GIS Odyssey Journal

2021 • Volume 1 • Number 2

https://doi.org/10.57599/gisoj.2021.1.2.71

Beata Konieczna-Drzewiecka[1]

PASSENGER NAME RECORD (PNR) – REVIEW OF REGULATIONS

Abstract: The flows of personal data to and from countries outside the Union are essential to the development of international trade and cooperation. The increase in such flows has raised new challenges and concerns with respect to the protection of personal data, which the EU Data Protection Reform was intended to counteract. Since May 2018, the transfer of data to third countries can only take place in full compliance with the General Data Protection Regulation. However, in addition to this EU regulation, a number of regulations relating to the processing of passenger name record have been developed in the European Union. The aim of this article is to present these regulations and to show the impact of GDPR on them.

Keywords: General Data Protection Regulation, Safe Harbor, Privacy Shield, Advance Passenger Information, binding corporate rules

Received: 23 November 2021; accepted: 08 December 2021

[1] Cardinal Stefan Wyszyński University, Faculty of Law and Administration, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-9616-4055, email: b.konieczna@uksw.edu.pl

Introduction

In the era of digitization and constant development of new technologies, the need for data transfer is constantly growing. At the same time it is becoming increasingly difficult to maintain the information autonomy of European Union (EU) citizens. According to Rojszczak (2019), "information autonomy will not be complete if an individual is deprived of control over the circulation of information about him or her" (Ratajczak, 2019). Cross-border transfer of personal data, which involves the use of multiple devices by multiple parties, raises questions about legal protection instruments. In particular, there is a question how the EU regulations protect the rights of persons whose data are transferred to third countries.

For the transfer of flight passenger data PNR to third countries analyzed in this article, two events are relevant, i.e. the Edward Snowden case, which contributed to changes in EU data protection regulation, and then the judgment of the Court of Justice of the European Union (CJEU) in Maximilian Schrems v. Data Protection Commissioner Data Protection Commissioner and Facebook Ireland Ltd, which had a significant impact on the interpretation of the provisions of Chapter V General Data Protection Regulation (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).

As a reminder, in mid-2013. Edward Snowden, a former employee of the U.S. National Security Agency (NSA), published secret U.S. intelligence service documents revealing the service's practices of accessing personal data processed on the Internet through the services of leading providers such as Google, Microsoft, Yahoo!, Facebook, Apple, and LinkedIn. In the second case, Maximilian Schrems argued that US law and practice did not provide effective protection for personal data transferred to the US from the EU, including in particular the protection of Facebook users. He claimed that data from the service were transferred by an Irish company (Facebook Ireland Ltd) to servers on US territory belonging to Facebook Inc. US law allowed the collection of personal data of EU citizens who did not have effective legal protection.

Pre-GDPR regulations for PNR data

In 2000, a European Commission Decision was adopted on 26 July under Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles. Thus, the European Union recognized that U.S. companies that join the Safe Harbour program would be treated as providing an adequate level of protection for personal data. Companies or other entities only had to declare that they followed certain rules and report to the U.S. Department of Commerce (Commission Decision, 2008; Szpor, 2012).

Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data was adopted on 29 April 2004. It regulates the transfer of Advance Passenger Information (API) by air carriers to the competent national authorities in order to improve border controls and to combat illegal immigration. The Directive, also

known as the "API Directive", was implemented by Poland by the Act of 3 July 2002 – Aviation Law (Act, 2002).

On 6 November 2007, the European Commission presented a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 261,6.8.2004, p. 24). In this regard, the Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes has also been prepared (Opinion of the European Data Protection Supervisor, 2008). The EDPS pointed out that the proposal concerns the processing of PNR data within the EU, and is closely related to other systems of collection and use of passenger data, in particular the July 2007 agreement between the EU and the US. The proposal aimed to harmonise Member States' provisions on obligations for air carriers operating flights to or from the territory of at least one Member State to transmit PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and transnational organised crime. Within the EU, the proposal was intended to complement Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, known as API data, in order to combat illegal immigration and improve border controls. The directive was to be transposed into the national legislation of the Member States by 5 September 2006 at the latest. However, the European Commission's proposal became obsolete because the Council had not adopted it by 1 December 2009, the date of the entry into force of the Lisbon Treaty (The Treaty entered into force on 1 December 2009, whereas in the hierarchy of sources of law of the legal order of the Republic of Poland it is binding upon its announcement in the Journal of Laws, which took place on 2 December 2009 (Act, 2009).

Then, on 4 May 2010, the "Stockholm Programme – An open and secure Europe serving and protecting citizens" (The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 2010/C 115/01) called on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

In the Communication of 21 September 2010. on "The global approach to transfers of Passenger Name Record (PNR) data to third countries", the Commission presented the main elements of EU policy in this area. The Communication characterised the trends in the use of PNR data within the EU and in the world. The Commission considered it necessary for the EU to review its global approach on PNR (Communication from the Commission, 2010). In addition, the objective of the European Commission communicating the principles was to bring about greater convergence between the various PNR agreements and respect for the fundamental rights to respect for private life and to protection of personal data. At the same time, the Commission pledged to remain flexible in taking into account the specific security concerns of individual third countries and their national legal orders.

For example, on 29 September 2011, the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data by air

carriers to the Australian Customs and Border Protection Service was concluded in Brussels (Agreement EU-Australia, 2012). Subsequently, on 14 December 2011, an agreement was concluded in Brussels between the European Union and the United States of America on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (Agreement EU-USA, 2012).

The breakthrough came after the CJEU's Schrems ruling on October 6, 2015 (Judgment, C-362/14), in which the Court of Justice of the EU invalidated the European Commission's Decision 2000/520/EC of July 26, 2000 on the adequacy of the protection provided by the Safe Harbor Privacy Principles and the related Frequently Asked Questions issued by the U.S. Department of Commerce. The Court assessed the data protection rules under the Safe Harbor program against the standards that resulted from Directive 95/46/EC and the Charter of Fundamental Rights. It concluded that the US law allows public authorities almost unlimited and uncontrolled access to Europeans' data and thus undermines the very essence of the right to privacy. The decision approving the Safe Harbor program specifically alleged that: "the Principles apply (...) only to self-certified U.S. organizations that receive personal data from the Union, with no requirement that U.S. public authorities be required to respect the Principles" (Judgment, C-362/14). The impact of the ruling was also important for the negotiations of the TTIP agreement – the Transatlantic Trade and Investment Partnership. Completely different standards of privacy protection prevailing on both sides of the Atlantic were perceived by American companies as a barrier to unfettered economic development. The agreement has not been concluded so far.

The literature indicates that the interpretation of the Court of Justice has left its mark on the final form of Chapter V of the GDPR. It raised expectations for third countries, replacing the requirement of "adequate" protection with a standard of "substantial equivalence" (Grusza, 2020).

The principles of data transfer between Europe and the US were therefore called into question at the end of 2015, and data controllers had to look for other rationales to legalize data transfers while waiting for another agreement on data transfers between the two continents. On 12 July 2016, European Commission Implementing Decision (EU) 2016/1250 was adopted under Directive 95/46/EC of the European Parliament and of the Council, on the adequacy of the protection provided by the EU-US Privacy Shield, which concluded that the United States provides an adequate level of protection for the personal data of Europeans. Privacy Shield became the system that supports data flows between the European Union and the United States, replacing the Safe Harbor program. It should be mentioned that the Article 29 Data Protection Working Party, when giving its opinion on the draft Commission Decision 2016/2295 on the adequacy of the protection of personal data by certain countries, indicated that a detailed analysis of the conditions under which services from third countries can access the transmitted data should be made before taking a decision on adequacy (Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision).

The shield guaranteed a number of benefits, such as the right to receive information about the transfer of data and the right to access the data. The program also allowed control over whether a company was certified. In addition, U.S. companies wishing to self-certify and enjoy the benefits of program membership had to meet a number of requirements, such as being subject to the "investigatory and enforcement powers" of the Federal Trade Commission, the U.S. Department of Transportation, or "other statutory authority that effectively ensures compliance" (C(2016) 4176). The Shield required the organization to publish its privacy policy (Karwala, 2018).

Additionally, in 2016, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was adopted by Member States, which was implemented into the Polish legal order by the Act of 14 May 2018 on the Processing of Passenger Name Record Data (Act, 2018).

After GDPR regulations for PNR data

Even before the entry into force of the GDPR provisions, i.e. before 25 May 2018, the terms and conditions for the transfer of passenger flight data by air carriers and the processing of such data for the purposes of detecting, combating, preventing and prosecuting terrorist offences and other crimes or fiscal offences, as well as the entities competent in these matters, were regulated by the Law of 14 May 2018. In the explanatory memorandum to the draft law, it was pointed out that the provisions in force before May 2018 did not regulate matters concerning the processing of PNR data for the purpose of combating crime, but only regulated the transfer by air carriers, at the request of the commander of the relevant Border Guard post, of information concerning passengers on board an aircraft (API data) landing on the territory of the Republic of Poland. In the justification it was indicated that the solutions in this area constituting the transposition of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data were implemented into Polish law by the Act of 3 July 2002 – Aviation Law (Article 202a-202d and Article 209u, OJ 2016, item 605).

For the rest, the obligation of air carriers to transfer the PNR data they collect is governed by international agreements concluded between the European Union and third countries.

To this extent, the provisions of Chapter V of GDPR, which address the issue of transfer of data to third countries or international organizations, are applicable. As a rule, the Regulation provides for a prohibition of transfer of personal data to third countries and international organizations, which is not in fact expressed directly, but may be inferred from the overall regulation. However, the ban may only be lifted after it has been established that the third country ensures an adequate level of data protection. One of the ways indicated in Article 45 GDPR is that a transfer of data is permitted on the basis of a decision of the European Commission stating that the third country, a territory or a specific sector within that third country, or an international organization

ensures an adequate level (degree) of protection. On the other hand, in the absence of an implementing decision of the European Commission, the data exporter should proceed to the application of the appropriate measures provided for in the GDPR to compensate for the lack of protection (Fischer, 2018). The first group of safeguards legalizing the transfer does not require the consent of the supervisory authority and consists of the choice made by the transferring party from among: (1) binding corporate rules i.e. personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity, (2) standard data protection clauses adopted by the European Commission; (3) standard data protection clauses adopted by a supervisory authority and approved by the European Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR; (4) approved codes of conduct, which should be understood to mean accepted specific principles and practices for the processing of personal data; (5) approved certification mechanisms if they are linked to binding and legally enforceable obligations on the controller or processor in a third country (i.e. by contract or through other legally binding instruments) to apply appropriate safeguards, including with respect to the rights of data subjects; 6) a legally binding and enforceable instrument between bodies or entities belonging to the public law sphere, whereby the GDPR provides no indication as to the legal nature of such an instrument.

The group of safeguards that require authorisation by the supervisory authority includes: 1) contracts concluded between a controller or processor and a controller, processor or recipient of personal data in a third country or international organization (ad hoc contracts); 2) provisions of administrative arrangements between public authorities or entities, which will provide for enforceable and effective rights of data subjects.

In the context of considering the grounds for processing PNR data, it should be noted that after the enactment of the GDPR, the European Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, which, in conjunction with Article 46 of the GDPR, remained in force.

Also, many Commission decisions under the former Directive 95/46/EC, where the mechanism of country-by-country assessment was similar, remained in force until amended, replaced or repealed. The EC issued the following decisions concluding on the level of security of personal data in the following third countries (Table 1).

Table 1. European Commission Decisions concluding on the level of security of personal data in the following third countries

State	Commission Decision
Switzerland	Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act
Canada	Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act
Argentina	Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina
The County of Guernsey	Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey.
Isle of Man	Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man
Jersey	Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey
The Faeroe Islands	Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data
Andorra	Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra
Israel	Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data
Eastern Republic of Uruguay	Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data
New Zealand	Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand

Source: own study

In the context of this dispute between the Data Protection Commissioner and Facebook Ireland Ltd and Maximillian Schrems, a reference for a preliminary ruling was made to the Court of Justice on 9 May 2018. It seeks to interpret and examine the validity of Commission Decision 2010/87/EU and Commission Implementing Decision (EU) 2016/1250 on the adequacy of the protection afforded by the EU-US Privacy Shield.

In a judgment dated July 16, 2020, the Court of Justice of the EU challenged the Commission's finding that the United States provides a degree of protection substantively equivalent to that guaranteed in the European Union by the GDPR. Additionally, the Privacy Shield decision was annulled, so the program can no longer be the basis for data transfers to the U.S., and companies and others should either find another basis for the transfer or stop the transfer altogether.

Also, the entry into force on 27 June 2021 of European Commission Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries, replacing Commission Decision 2010/87/EU, does not change the status quo, especially since the existing standard clauses are to remain in force until 27 December 2022.

It is clear from the GDPR regulations that entities should not transfer data to a country that does not provide an adequate level of data protection. It is incumbent upon a controller who is established in the European Union to verify, prior to the transfer of data, whether the level of data protection in the country in question is equivalent to that required by Union law. An in-depth analysis of the law of the third country must therefore be carried out by the controller, including a reference to the access of public authorities to the transferred data. A thorough analysis of the judgment leads to the conclusion that the transfer of data to the US should not be based on the standard contractual clauses and that therefore the applicability of Commission Decision (EU) 2021/914 remains questionable.

Christopher Kruner points out that in a world marked by constitutional diversity and legal pluralism, it is an illusion to expect a legal order to be able to protect individuals on a global scale by persuading other states to adopt its own standards; rather, what is needed are creative solutions that take into account the differences of other legal systems and, ultimately, international treaty solutions (Kruner, 2014) and it is hard to disagree with him.

Entities, including those from third countries, that process personal data, including flight passenger data, operate within a legal framework. Therefore, it is difficult to expect that, in the case of a conflict of standards, an entity will ignore the provisions of its national law in favor of conflicting European regulations arising from contractual obligations. This demonstrates the weakness of the GDPR and Privacy Shield model of data protection for third country processors and the lack of legal means to oblige them to apply EU law. The Regulation, which aims to approximate legal solutions for data controllers in individual Member States, allowed the use of model clauses and Binding Corporate Rules. It also introduced new data protection guarantees in the form of approved codes of conduct and approved certification mechanisms. Systemically, however, the principles of data transfer to a third country have not fundamentally

changed. The judgment of the Court of Justice annulling the Privacy Shield Decision, which indicates that the United States does not provide a substantively equivalent level of protection to that guaranteed in the European Union, creates the need to seek another legal basis for the transfer of personal data, including flight passenger data, or forces the suspension of transfers. The above affects legal uncertainty, which is further burdened by the awareness of severe penalties for non-compliance.

Again, there is currently no systemic solution to legalize data transfers to the US. With regard to the transfer of personal data from the EU to third countries, including the U.S., the application of standard contractual clauses developed by the European Commission requires an EU entity to examine whether the legal system of the recipient country provides adequate protection of personal data. New solutions are therefore needed, with the existing contractual clauses still in force needing to be modified accordingly on the basis of the new ones introduced by Commission Decision (EU) 2021/914, and by 27 December 2022.

Conclusions

Christopher Kruner points out that in a world marked by constitutional diversity and legal pluralism, it is an illusion to expect a legal order to be able to protect individuals on a global scale by persuading other states to adopt its own standards; rather, what is needed are creative solutions that take into account the differences of other legal systems and, ultimately, international treaty solutions (Kruner, 2014) and it is hard to disagree with him.

Entities, including those from third countries, that process personal data, including flight passenger data, operate within a legal framework. Therefore, it is difficult to expect that, in the case of a conflict of standards, an entity will ignore the provisions of its national law in favor of conflicting European regulations arising from contractual obligations.

This demonstrates the weakness of the GDPR and Privacy Shield model of data protection for third country processors and the lack of legal means to oblige them to apply EU law. The Regulation, which aims to approximate legal solutions for data controllers in individual Member States, allowed the use of model clauses and Binding Corporate Rules. It also introduced new data protection guarantees in the form of approved codes of conduct and approved certification mechanisms.

Systemically, however, the principles of data transfer to a third country have not fundamentally changed. The judgment of the Court of Justice annulling the Privacy Shield Decision, which indicates that the United States does not provide a substantively equivalent level of protection to that guaranteed in the European Union, creates the need to seek another legal basis for the transfer of personal data, including flight passenger data, or forces the suspension of transfers. The above affects legal uncertainty, which is further burdened by the awareness of severe penalties for non-compliance. Therefore, work should be urgently undertaken to develop legal regulations guaranteeing safe data transfer to third countries, including the United States

Summary

There is currently no systemic solution to legalize data transfers to the United States. With regard to the transfer of personal data from the EU to third countries, including the United States., the application of standard contractual clauses developed by the European Commission requires an EU entity to examine whether the legal system of the recipient country provides adequate protection of personal data. New solutions are therefore needed, with the existing contractual clauses still in force needing to be modified accordingly on the basis of the new ones introduced by Commission Decision (EU) 2021/914, and by 27 December 2022.

References

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, pp. 4–16.

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 2015, 11.8.2012, pp. 5–14.

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, OJ L 2015, 25.8.2000, pp. 7–47.

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

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

Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, pp. 19–22.

Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, notified under document number C(2003) 4309, OJ L 308, 25.11.2003, pp. 27–28.

Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.4.2004, pp. 48–51.

Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, notified under document number C(2008) 1746, OJ L 138, 28.5.2008, pp. 21–23.

Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, notified under document C(2010) 1130, OJ L 58, 9.3.2010, pp. 17–19.

Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084, OJ L 277, 21.10.2010, pp. 27–29.

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

Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, notified under document C(2011) 332, OJ L 27, 1.2.2011, pp. 39–42.

Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, notified under document C(2012) 5704, OJ L 227, 23.08.2012, pp. 11–15.

Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, notified under document C(2012) 9557, OJ L 28, 30.1.2013, pp. 12–14.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, notified under document C(2016) 4176, OJ L 207, 1.8.2016, pp. 1–112.

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, OJ L 199, 7.6.2021, pp. 31–61.

Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM/2010/0492.

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 216, 6.8.2004, p. 4.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , OJ L 281, 23.11.1995, pp. 31–50.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection,

investigation and prosecution of terrorist offences and serious crime, (OJ UE L 132, 4.5.2016, p. 119.

Fischer B. (2018). Art 46 Transfers subject to appropriate safeguards. In: M. Sakowska-Baryła (ed.), General Data Protection Regulation. Commentary, Warszawa, C.H. Beck, p. 472.

Grusza M. (2020). New rules for transferring personal data from the European Union to third countries (selected issues). Legal Review, no. 2, p. 15.

Judgment of the Court in case C-362,14, 6.10.2015, ECLI: EU:C:2015:650, no. 82

Karwala D. (2018). Commercial transfers of personal data to third countries. Warsaw, p. 437.

Kuner C. (2014). Safe Harbor before the EU Court of Justice. Cambridge Journal of International and Comparative Law, 13.4.2014, Safe Harbor before the EU Court of Justice – Cambridge International Law Journal (cilj.co.uk) [access: 21.11.2021].

Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM/2010/0492, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:EN:PDF [access: 21.11.2021].

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, Article 29 Data Protection Working Party, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [access: 21.11.2021].

Rojszczak M. (2019). Protecting privacy in cyberspace, taking into account the threats posed by new information processing techniques. Warsaw, Wolters Kluwer, p. 335.

Szpor G. (2012). Administrative and legal problems associated with the expansion of the Internet. In: G. Szpor, W. Wiewiórowski (ed.). Internet. Problems of Net, Portals and e-Services. Warsaw, C.H. Beck, pp. 71–80.

The Act of 3 July 2002 – Aviation Law, OJ 2017, item 959 and 1089.

The Act of 14 May 2018 on the Processing of Passenger Name Record Data, OJ 2018, item 894.

The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 2010/C 115/01.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, done at Lisbon on 13 December 2007, OJ 2009, No. 203, item 1569.