Studia Iuridica 107
ISSN 0137-4346; e-ISSN 2544-3135

https://doi.org/10.31338/2544-3135.si.2025-107.8

Ewa Milczarek
University of Szczecin, Poland
e-mail: ewa.milczarek@usz.edu.pl
ORCID:0000-0003-0726-0959

SECURITY OF CROSSBORDER DATA TRANSFER – THE EU-USA PERSPECTIVE

Abstract

In the era of the information society, the security of personal data has become a key issue, both at the individual and state levels. Significant challenges arise in the context of cross-border data transfers between the European Union and the United States, where differences in approaches to privacy protection and legal frameworks create numerous tensions and difficulties. The main issues concern the lack of coherent legal frameworks allowing for the secure transfer of personal data to the United States in compliance with EU privacy standards. Previous mechanisms, such as Safe Harbor and Privacy Shield, were deemed incompatible with EU regulations by the Court of Justice of the European Union, leaving data flows in a legal vacuum.

The study aims to analyze the current conditions of cross-border data transfers between the EU and the US in the context of protecting the security and privacy of EU citizens' data. The key outcome is to identify potential regulatory scenarios that could ensure effective protection of Europeans' personal data. The analysis includes case studies of regulatory mechanisms (Safe Harbor, Privacy Shield) and EU legal frameworks, such as the GDPR, in light of CJEU decisions. The research also explores possible future scenarios for transatlantic data transfer cooperation, examines the political and legal differences in privacy approaches between the EU and the US, and considers alternative solutions, such as data localization or technical protection barriers.

KEYWORDS

data transfer, EU-US, data protection, GDPR, Safe Harbor, Privacy Shield, cross-border regulations

SŁOWA KLUCZOWE

przekazywanie danych, UE-USA, ochrona danych, RODO, program *Safe Harbor*, program *Privacy Shield*, przepisy transgraniczne

1. INTRODUCTION

In the era of the information society, data security becomes of key importance in the individual and national context. The influence of the United States in this matter is undoubtedly significant. The United States has control over network and server management. They also have a substantial impact on the largest Internet companies, such as Facebook, Google and Microsoft, which are used by billions of people around the world.

The data flow between the EU and other countries is an indispensable part of the Internet. This transfer should be implemented in compliance with EU data security standards. One way of transferring personal data abroad is based on a decision by the European Commission, which states that a given country applies adequate protection of personal data.

Since 2000, this flow has been based on the Safe Harbor scheme,[1] annulled by the judgment of the CJEU in the *Schrems* case.[2] A similar fate befell the successor of the program – the Privacy Shield, which was invalidated by the CJEU under the *Schrems II* judgment[3] in 2020. Since then, it has not been enough to reach an agreement between the EU and the US, leaving the data flow regulations in a legal vacuum.

---

[1] 2000/520/EC: Commission Decision 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), L 215, 25/08/2000.

[2] Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd,* ECLI:EU:C:2015:650.

[3] Judgment of CJEU of 16 July 2020, C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* ECLI:EU:C:2020:559.

The chapter is divided into three analytical parts. The first of them defines the conditions for secure cross-border data flow based on standards developed by EU legislation and case law. The second part is devoted to legal forms that allow cross-border data flow between the EU and the US. The third part presents possible scenarios for future US-EU cross-border data transfers. The research objective of this chapter is to determine the current conditions of data flow to the United States in terms of security and privacy protection of EU citizens. The result of the considerations is the determination of how the cross-border data flow between the US and the EU should be regulated to protect the privacy of Europeans.

2. DATA SECURITY AND PRIVACY IN THE EU – OUTLINE OF THE SUBJECT

The intensive development of the Internet has led to the transfer of most social and economic contacts to the Internet, thus facilitating access to information. Technological advances open up possibilities for highly sophisticated surveillance and espionage, through methods where the older rules of the game may not be enough to keep everything in check.[4] Privacy and data protection are the most vulnerable in the face of new pressures from surveillance technology.[5]

The experience related to the development of the Internet led to the conclusion that online privacy and data protection require different tools than those that were sufficient offline. For years, the internet environment has developed without significant government oversight. Left unsupervised, the sector created its own regulations, often detached from offline legal relationships. The innovative[6] and transnational nature of the Internet makes it difficult for legislators to define an appropriate legal framework for effective data protection. The European Union is trying to meet these challenges. In the last years, the EU privacy protection system has evolved[7] to be more responsive to the challenges of the information

[4] Stig Strümholm, 'Right of Privacy and Rights of The Personality a Comparative Survey; Working paper prepared for the Nordic Conferen.ee on privacy organized by the International Commission of Jurists' (Stockholm 1967), 18–19.

[5] Alan Westin, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy' (1966) Columbia Law Review 66 (6), 1003–1050.

[6] Colin J. Bennett, 'Regulating Privacy: Data Protection and Public Policy in Europe and the United States', Cornell University Press, (New York, 1992), 4–5.

[7] Denitza Toptchiyska, 'The Rule of Law and EU Data Protection Legislation: Some Controversial Issues in light of the new EU General Data Protection Regulation', (2017) The ORBIT Journal 1(1), 1–16, doi.org/10.29297/orbit.v1i1.16.

society. Today, one of the main aims of the European Area of Freedom, Security and Justice is stronger data protection.[8]

The EU considers privacy and protection of personal data to be fundamental rights. Articles 7 and 8 of the Charter of Fundamental Rights of the EU[9] (the Charter) provide that 'everyone has the right' to the 'protection of personal data concerning him or her' and that data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. Article 52 of the Charter states that any limitations on these rights must be subject 'to the principle of proportionality' and must be 'necessary and genuinely meet objectives of general interest of the Union or the need to protect the rights and freedom of others'. These rights are implemented by a number of legal acts, of which the most important is the General Data Protection Regulation (GDPR),[10] which constitutes a general legal framework providing rules on the processing of personal data in the EU. The reform added a new value to the informational sovereignty of EU citizens in the digital space.[11] The GDPR formulates principles relating to personal data processing, which are: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability.[12] One of the aspects regulated in GDPR is the transfer of European Union citizens data to third countries, including the US.

The United States was the birthplace of the Internet, so from the very beginning, it played a key role in its development.[13] This affected the strategic role of the United States in network and server management. Also, since the 1990s, commercialization of the internet took off, leading to the development of new industries, such as e-commerce and online advertising. The companies of the United States

[8] Danijela Vrbljanac, 'Personal Data Transfer to Third Countries – Disrupting the Even Flow?', (2018) Athens Journal of Law 4 (4), 349, 337–358, doi.org/10.30958/ajl.4-4-4.

[9] Charter of Fundamental Rights of the European Union, Arts 7–8, 18 December 2000, 2000 O. J. C 364/1.

[10] 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, 1–88.

[11] Mira Burri and Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy', (2016) Journal of Information Policy 6, 506, 479–511.

[12] Efrén Díaz Díaz, 'The New European Union General Regulation on Data Protection and the Legal Consequences for iInstitutions, Church', (2016) Communication and Culture 1 (1), 206–239, doi.org/10.1080/23753234.2016.1240912.

[13] Barry M Leiner and others, *A brief history of the internet*, (2009) Computer Communication Review 39(5), 22–31, doi.org/10.1145/1629607.1629613.

took the lead in this. Today, US technology companies, such as Google, Facebook, and Amazon, continue to dominate the global internet landscape. Also, US-based online platforms, when their services are used within the territory of the EU, are bound to comply with both the EU and US data protection laws, including the data protection laws of all the respective Member States. It may become complicated for them to define their legal obligation in processing personal data.[14] Each of our activities on the Internet is related to the production of data and its flow. Most of the data flows to the United States. They, therefore, play a key role in terms of international data security.

3. EU-US DATA TRANSFERS REGULATIONS

Generally, GDPR allows to transfer personal data outside the UE if the third country provides an 'adequate level of protection' for the data (Article 45 GDPR) or when the controller adduces adequate safeguards with respect to the protection of privacy (Article 46 GDPR).

Data transfer between the EU and the US primarily occurs through data transfer mechanisms such as:

1. Decision of the European Commission that transfer of personal data from the EU to the US that has been deemed adequate.
2. Provision of appropriate safeguards and on condition:
   2.1.1. Standard contractual clauses (SCCs), SCCs are agreements between data controllers and data processors that ensure adequate data protection measures are in place. They are a form of Article 46 contractual clause pre-approved by the European Commission.
   2.1.2. Binding corporate rules (BCRs). BCRs are internal company policies and procedures for data protection that have been approved by European data protection authorities.
   2.1.3. Code of conduct or certification mechanism.
3. Consent.

This system was created hierarchically. The use of subsequent ones is possible when those 'higher' in the hierarchy have not been established.

[14] Shakila Bu-Pasha, 'Cross-border issues under EU data protection law with regards to personal data protection', (2017) Information & Communications Technology Law 26(3) doi.org/10.1080/13600834.2017.1330740.

3.1. ADEQUACY DECISION

Currently, data transfer to third countries is allowed under the GDPR if the European Commission considers the legal system of those countries as providing an 'adequate' level of personal data Protection.[15] GDPR facilitates transnational data transfers with improved mechanisms and provides procedures, conditions and restrictions for personal data transfers outside the EU, to third countries or to 'a territory or specified sector within a third country, or an international organisation' upon the European Commission's adequacy decision.[16] In order to determine the adequacy, the European Commission takes into account a number of factors, such as the existing legal system, criminal law and access to justice in the country in question; inter alia: the rule of law, respect for human rights and fundamental freedoms and relevant legislation, including in the field of data protection, defence, national security and criminal law, and access by public authorities to personal data. The system is to guarantee effective, enforceable rights, including the right to effective administrative and judicial remedies for individuals and the existence of an effectively functioning independent supervisory authority. Compliance with legally binding conventions, in particular the Council of Europe Convention No 108,[17] and participation in multilateral or regional data protection regimes should also be considered.

So far, the flow between the United States and the European Union has been carried out around two programs: Safe Harbor[18] (2000–2015) and Privacy Shield (2016–2020). Neither of these programs can be considered successful – they were withdrawn after the CJEU judgments declaring them incompatible with EU law. The analysis below will provide a clue to the problems with the functioning of these two programs. It should be noted at the outset that the Safe Harbor and Privacy Shield programs were implemented before the introduction of the GDPR (but Privacy Shield was in effect during the GDPR period).

[15] Chapter V (Arts 44–49) of the GDPR.
[16] Recitals 103–107, 169, Art 45 GDPR.
[17] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No 108).
[18] 2000/520/EC: Commission Decision 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), L 215, 25/08/2000 P. 0007 – 0047.

3.1.1. SAFE HARBOR

Directive 95/46/EC[19] (GDPR predecessor) also allowed for cross-border data transfer based on the decision of the European Commission recognizing the adequacy of the principles of the program to the European level of protection of personal data. Enterprises wishing to join the Safe Harbor program or wishing to undergo certification notified their intention to the US Department of Commerce. Directive 95/46/EC forbids the transfer of personal data to a third country that does not ensure an adequate level of protection. Third countries can ensure different solutions of protection, varying from those employed within the European Union. However, requirements must be effective in order to ensure protection essentially equivalent to that guaranteed within the European Union. The CJEU found that Safe Harbor did not meet these conditions.[20] Undermining the effectiveness of Safe Harbor was related to the disclosure of data collection practices by US intelligence services, including through the PRISM[21] and FISA[22] program.[23]

The European Commission has confirmed reservations about the level of protection of personal data of EU citizens transferred to the United States under the Safe Harbor program due to the voluntary and declarative nature of the system. US authorities have had access to personal data of EU citizens transferred to the US under the Safe Harbor program and may process it in a way that is incompatible with EU data protection principles. Most US internet companies targeted by surveillance programs such as PRISM or FISA have had Safe Harbor clearances,[24] thus, it has become one of the channels for US intelligence authorities to access personal data which has been pre-processed in the EU.

[19] 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, L 281, 23/11/1995 P. 0031 – 0050.

[20] Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd,* ECLI:EU:C:2015:650.

[21] Liane Colonna 'Prism and The European Union's Data Protection Directive', (2013) The John Marshall Journal of Information Technology & Privacy Law 4 (3), 203–221.

[22] Foreign Intelligence Surveillance Act of 1978 (FISA Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36).

[23] Ewa Milczarek, 'Prywatność wirtualna: unijne standardy ochrony prawa do prywatności w Internecie, (Warszawa 2020), 176–183.

[24] Dot. 2 Communication From the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, Brussels, 29 February 2016, COM(2016) 117 final.

The following deficiencies were identified:[25]

- certified US companies do not adhere to the Safe Harbor principles for secure data transfer;
- structural deficiencies were found in transparency and law enforcement, as well as in specific Safe Harbor principles and the functioning of the National Security Clause;
- the program also acts as a conduit for the transfer of personal data of EU citizens from the European Union to the US through companies required to provide data to US intelligence services under US data collection programs.

The US law enforcement requirements, including assurance of national security and public interest, received preference over the Safe Harbour framework. The US public authorities would prevail, allowing the US undertakings to ignore the Safe Harbour principles.[26]

This information undermined the trust of both EU citizens and EU institutions in the security of cross-border data transfers to the United States. Resolution of the European Parliament from 2014 calls on the US to 'revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens'.[27]

As Simon Davies points out, the Safe Harbor was 'generally viewed as a minimalist solution that was supposed to evolve into something stronger. It transpired, however, that the United States never intended to follow through on commitments to strengthen it'.[28]

The European Commission has started work on a new agreement. It should be remembered that after the end of Safe Harbor, data transfer to the United States continues (the majority of companies can continue using the conventional

[25] Dot. 3.2. ibid.

[26] Martin A Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research Service, 19 May 2016) 6. <https://sgp.fas.org/crs/misc/R44257.pdf> .

[27] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), C 378/104.

[28] Simon Davies, 'Privacy Opportunities and Challenges with Europe's New Data Protection Regime' in Privacy in the Modern Age 55, 57 (Marc Rotenberg, Julia Horwitz & Jeramie Scott (eds), The New Press 2015).

SCCs). The lack of an agreement raises even greater doubts about the security of cross-border data transfers.[29]

3.1.2. PRIVACY SHIELD

On 12 July 2016, the European Commission adopted a decision[30] recognizing the new program, the Privacy Shield, as meeting an adequate level of protection of personal data in accordance with EU standards.[31] Like Safe Harbor, it was based on the mechanism of self-certifying companies located in the United States. Also, the principles themselves are similar to those under the Safe Harbor[32] (notice; purpose limitation; compliance responsibility or accountability; relevancy; recourse). The similarities were so significant that, according to Schrems, Privacy Shield was only a 'soft update' of the Safe Harbor.[33] The program also raised objections as to its compliance with the CJEU guidelines set out in *Schrems I*.[34]

US companies had to register with the US Department of Commerce. The Department was responsible for managing and administering the Privacy Shield and ensuring that enterprises complied with their commitments. Companies operating under the scheme had to inform EU citizens about: the types of personal data they processed, the reasons for processing the personal data, whether they intended to transfer personal data to other companies and for what purpose. The protection of individuals' rights and access to justice was slightly improved. Complaints were resolved either by the company itself or by national data protection authorities, who then would contact the Federal Trade Commission. An arbitration route was also introduced.[35]

---

[29] David Bender, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective' (2016) International Data Privacy Law 6 (2), 117–138. doi.org/10.1093/idpl/ipw005.

[30] 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. L 207/1.

[31] <https://www.privacyshield.gov/welcome> accessed 1 January 2022.

[32] Gregory W Voss, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) Journal of Internet Law 19(11), 1, 9–18.

[33] Max Schrems, 'The Privacy Shield is a Soft Update of the Safe Harbor' (2016) European Data Protection Law Review. 148, doi.org/10.21552/EDPL/2016/2/4.

[34] Xavier Tracol, 'EU–U.S. Privacy Shield: The saga continues' (2016) Computer Law & Security Review 32(5), 775-777, doi.org/10.1016/j.clsr.2016.07.013; Fabien Terpan, 'EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?' (2018) European Papers 3, 1045-1059, doi: 10.15166/2499-8249/261.

[35] European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, 12 July 2016, <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461>.

In 2017, the first review of the functioning of the program took place. Article 29 The Working Party[36] and the European Data Protection Supervisor described its functioning as far from satisfactory.[37] They recommendations, among others included: more active and regular monitoring of enterprises in terms of meeting the obligations imposed by the Privacy Shield by the US Department of Commerce; increased scrutiny of companies misleading their users about their participation in the scheme; strengthening cooperation between the Department of Commerce and the Federal Trade Commission and EU data protection authorities to develop appropriate guidance for companies and law enforcement authorities; appointment of the Privacy Shield Ombudsman.[38]

Privacy Shield was the subject of another Schrems' complaint to the CJEU.[39] In July 2020, the CJEU declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programmes, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. In particular, the CJEU highlighted two problems with the US system: that intelligence agencies' abilities to collect and analyse EU citizens' data (like US surveillance programmes such as PRISM and UPSTREAM[40]) was unnecessarily broad and included inadequate safeguards to protect rights and the judicial review mechanisms for EU citizens did not meet the standards required by the EU Charter of Fundamental Rights.[41]

3.1.3. TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

In March 2022, the EU and USA announced the agreement in principle on the Trans-Atlantic Data Privacy Framework. Under the framework, US intelligence agencies are to adopt procedures to ensure effective oversight of new privacy

[36] The Article 29 Working Party was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR).

[37] European Data Protection Supervisor Annual Report 2018, Executive Summary, Luxembourg: Publications Office of the European Union, 2019, 7.

[38] Report From The Commission To The European Parliament And the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield{SWD(2017) 344 final}, Brussels, 18.10.2017COM(2017) 611 final, 5–7.

[39] Judgment of CJEU of 16 July 2020, C-311/18 , *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* ECLI:EU:C:2020:559.

[40] Caspar Bowd and Didier Bigo, 'Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs Civil Liberties, Justice And Home Affairs, The US surveillance programmes and their impact on EU citizens' fundamental rights', PE 474.405.

[41] Dara Hallinan and others, 'International transfers of personal data for health research following Schrems II: a problem in need of a solution'; (2021) European Journal of Human Genetics 29, 1502–1509, doi.org/10.1038/s41431-021-00893-y.

and civil liberties standards; a new two-tier redress system to investigate and resolve complaints of Europeans on access to data by US Intelligence authorities, which includes a Data Protection Review Court.[42] In August 2025, the European Commission and the United States Trade Representative reached an agreement on a Framework Agreement for Reciprocal, Fair and Balanced Trade, marking a new stage in transatlantic economic cooperation.[43]

3.2. ADEQUATE SAFEGUARDS WITH RESPECT TO THE PROTECTION OF PRIVACY

In the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Those safeguards are:[44]

- the so-called binding corporate rules – in the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on internal policies approved by the competent supervisory authority, which ensure adequate data protection safeguards across the group;
- contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission;
- adherence to a code of conduct or certification mechanism, together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.

3.2.1. STANDARD CONTRACTUAL CLAUSES

Standard contractual clauses (SCCs) are 'standardised and pre-approved model data protection clauses that allow controllers and processors to comply with their obligations under EU data protection law'.[45] In 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers

[42] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework <https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087>.
[43] Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade <https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en >.
[44] <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en>.
[45] The New Standard Contractual Clauses – Questions And Answers Overview, <https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf>.

from controllers or processors in the EU to controllers or processors established outside the EU.[46]

There are two sets of Standard Contractual Clauses:

- SCCs for the relationship between controllers and processors based on Article28(3) and (4) of 'GDPR' and on Article 29(3) and (4) of Regulation 2018/1725[47] – which can be used by public and private entities as well as by EU institutions, bodies, offices and agencies.
- SCCs as a tool for data transfers[48] to comply with the requirements of the GDPR fortransferring personal data to countries outside of the EEA. The are most used data transfer instrument for European companies.[49]

The protection may differ from that in the EU, as long as they prove to be effective in practice. The objective is not to mirror the European legislation point by point, but to establish the essential core requirements of that legislation.[50] Aspects such as the essence of the right to privacy, its effective implementation, enforcement and supervision should be taken into account. Obligations of the parties include standards like: purpose limitation; transparency; accuracy and data minimisation; storage limitation; security of processing. The CJEU in *Schrems II*, stipulated stricter requirements for the transfer of personal data based on standard contract clauses (SCCs). Data controllers or processors that intend to transfer data based on SCCs must ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the General Data Protection Regulation (GDPR) and the EU Charter of Fundamental Rights (CFR) – if necessary, with additional measures to compensate for lacunae in the protection of third-country legal systems. When failing to meet that requirement, operators must suspend the transfer of personal data outside the EU.

---

[46] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance).

[47] Regulation (Eu) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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.

[48] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972 OJ L 199, 7 June 2021, 31–61.

[49] PP-EY Annual Privacy Governance Report 2019.

[50] Laura Bradford, Mateo Aboy, Kathleen Liddell, 'International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an "adequate" level of protection' (2020) Journal of Law and the Biosciences 7(1), doi: 10.1093/jlb/lsaa055.

Standard contractual clauses (SCCs), the main alternative legal mechanism for EU-US data transfers, are also vulnerable. Complaints, investigations and potentially suspensions of SCCs used to transfer data to the US are highly likely to increase in the coming years. This implicates major internet and telecommunications companies being most affected by the US mass surveillance law.

3.2.2. BINDING CORPORATE RULES (BCR)

Binding Corporate Rules are one of the ways in which such adequate safeguards (Article 47 GDPR) may be demonstrated by a group of undertakings, or a group of enterprises engaged in a joint economic activity. BCR was first introduced by Article 29 Data Protection.[51]

Binding corporate rules constitute an important aspect. They are internal rules adopted by multinational groups of enterprises in order to transfer data within the same group of enterprises to related entities located in countries that do not provide an adequate level of protection.[52] BCRs are designed to facilitate data transfers within an organisation and must be approved by the competent domestic supervisory authority in accordance with Article 63 of the GDPR. They are approved when two conditions are achieved, namely that they are legally binding, applied and enforced by every member concerned of the group of undertakings or enterprises, including employees, and that they expressly confer enforceable rights on data subjects.[53]

This requires approval from the relevant EU data protection authority to facilitate data transfers within a company or group of companies. They are almost exclusively used by large multinational corporations operating in multiple jurisdictions, because they are relatively costly and burdensome for organisations.[54]

Unlike the SCCs, there is no set wording for the BCRs, so companies can tailor them to suit their own needs.[55]

---

[51] Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, 17/EN WP264.

[52] Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, Brussels, 10 January 2017 COM(2017) 7 final.

[53] Danijela Vrbljanac, 'Personal Data Transfer to Third Countries – Disrupting the Even Flow?' (2018) Athens Journal of Law 4(4), 345, 337–358.

[54] Oliver Patel and Dr Nathan Lea, 'EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows', (2020) UCL European Institute Policy Paper, 9.

[55] Philip Rees, Dominic Hodgkinson, 'Binding Corporate Rules: A simpler clearer vision?' (2007) Computer Law & Security Review 23(4), 352-356, doi.org/10.1016/j.clsr.2007.03.004.

3.2.3. CODE OF CONDUCT

Code of conduct is a new transfer mechanism introduced by Articles 40(3) and 46(2)(e) GDPR. Once approved by the competent supervisory authority and having been granted general validity within the Union by the Commission, a code of conduct may be adhered to and used by controllers or processors not subject to the GDPR located in third countries, for the purpose of providing appropriate safeguards to data transferred to third countries. Then, the controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code, including with regard to the rights of data subjects as required by Article 40(3).

In the meaning of Article 46, the following elements need to be addressed:[56]

- Essential principles, rights and obligations arising under the GDPR for controllers/processors;
- Guarantees that are specific to the context of transfers (such as with respect to the issue of onward transfers, conflict of laws in the third country).

As Krekora-Zając and Marciniak point out, the codes of conduct provide an unprecedented possibility of the sector self-regulation, enabling a real influence on the adopted regulations to all stakeholders.[57] Nevertheless, the role of such a code of conduct is not to supplant the GDPR's obligations, only to clarify and assist in interpreting them in a particular context. It is possible to violate the GDPR even assuming perfect adherence to an approved code of conduct.[58]

3.3. CONSENT

Moreover, when a transfer can be made based on a number of derogations for specific situations, for example, where an individual has explicitly consented to the proposed transfer after having been provided with all the necessary information about the risks associated with the transfer[59] (Article 49(1)(a) GDPR). In view

[56] Guidelines 04/2021 on Codes of Conduct as tools for transfers.
[57] Dorota Krekora-Zając, Błażej Marciniak and Jakub Pawlikowski, 'Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on the GDPR art.40' (2021) Frontiers in Genetics 12:711614, doi: 10.3389/fgene.2021.711614.
[58] Mark Phillips, *International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)* (2018) Human Genetics 137(8), 575-582. doi: 10.1007/s00439-018-1919-7.
[59] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 adopted on 25 May 2018.

of recital 111 GDPR, data transfers on the grounds of this derogation may take place 'where the transfer is occasional and necessary in relation to a contract. Also transfer must be necessary for important reasons of public interest or for the establishment, exercise or defense of legal claims or 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. Transfer must be made from a public register'.

Obligations regarding the consent:

- Consent must be explicit;
- Consent must be specific for the particular data transfer/set of transfers;
- Consent must be informed, particularly as to the possible risks of the transfer.

According to Article 49(4), only public interests recognized in European Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.

4. FUTURE OF EU-US DATA TRANSFER – REVIEW OF SCENARIOS

The influence of the US on EU data transfer continues to be a topic of discussion and negotiation between the two regions. Also, these two regions have different approaches to data privacy and protection – an emphasis on self-regulation in the former versus strict legal requirements in the latter.[60] Both authorities have an interest in enforcing their privacy laws in an extraterritorial manner.[61]

Data protection depends on normative commitments established in advance.[62] The failure of Safe Harbor and Privacy Shield weakens the security of Europeans. The lack of implementation of data protection standards in such a significant element as the EU-US data flow allows us to conclude that the protection is only theoretical. Moreover, Safe Harbor and Privacy Shield were focused on legalistic

[60] Gerhard Steinke, 'Data privacy approaches from US and EU perspectives', (2002) Telematics and Informatics 19 (2), 193-200, doi.org/10.1016/S0736-5853(01)00013-2.

[61] Briseida S Jiménez-Gómez, 'Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic DisputeTransatlantic Dispute', (2021) Santa Clara Journal of International Law 19(2) 44.

[62] Derek E Bambauer, 'Privacy Versus Security', (2013) Journal of Criminal Law and Criminology 103(3) 673, 667–684.

mechanisms to protect data transfers rather than on protection in practice.[63] This raises doubts about the effectiveness of the current regulatory direction.

Alkiş-Tümtürk points out that the best and quickest way for the US to achieve an adequate level of data protection may be a two-way data protection approach with stricter Supplementary Rules covering only EU data subjects; requiring intelligence services to stop accessing data received from the EU unless there is a reasonable concern for national security; ensuring an independent oversight mechanism; and providing effective redress mechanisms especially in the event of intelligence services' non-proportional and limitless access.[64] In my opinion, the problem is not legal or practical, but political. The US does not want to comply with EU data protection guidelines. It is worth noting that during the Privacy Shield and current negotiations, the US government has implemented laws, such as the CLOUD Act.[65] CLOUD Act obligates the US companies to disclose information about the user, regardless of whether the information was stored in the US or outside the US. It is clear that laws like that are evidently contradictory to EU privacy laws.

The issue of regulating cross-border data flows is essential for the EU economy. However, it is worth noting that the United States' failure to comply with EU data protection standards is not solely due to a lack of political will or disregard for European values, but it also has a rational justification in the American logic of national interest. The measures taken by the US authorities, including the introduction of legal acts such as the CLOUD Act, are part of a broader strategy to ensure national security as well as combat terrorism and organised crime. In this context, access to data, including data processed by foreign companies, is seen as a key element of effective prevention and prosecution of serious crimes. This security logic may clash with the European perspective based on the primacy of individual rights and privacy protection, but it does not mean that the US position is irrational. At the same time, it seems reasonable to ask whether some of the security arguments are not also serving as a smokescreen for deeper economic interests, in particular, control over global data flows, which gives an advantage to US-based technology companies. Further analysis of US motivations, both explicit and implicit, could enrich the debate by providing a broader geopolitical and economic context.

---

[63] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal 18(4), 881-918. doi:10.1017/S2071832200022197.

[64] Asli Alkiş-Tümtürk, 'Uncertain future of transatlantic data flows: Will the United States ever achieve the 'adequate level' of data protection?' (2022) Hungarian Journal of Legal Studies 63(3), 308, 294–311 doi.org/10.1556/2052.2022.00376.

[65] Clarifying Lawful Overseas Use of Data Act or the CLOUD Act, H.R.4943.

The current state of uncertainty, when another agreement between the United States and Europe is called into question, prompts a change of perspective on this problem and the need to find an alternative solution. Christakis and Terpan indicate three possible scenarios for the future of EU-US relations:[66]

- the 'PNR' or 'TFTP' model – comprehensive and self-standing EU–US Agreement;
- the 'MLA' or 'Extradition' model – bilateral agreements between the US and EU Member States;
- mixed agreement of the two above options.

Moreover, many sectors, including the health sector, due to the critical need for data transfer, began to create *lex specialis* for their fields in the area of transfer based on the possibilities of GDPR (e.g., based on the code of conduct[67]). For health data, there are postulates that the transmission should be based on the HIPAA[68] shield.[69]

These solutions, however, do not include the clue to the problem of the general reluctance to adapt the American system to European standards. The source of the problem is divergence between European and American approaches to privacy.[70] In the American system, the right to privacy is a derivative of the right to property and personal inviolability.[71] In the European culture, the right to privacy is of a different nature.[72] It is an inherent element of human dignity and personal good. As a human right, it is universal, natural, inalienable and inviolable. This attitude to privacy is the foundation of liberal policy and the assumptions of the

[66] Theodore Christakis and Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', (2021) International Data Privacy Law (11) 2, 81–106, doi.org/10.1093/idpl/ipaa022

[67] Fruzsina Molnár-Gábor, Jan O Korbel, 'Genomic data sharing in Europe is stumbling – Could a code of conduct prevent its fall?' (2020) EMBO Molecular Medicine 12:e11421 doi.org/10.15252/emmm.201911421.

[68] Health Insurance Portability and Accountability Act of 1996.

[69] Laura Bradford, Mateo Aboy, Kathleen Liddell, 'International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection', (2020) Journal of Law and the Biosciences 7(1) doi.org/10.1093/jlb/lsaa055.

[70] Shannon Togawa Mercer, 'The Limitations of European Data Protection As A Model for Global Privacy Regulation' (2020) AJIL Unbound 114, 20–25. doi:10.1017/aju.2019.83

[71] Judith Jarvis Thomson, 'The Right to Privacy', (1975) Philosophy and Public Affairs 4, 308.

[72] Vera Bergelson, 'It's Personal but Is It Mine? Toward Property Rights in Personal Information' (2003) University of California, Davis Law Review 37, 383, 379–451; Jessica Litman, 'Information Privacy/Information Property' (2000) Stanford Law Review 52, 1286, 1283–1314.

rule of law.[73] Failure to unify these differences will always require one of the parties to 'give in'. However, neither side is willing to do so.

Due to the nature of the network, the EU should not only strive to ensure the protection of users on its territory, but also influence the global standard of data protection in the network by disseminating its values and standards. The unification of legal systems has a positive effect on ensuring the rights of Europeans. The problem of over-surveillance is not just between the EU and the US, but between the US and every region of the world.

There are various proposals among researchers related to the global unification of international privacy protection on the Internet. Briseida S Jiménez-Gómez suggests adopting the International Principles on the Application of Human Rights to Communications Surveillance[74] as a way to global protection of privacy as a human right. Yik-Chan Chin points out China's proposition of unification of the cross-border data flow in the following initiatives – 'Global Initiative on Data Security' and 'Global Security Initiative'.

It seems that developing common global standards is the best solution. However, this approach generates two main problems. The idea is to promote connectivity in the digital era and support the strengthening of international cooperation in the digital economy and security, including participating in or joining the negotiations on relevant regional trade rules.[75] Proposals to unify the online legal space have appeared since the beginning of the Internet's history. However, significant differences in legal cultures, along with the threat of legal dualism – i.e., varying online and offline protection, stand in the way. The second problem is more significant. It should be remembered that access to data gives enormous power. The question is whether the United States is able to give it up. If not, any agreement will exist only on paper.

The Internet, although it represents the global media, is becoming a legal regionalization. The regional protection is based on legal tradition and cultures, depending on the origin of region.[76] This allows to maintain a satisfactory level of

[73] Sławomir Oliwiak, 'Giorgio Agamben o prawach człowieka we współczesnym demokratycznym państwie prawa' in Marta Andruszkiewicz, Anetta Breczko and Sławomir Oliwniak (eds) *Filozoficzne i teoretyczne zagadnienia demokratycznego państwa prawa*, (Białystok 2015), 103.

[74] <https://www.eff.org/files/necessaryandproportionatefinal.pdf>.

[75] Yik-Chan Chin and Jingwu Zhao, 'Governing Cross-Border Data Flows: International Trade Agreements and Their Limits', (2022) Laws 11(4), 63; doi.org/10.3390/laws11040063.

[76] Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', (2011) OECD Digital Economy Papers 187 (OECD Publishing, Paris), 7. doi.org/10.1787/5kg0s2fk315f-en.

protection in a given region, but in a case such as trans-regional data transfer, it creates problems. It seems obvious that a company wishing to operate in the EU should respect the local legal system. That means we need to consider the need for companies to transfer personal data from the EU to third states in general and to the US in particular. Therefore, the possibility of storing and processing personal data on servers located in the European Union should be carefully considered as a legitimate and feasible alternative to data transfers outside the EU.[77] Nevertheless, some researchers argue that data localization neither solves the problem of foreign surveillance, nor enhances personal privacy, while undermining other values embraced by the European Union.[78] Also, the technological solutions like encryption will not prove useful in all contexts.[79]

5. CONCLUSIONS

The development of the information society, including the transfer of social, economic and political relations to the Internet, increases the risk related to the use of data by unauthorized entities. The development of sophisticated methods of surveillance on the Internet combined with big data technologies, which allow for real-time analysis of large amounts of data, affects the security of individuals of entire societies. Protecting the right to privacy on the Internet is an ever-changing challenge. Rapid technological changes require a flexible approach that allows you to quickly adapt to new threats.

EU is shaping how the world thinks about data privacy.[80] The EU has impacted the development of data protection laws globally and taken an essential role. Standards developed by the EU often become the basis for regulations in other regions. The world is, therefore, watching how the EU will deal with the problem of cross-border data transfer to the US.

[77] Xavier Tracol, '"Schrems II": The return of the Privacy Shield', (2020) Computer Law & Security Review 39, doi.org/10.1016/j.clsr.2020.105484.
[78] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) Journal of International Economic Law 23 (3), 771–784, doi.org/10.1093/jiel/jgaa024.
[79] Maria Helen Murphy, 'Assessing The Implications Of Schrems Ii For Eu–Us Data Flow, (2022) International & Comparative Law Quarterly 71(1), 245–262. doi:10.1017/S0020589321000348.
[80] Paul M Schwartz, 'Global Data Privacy: The EU Way', (2019) New York University Law Review 94 (4), 771, 771–818.

Over the years, tensions have arisen in the USA-EU data transfer relationship.[81] The United States claims that the EU has burdensome standards. The EU, after many scandals related to the illegal use of data by US surveillance authorities, also approaches cross-border transfers with due caution.

The existing solutions, which have been described in this chapter, provide only theoretical protection. They cannot be considered sufficient in terms of protecting the security of European data. Solving problems with data transfer between the EU and the US is not an easy task. This problem results from significant differences between the European and American legal systems, mentality and understanding of the essence of the right to privacy. The EU approach is significantly different than US privacy law.[82] However, the crux of the problem is not the legal impossibility of regulating the transfer. The problem is political will. The transfer of personal data from Europe to the US will remain an issue because it is not likely that the US will adopt privacy rules that could lead to an adequacy status.[83] The adoption of legislation such as the CLOUD Act shows that the United States is not interested in limiting its access to the data of third-country nationals.

The dominant role of the United States in the internet area makes negotiations difficult. Despite violating the principles of Safe Harbor and Privacy Shield, respectively, data transfer takes place continuously. The US is, therefore, not sufficiently interested in bringing its practices into line with EU requirements, as the absence does not result in the closure of the EU market. The solution to the situation is to take up the challenge by the EU in terms of developing technological barriers that inhibit access to the data of Europeans. Only if no one can reach them, only then will they be safe.

REFERENCES

Alkiş-Tümtürk A, 'Uncertain future of transatlantic data flows: Will the United States ever achieve the "adequate level" of data protection?' (2022) Hungarian Journal of Legal Studies 63(3), doi.org/10.1556/2052.2022.00376

[81] Maria Helen Murphy, 'Assessing The Implications Of Schrems Ii For Eu–Us Data Flow, (2022) International & Comparative Law Quarterly 71(1), 245–262. doi:10.1017/S0020589321000348.

[82] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means', (2019) Information & Communications Technology Law, 28:1, 65–98, doi: 10.1080/13600834.2019.1573501.

[83] Dorothee Heisenberg, 'Negotiating Privacy: The European Union, the United States, and Personal Protection', in the series iPolitics: Global Challenges in the Information Age (Boulder, 2005) doi.org/10.1515/9781626370074.

Bambauer DE, 'Privacy Versus Security', (2013) Journal of Criminal Law and Criminology 103(3)

Bender D, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective' (2016) International Data Privacy Law 6(2), doi.org/10.1093/idpl/ipw005

Bennett CJ, 'Regulating Privacy: Data Protection and Public Policy in Europe and the United States', Cornell University Press, (New York, 1992)

Bergelson V, 'It's Personal but Is It Mine? Toward Property Rights in Personal Information' (2003) University of California, Davis Law Review 37, 383, 379–451; Jessica Litman, 'Information Privacy/Information Property' (2000) Stanford Law Review 52

Bowd C and Bigo D, 'Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs Civil Liberties, Justice And Home Affairs, The US surveillance programmes and their impact on EU citizens' fundamental rights', PE 474.405

Bradford L, Aboy M, Liddell K, 'International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an "adequate" level of protection' (2020) Journal of Law and the Biosciences 7(1), doi: 10.1093/jlb/lsaa055

Bu-Pasha S, 'Cross-border issues under EU data protection law with regards to personal data Protection', (2017) Information & Communications Technology Law 26(3) doi.org/10.1080/13600834.2017.1330740

Burri M and Schär R, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy', (2016) Journal of Information Policy 6, 506

Chander Anupam, 'Is Data Localization a Solution for Schrems II?' (2020) Journal of International Economic Law 23 (3), doi.org/10.1093/jiel/jgaa024

Chin Y-Ch and Zhao J, 'Governing Cross-Border Data Flows: International Trade Agreements and Their Limits', (2022) Laws 11(4), doi.org/10.3390/laws11040063

Christakis Te and Terpan F, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', (2021) International Data Privacy Law (11) 2, 81–106, doi.org/10.1093/idpl/ipaa022

Colonna Liane 'Prism and The European Union's Data Protection Directive', (2013) The John Marshall Journal of Information Technology & Privacy Law 4 (3)

Davies Simon, 'Privacy Opportunities and Challenges with Europe's New Data Protection Regime, in Privacy in the Modern Age 55, 57 (Marc Rotenberg, Julia Horwitz & Jeramie Scott (eds), The New Press 2015)

Díaz Díaz Efrén, 'The new European Union General Regulation on Data Protection and the legal consequences for institutions, Church', (2016) Communication and Culture 1 (1) doi.org/10.1080/23753234.2016.1240912

Hallinan D and others, 'International transfers of personal data for health research following Schrems II: a problem in need of a solution'; (2021) European Journal of Human Genetics 29, doi.org/10.1038/s41431-021-00893-y

Heisenberg D, 'Negotiating Privacy: The European Union, the United States, and Personal Protection', in the series iPolitics: Global Challenges in the Information Age (Boulder, 2005) doi.org/10.1515/9781626370074

Hoofnagle ChJ, van der Sloot B and Zuiderveen BF, 'The European Union general data protection regulation: what it is and what it means', (2019) Information & Communications Technology Law, 28:1, doi: 10.1080/13600834.2019.1573501

Jiménez-Gómez BS, 'Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute Transatlantic Dispute', (2021) Santa Clara Journal of International Law 19(2) 44

Krekora-Zając D, Marciniak B and Pawlikowski J (2021) 'Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on the GDPR art. 40' (2021) Frontiers in Genetics 12:711614, doi: 10.3389/fgene.2021.711614

Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal 18(4), 881-918. doi:10.1017/S2071832200022197

--, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', (2011) *OECD* Digital Economy Papers 187 (OECD Publishing, Paris), 7. doi.org/10.1787/5kg0s2fk315f-en

Leiner BM and others, 'A brief history of the internet', (2009) Computer Communication Review 39(5), doi.org/10.1145/1629607.1629613

Milczarek E, 'Prywatność wirtualna: unijne standardy ochrony prawa do prywatności w Internecie, (Warszawa 2020)

Molnár-Gábor F, Korbel JO, 'Genomic data sharing in Europe is stumbling – Could a code of conduct prevent its fall?; (2020) EMBO Molecular Medicine 12:e11421 doi. org/10.15252/emmm.201911421

Murphy MH, 'Assessing The Implications Of Schrems Ii For Eu–Us Data Flow, (2022) International & Comparative Law Quarterly 71(1). doi:10.1017/S0020589321000348

Oliwiak S, 'Giorgio Agamben o prawach człowieka we współczesnym demokratycznym państwie prawa' in Marta Andruszkiewicz, Anetta Breczko and Sławomir Oliwniak (eds) *Filozoficzne i teoretyczne zagadnienia demokratycznego państwa prawa*, (Białystok 2015), 103

Patel O and Lea N, 'EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows', (2020) UCL European Institute Policy Paper, 9

Phillips Mark, *International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)* (2018) Human Genetics 137(8), 575-582. doi: 10.1007/s00439-018-1919-7

PP-EY Annual Privacy Governance Report 2019

Rees P, Hodgkinson D, 'Binding Corporate Rules: A simpler clearer vision?' (2007) Computer Law & Security Review 23(4), 352–356, doi.org/10.1016/j.clsr.2007.03.004

Schrems M, 'The Privacy Shield is a Soft Update of the Safe Harbor', (2016) European Data Protection Law Review 148, doi.org/10.21552/EDPL/2016/2/4

Schwartz PM, 'Global Data Privacy: The EU Way', (2019) New York University Law Review 94 (4)

Steinke G, 'Data privacy approaches from US and EU perspectives', (2002) Telematics and Informatics 19 (2), 193–200, doi.org/10.1016/S0736-5853(01)00013-2

Strümholm S, 'Right of Privacy and Rights of The Personality a Comparative Survey; Working paper prepared for the Nordic Conferen.ee on privacy organized by the International Commission of Jurists' (Stockholm 1967)

Terpan F, 'EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?' (2018) European Papers 3, doi: 10.15166/2499-8249/261

The Article 29 Working Party was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR)

Thomson JJ, 'The Right to Privacy', (1975) Philosophy and Public Affairs 4, 308

Togawa Mercer Shannon, 'The Limitations of European Data Protection As A Model for Global Privacy Regulation' (2020) AJIL Unbound 114, doi:10.1017/aju.2019.83

Toptchiyska D, 'The Rule of Law and EU Data Protection Legislation: Some Controversial Issues in light of the new EU General Data Protection Regulation', (2017) The ORBIT Journal 1(1) doi.org/10.29297/orbit.v1i1.16

Tracol Xavier, 'EU–U.S. Privacy Shield: The saga continues', (2016) Computer Law & Security Review 32(5), 775–777, doi.org/10.1016/j.clsr.2016.07.013;

--, '"Schrems II": The return of the Privacy Shield', (2020) Computer Law & Security Review 39, doi.org/10.1016/j.clsr.2020.105484

Voss G W, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) Journal of *T*ernet Law 19(11).

Vrbljanac D, 'Personal Data Transfer to Third Countries – Disrupting the Even Flow?' (2018) Athens Journal of Law 4 (4) doi.org/10.30958/ajl.4-4-4

-- 'Personal Data Transfer to Third Countries – Disrupting the Even Flow?', (2018) Athens Journal of Law 4(4), 345, 337–358

Weiss M A and A K, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research Service, 19 May 2016) 6. <https://sgp.fas.org/crs/misc/R44257.pdf>

Westin A, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy' (1966) Columbia Law Review 66 (6)