transfer to third countries. The third part of this paper includes discussions concerning the critical issues the Court of Justice of the European Union raised concerning the equivalent level of protection.

Transfer of personal data

The GDPR specifies that personal data signifies any information relating to a particular person that may be identified or identifiable (Regulation (EU) 2016/679, Recital 26). Under the first paragraph of Article 4 of the Regulation, personal data refers to "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person"* (Regulation (EU) 2016/679, Article 4). In light of the above, any information that may be used to identify an individual, such as a name (See Valsecchi, 2022, p. LII-LIII), phone number, or other information that may be linked to an IP

address or cookie identifier, should be deemed personal data (Regulation (EU) 2016/679, Recital 30; Arnaboldi, 2018, p. 25).

The protection of personal data is a fundamental right under Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) (Regulation (EU) 2016/679, Recital 1). On the one hand, these documents provide that everyone, regardless of nationality or residence, has the right to personal data protection (Regulation (EU) 2016/679, Recital 1 and 14). Nonetheless, the right to personal data protection is not absolute, and it must be evaluated in relation to its purpose in society in order to strike a balance with other rights in line with the principle of proportionality. (Regulation (EU) 2016/679, Recital 4; CJEU, C-507/17, 2019, September 24; C-92/09 and C-93/09, 2010, November 9; Schwarz, C-291/12, 2013, October 17; EDPB, 2020, p. 9). In this context, the right to data protection may be restricted when necessary to protect the rights or freedoms of others under EU legislation (CJEU, Schrems II, 2020, July 16, para. 174). In this regard, the European Data Protection Board in 2020 adopted recommendations for controllers and processors based on the principle of accountability, which requires them to ensure the equivalent level of protection guaranteed by the GDPR in every transfer of personal data to third countries or international organizations (EDPB, 2020, p. 5-8).

Pursuant to Article 44 of GDPR, the EU Regulation applies to "*any transfer of personal data which is undergoing processing or is intended for processing after transfers to a third country or to an international organization.*" The term "*transfer*" refers to any type of transmission activity that can take place via any form or device (Kirschen, 2019, p. 264; Piroddi, 2021, p. 621), excluding dissemination and communication in the strict sense (Rich. Imperiali & Ros. Imperiali, 2003, pp. 8 et seq.). The Court of Justice of the European Union has commented on the notion of "transfer" more than once. In the Lindqvist case, the Court of Justice of the European Union has analyzed whether the mere fact of uploading personal data to a website stored by a server located in the same state or another state, should be considered a "transfer". On this occasion, the Court has concluded that the uploading of personal data onto an Internet page does not constitute a transfer of personal data, even when those data are accessible to *"anyone who connects to the internet, including people in a third country"* (CJEU, Case C-101/01). Subsequently, in the Schrims I case of October 6, 2015, the Court of Justice deals with the notion of transfer, including "*any operation or set of operations carried out with or without the aid of automated processes and applied to personal data*" (CJEU, C-362/2014, para. 45).

Conditions for allowing the transfer of personal data to third countries or international organizations

According to Article 45 of the GDPR, several steps must be taken to enable the transfer of personal data from the EU or EEA countries to third countries or international organizations. The first step in the transfer of personal data is to assess whether the

destination country or the international organization provides an adequate level of protection (Regulation (EU) 2016/679, Article 45 (1), Recital 103). In this regard, it is necessary to know whether there is a European Commission decision on the adequacy of the country where the transfer will take place. Through this decision, the European Commission states that the country offers adequate protection for the rights and freedoms related to personal data by allowing the transfer of data if it is under the provisions of the Regulation (Regulation (EU) 2016/679, Recital 103). In assessing the adequacy of the level of protection, the European Commission, based on Article 45, Paragraph 2 of the GDPR, considers various elements such as laws, respect for human rights and freedoms, national security, rules of personal data protection, the existence of a data protection authority, and binding commitments made by the country concerning data protection (Kirschen, 2019, pp. 269-270; Piroddi, 2021, pp. 634-639; Bernardi, 2020, p. 144). Another requirement added by the Regulation is that the Commission conduct a review of the adequacy decision every four years (Regulation (EU) 2016/679 Article 45, paras (3), (2a, 2b, 2c), (5), and Recitals 103 and 104; Arnaboldi, 2018, p. 173).

When a third country, according to the EU Commission, does not offer an adequate level of data protection, transfer to the latter is not permanently prohibited, but some other conditions are provided. It may, however, continue to comply with the provisions relating to transfers subject to appropriate safeguards (Regulation (EU) 2016/679, Article 46 (1), (2), and Recital 108; EDPB, 2020; EU Regulation No. 2018/1725, Article 48) according to Article 46, paragraph 2. Based on Recital 108 of the GDPR, the appropriate safeguards provided for by Article 46[1] must respect the protection of the personal data of the interested parties and ensure effective administrative or judicial remedies together with the possibility of compensation for damages (Recital 108, GDPR; Kirschen, 2019, p. 272; Piroddi, 2021, pp. 642-643; De Mozzi, 2022, p. 141). In the absence of the appropriate safeguards, Article 49 of the GDPR provides for some derogations to the general principle that personal data may be transferred to a third country if the latter provides for an appropriate level of protection. The basic rule for performing any data transfer is that the data exporter must first respect the adequate level of protection under the provisions of Article 46 to guarantee the exercise of fundamental rights concerning the processing of personal

[1] According to Article 46, paragraph 2, the appropriate safeguards consist of: "(a) A legally binding and enforceable instrument between public authorities or bodies; (b) Binding corporate rules in accordance with Article 47; (c) Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) An approved code of conduct according to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; (f) An approved certification mechanism according to Article 42 together with binding and enforceable commitments of the controller or processor in the third country".

data and only, in the absence of the latter, utilize the derogations provided for in Article 49 (1) (Arnaboldi, 2018, p. 182). These derogations allow the transfer of data in specific situations, such as based on the explicit, informed consent of the interested party, for the performance or termination of a contract, for the exercise of lawful requirements, to protect the vital interests of the data subject, when they cannot give consent or for important reasons of public interest (See Piroddi, 2021, pp. 675-677; Arnaboldi, 2018, p. 181). Given the fact that derogations do not provide adequate protection or guarantees for the personal data being transferred (Kirschen, 2019, p. 285; Piroddi, 2021, p. 679) and that they do not require prior authorization from a national supervisory authority (EDPB, 2018, p. 4), the rights and freedoms of the data subjects being transferred may be at risk. The condition to be met in the case of derogations is that transfers must be random, necessary, and not repetitive (Regulation (EU) 2016/679, Article 49 (1); EDPB, 2018, p. 4; De Mozzi, 2022, p. 143; Bernardi, 2020, p. 149). In case of application of this derogation, must be informed the Supervisory Authority and the interested party for the transfer and the legitimate interests pursued.

The invalidation of the European Commission's Decision No. 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield by the Court of Justice of the European Union

The Court of Justice of the European Union has issued two important decisions on the transfer of personal data from the EU to the United States. The first decision, on October 6, 2015 (Schrems I), declared the invalidity of Decision No. 2000/520 regarding the Safe Harbour Agreement (Commission Decision 2000/520/EC) because it failed to provide an adequate level of protection required by Directive 95/46 for the transfer of personal data from the European Union or Exclusive Economic Area to the United States. And in the second decision (Schrems II), the Court of Justice of the European Union declared the invalidity of the European Commission's Decision No. 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield (Commission Decision No. 2016/1250) because it didn't ensure a level of protection for personal data equivalent to the European legislation (See Piroddi, 2021, p. 625; De Mozzi, 2022, p. 151). The European Commission's decision No. 2016/1250, on the adequacy of the protection provided by the EU-US Privacy Shield, adopted in 2016, provided for the possibility of the transfer of personal data from the European Union to the United States. This tool was used by businesses in the EU or EEA to transfer personal data to US companies listed on the Privacy Shield and provided specific guarantees for personal data protection (CJEU, Schrems II, 2020, July 16).

The issue concerns an Austrian national who was a Facebook user whose personal information was transmitted from Facebook Ireland to Facebook Inc., situated in the United States. Mr. Schrems filed a complaint with the Commissioner in June 2013 to prohibit the transfer of his data to the United States, claiming that the latter did not

ensure the same level of protection as guaranteed by the European Union (CJEU, Schrems II, 2020, July 16, paras 50, 51 and 52). Following a reformulation of Mr. Schrems' complaint, the Commissioner published a draft decision stating that the personal data transferred to the US was destined to be consulted and processed in a manner that was incompatible with Articles 7, 8, and 47 of the European Union's Charter of Fundamental Rights (CJEU, Schrems II, 2020, July 16, paras 55 and 56). As a result, the Commissioner took the issue to the High Court.

According to the High Court, the United States processed personal data without ensuring adequate protection as provided for in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. As a result, European nationals' data was not protected at the same level as American citizens. To begin with, the Court declared that the United States Constitution's fourth amendment does not apply to European nationals. According to the Court, the protection of the personal data of European individuals encounters some obstacles. The first issue is the *locus standi*. The second is the National Security Agency's (NSA) activity, which includes copying and filtering internet traffic flows without being subject to judicial oversight. And the third issue is the Privacy Shield's Ombudsperson, who is not a tribunal in the sense of Article 47 of the Charter (CJEU, Schrems II, 2020, July 16, para. 65). So the High Court brought the case to the Court of Justice of the European Union for a preliminary ruling.

The Court of Justice of the European Union in the case Schrems II examined various issues, concluding that, according to Article 45 GDPR, the transfer of personal data from the EU or EEA to a third country or international organization should be based on an adequacy decision of the Commission. In the absence of the latter, the controller or processor may transfer the personal data only in the presence of “appropriate safeguards” to guarantee the appropriate protection of the subjects’ rights and effective legal remedies (CJEU, Schrems II, 2020, July 16, paras. 91 and 92) under article 46 GDPR. In this sense, the controller or the processor may transfer personal data from the EU or EEA to a third country only in the presence of effective protection of personal data “essentially equivalent” to the GDPR.

The Court considers the role of national supervisory authorities in the protection of personal data in accordance with Article 51 (1) and 57 (1) GDPR, stating that national authorities are responsible for ensuring that the EU Regulation requirements are followed when personal data is transferred from the EU or EEA to third countries or international organizations (CJEU, Schrems II, 2020, July 16, para. 107 and case C-362/14, 2015, October 6, Schrems I, para. 47; Piroddi, 2021, p. 631; De Mozzi, 2022, p. 151). Even if the Commission has issued an adequacy decision allowing the transfer of personal data, the national supervisory authority should be able to investigate a complaint and determine whether the transferred data meets the GDPR's standards (CJEU, Schrems II, 2020, July 16, para. 120).

According to the Court, the European Commission Decision No. 2016/1250 affects the fundamental rights of people whose personal data is transferred from the European

Union to the United States because of the restrictions provided for by this decision. These restrictions are based on national security and public interest considerations as well as US domestic legislation (Commission Decision, No. 2016/1250, 2016, July 12, para. 1.5, Annex II, Recitals 67-137), and are particularly related to the access or use of personal data by US public authorities (CJEU, Schrems II, 2020, July 16, paras. 164-165). However, the Privacy Shield stipulates that restrictions are placed only where they are essential for a legitimate goal and that the subject's rights are protected (Commission Decision, No. 2016/1250, 2016, July 12, Recital 140).

The Court of Justice of the European Union argues that the communication of personal data to public authorities under US law constitutes an infringement on the fundamental rights guaranteed by Articles 7 and 8 of the Charter (CJEU, Schrems II, 2020, July 16, para. 171; De Mozzi, 2022, p. 151). On the other hand, the Court believes that the interferences with the subjects' rights are not limited to what is strictly necessary and do not respect the proportionality principle established by the European regulation (CJEU, Press release No. 91/20).

In this sense, the Court of Justice of the European Union considers that the Privacy Shield does not ensure, in the cases of interference, effective and enforceable rights to the subject whose data has been transferred (CJEU, Schrems II, 2020, July 16, paras 168 and 181) in violation of Article 47 of the Charter of Fundamental Rights of the European Union, which provides the right to an effective remedy and to a fair trial. Furthermore, because the Privacy Shield's ombudsperson is appointed by the Secretary of State, it is not an independent institution and is not a tribunal within the meaning of Article 47 of the Charter (CJEU, Schrems II, 2020, July 16, para. 168).

In conclusion, the Court found that the United States does not provide an "essentially equivalent" level of protection to that provided by the European Union under Article 45(1) GDPR, read in light of Articles 7, 8, and 47 of the Charter, which guarantee respect for private and family life, personal data protection, and the right to effective judicial protection, invalidating the adequacy decision. Accordingly, the transfer from the European Union to the United States should be based on other instruments under Chapter V of EU Regulation, such as Article 46, paragraph 2, which provides appropriate safeguards.

Following the repeal of the Privacy Shield, the European Commission adopted two sets of standard contractual agreements on June 4, 2021, to facilitate the transfer of personal data from the EU to third countries (Commission implementing decision of 4 June, Nos. 2021/914/UE and No. 2021/915/UE). These contractual clauses introduce novelty profiles concerning the number of parties that can adhere to the contract using these clauses and also provide for all the measures required to carry out the personal data transfer following the European Court of Justice's decision in the Schrems II case (De Mozzi, 2022, p. 155).

Discussions

The focus of the debate in the context of personal data transfer is on the level of protection that the third state or international organization provides for personal data. In this sense, according to the EU Regulation, the European Commission decision, which considers that the third state offers an adequate level of protection, is usually based on different elements that evaluate its adequacy. Those elements include legislation, respect for human rights and freedoms, national security, personal data protection standards, the presence of an independent data protection authority, and enforceable data protection commitments made by the country (Regulation (EU) 2016/679, Article 45, para. 2).

In this direction, in Decision Schrems II, the Court of Justice of the European Union addressed critical issues about the degree of personal data protection based on those elements. In this regard, the Court's crucial considerations are specifically connected to the communication of personal data to public authorities under US law. This communication, in the judgment of the Court, constitutes an interference with the enjoyment of the fundamental rights guaranteed by the European Charter of Fundamental Rights in Articles 7 and 8 (CJEU, Schrems II, 2020, July 16, para. 171; De Mozzi, 2022, p. 151).

But the most problematic issue regards the fact that those interferences are not limited to what is strictly necessary as provided for by the Privacy Shield, which limits the restrictions only where they are essential for a legitimate goal and that the subject's rights are protected (Commission Decision, No. 2016/1250, 2016, July 12, Recital 140). In this context, we are in front of an infringement of the proportionality principle (CJEU, Press release No. 91/20), which considers the measure applied in relation to the purpose and goal it seeks to achieve and to what is strictly necessary, and in any case, respecting the rights of the subjects. In this context, unlimited interference infringes on the rights of the subjects whose data is being transferred. On the other hand, the lack of an independent institution, such as an Ombudsman person equivalent to that provided by the GDPR, which can guarantee the rights and freedoms of individuals regarding personal data is a critical issue too, because the lack of this mechanism does not ensure the right to adequate judicial protection (CJEU, Schrems II, 2020, July 16, para. 168).

However, the Court of Justice of the European Union has ruled only on the European Commission's adequacy decision for the transfer of personal data from the EU to the US and not on the other European Commission adequacy decisions based on which personal data is transferred to other third countries, considering the fact that the legislation of those countries may formally fulfill EU criteria on fundamental rights and freedoms (See Meltzer, 2020). Consequently, we had to wait for the impact of the Court of Justice of the European Union decision in practice.

Conclusions

The issue of an "equivalent level of protection" in the third state, provided by the GDPR and subject to two decisions by the Court of Justice of the European Union, represents a problematic matter because different countries offer diverse mechanisms for the enjoyment of the right to personal data protection.

In this context, to ensure an "equivalent level of protection" to that provided by the GDPR, after the repeal of the Privacy Shield agreement, the European Union started negotiations with the United States to reach a new deal for data transfer. In March 2022, the UE and the US agreed in principle on the Trans-Atlantic Data Privacy Framework, based on which they will carry out the transfers while addressing the issues raised by the Court of Justice of the European Union with the Schrems II decision. In line with the Court decision, this mechanism provides US intelligence authorities with limited access to personal data in order to protect national security while adhering to the principle of proportionality[2]. In this context, we have to assess how the new US-EU agreement will address all of the issues highlighted by the court judgment, including the right to adequate judicial protection for the personal data of EU citizens.

Acknowledgement

This paper has been financially supported by the University of Shkodra "Luigj Gurakuqi".

References

[1] Arnaboldi, N. (2018). La nuova privacy. Gli adempimenti per imprese, professionisti e P.A. dopo il decreto di adeguamento al GDPR (D. Legs N. 101/2018), Maggioli Editore, Santarcangelo di Romagna.

[2] Bernardi, N. (A cura di), (2020). Privacy. Protezione e trattamento dei dati, Walters Kluwer, Milano.

[3] Commission Decision of 26 July 2000 (2000/520/EC) 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. Retrieved from https://eur-lex.europa.eu/eli/dec/2000/520/oj.

[4] Commission implementing decision (EU) 2016/1250. (2016, July 12) pursuant to directive 95/46/EC of the European Parliament and the Council on the Adequacy of the protection provided by the EU-U.S. Privacy Shield. Official

[2] Trans-Atlantic Data Privacy Framework, retrieved from file:///C:/Users/USER/Downloads/Trans-Atlantic_Data_Privacy_Framework.pdf.pdf.

Journal L 207/1, 01/08/2016. Retrieved from https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj.

[5] Commission implementing decision No. 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council. Retrieved from https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj.

[6] Court of Justice of the European Union (CJEU). (2003, November 6). Case C-101/01, Criminal proceedings against Bodil Lindqvist, para. 71. European Court Reports 2003 I-12971. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101.

[7] Court of Justice of the European Union (CJEU). (2010, November 9) Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, para. 48.

[8] Court of Justice of the European Union (CJEU). (2020, July 16). Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) paras 50-174. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311.

[9] Court of Justice of the European Union (CJEU). C-507/17. (2019, September 24). Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), para. 60.

[10] Court of Justice of the European Union (CJEU). Grand Chamber. (2015, October 6). Case C-362/14. M. Schrems v. Data protection Commissioner ("Schrems I"). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62014CJ0362.

[11] Court of Justice of the European Union (CJEU). Press release. No 91/20. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[12] Court of Justice of the European Union. (2013, October 17) Schwarz, C-291/12, EU:C:2013:670, para. 33.

[13] De Mozzi, B. (2022). Il ruolo delle binding corporate rules: economia e autonomia individuale nel diritto europeo ed extra-europeo, in Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, A cura di C. Pisani, G. Proia, A. Topo, Giuffrè, Milano, pp. 140-161.

[14] EU Regulation No. 2018/1725. (2018, October 23). On the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) no 45/2001 and decision no 1247/2002/EC. Official Journal of the European Union, L 295/39, 21.11.2018. Retrieved from http://data.europa.eu/eli/reg/2018/1725/oj.

[15] European Data Protection Board (EDPB). (2018, May 25). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

[16] European Data Protection Board (EDPB). (2020, November 10). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, pp. 5-8. Retrieved from https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf. [17] European Union. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, C. 326/391, 26.10.2012.

[17] European Union. Treaty on the European Union and the Treaty on the Functioning of the European Union. Official Journal of the European Union, C 326, 26/10/2012, 1 – 390.

[18] Garante per la Protezione dei Dati Personali (GPDP). (2019). Applicare il GDPR: Linee guida Europee, 350. Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9277035.

[19] Imperiali, Rich. & Imperiali, Ros. (2003). Il trasferimento all'estero dei dati personali, Milano, pp. 8 et seq.

[20] Kirschen, S. (2019). Il trasferimento all'estero dei dati, in Circolazione e protezione dei dati personali, tra libertà e regole del mercato, A cura di R. Panetta, pp. 261-291.

[21] Meltzer, J. P. (2020). The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security, retrieved from

https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

[22] Piroddi, P. (2021). Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, in Codice della Privacy e data protection, Giuffrè, Milano, pp. 616-680.

[23] Regulation (EU) 2016/679. (2016, April 27). On the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[24] Trans-Atlantic Data Privacy Framework, retrieved from file:///C:/Users/USER/Downloads/Trans-Atlantic_Data_Privacy_Framework.pdf.pdf.

[25] Valsecchi, Ch. (2022). Il diritto alla riservatezza nella ricostruzione stotico-giuridica, in Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, A cura di C. Pisani, G. Proia, A. Topo, Giuffrè, Milano, pp. XXVII-LXXXI.