KARAS, V. - KRÁLIK, A. Právo Európskej únie. 1. vydanie, Bratislava: C.H.Beck, 2012. ISBN 978-80-7179-287-1.

MAZÁK, J. - JÁNOŠÍKOVÁ, M. Základy práva Európskej únie. Bratislava: Wolters Kluwer, 2009. ISBN 978-80-8078-289-4.

MRÁZ, S. - POREDOŠ, F. - VRŠANSKÝ, P. Medzinárodné verejné právo, Bratislava: VO PF UK, 2003. ISBN 978-80-7160-175-6.

PROCHÁZKA, R. – ČORBA, J. Právo Európskej únie. Bratislava: Poradca podnikateľa, 2006. ISBN 978-80-8893-162-1.

SPECIALE, R. Fundamentals of Aviation Law. 1st Edition, Columbus: McGraw-Hill Education, 2006. ISBN 978-00-7145-867-2.

SYLLOVÁ, J. - PÍTROVÁ, L. - PALDUSOVÁ, H.; a kol. Lisabonská smlouva, komentář, Praha: C.H.Beck, 2010. ISBN 978-80-89406-07-4.

SVOBODA, P. Úvod do evropského práva. 4. vydání, Praha: C.H.Beck, 2011. ISBN 978-80-7400-313-4.

Periodiká a zborníky:

THIJSSEN, Ch. The Montreal Convention, EU Regulation 261/2004, and the Sturgeon Doctrine: How to Reconcile the Three?" In: 12 Issues Aviation Law & Policy, 2013.

VALEŠOVÁ, T. Vztah mezinárodního práva a vnitrostátního práva, vztah práva Evropských Společenství, Evropské Unie a vnitrostátního práva. Praha: Justiční akademie ČR, 2003.

OCHRANA OSOBNÝCH ÚDAJOV PO ROZSUDKU SCHREMS II
PERSONAL DATA PROTECTION AFTER THE SCHREMS II JUDGMENT

Daniela Galátová[1]

DOI: https://doi.org/10.24040/pros.13.11.2020.svp.77-83

Abstrakt

Článok sa venuje spracúvaniu osobných údajov mimo územia EÚ a EEAA. Prenos osobných údajov je v dobe čoraz zvyšujúcej sa digitalizácie na dennom poriadku. Právna úprava Európskej únie doposiaľ umožňovala prenos osobných údajov do Spojených štátov amerických na základe Vykonávacieho rozhodnutia Komisie (EÚ) 2016/1250 z 12. júla 2016, ktoré však bolo 21. augusta 2020 vyhlásené Súdnym dvorom EÚ za neplatné. Príspevok obsahuje jednak všeobecné informácie o prenose osobných údajov, ako aj stručný rozbor samotného rozhodnutia. V neposlednom rade sa venuje praktickým dopadom vyplývajúcich z tohto rozsudku.

Kľúčové slová

osobné údaje, GDPR, Schrems II, prenos osobných údajov, mechanizmy ochrany prenosu osobných údajov

Abstract

The Article is dedicated to processing of personal data outside the EU or EEAA territory. Transfer of personal data is done on daily basis with the more increasing digitalization. Legal framework of the European Union so far enabled the transfer of personal data to the United States of America on the basis of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, which was however declared invalid by the European Court of Justice on 12 August 2020.The paper consists of general information concerning transfers of personal data, as well as a brief analysis of the judgment itself. Last but not least, it includes information on practical implications stemming from this judgment.

Keywords

personal data, GDPR, Schrems II, transfer of personal data, mechanisms of transfer of personal data

[1] Mgr. et Mgr. Daniela Galátová, I. school-year PhD. student, department of International and European law, Faculty of law, Paneuropean university

Introduction

The importance of personal data protection raises with the fast development of technologies. We cannot anymore imagine life without social media, the flow of processed data increases and the capacity of servers provided on the EU level is not sufficient. Transfer of personal data therefore takes place outside the territory of the EU on daily basis. The protection of transfer of personal data to the USA having been put in place so far, was declared invalid by the European Court of Justice during the case C-311/18 - Facebook Ireland a Schrems (in this text as "Schrems II judgment")[2]. What legal impacts does this judgment have with regards to transfer of personal data to the USA and what implications stem from it to controllers and processors? Is it even possible to sufficiently safeguard the protection of personal data while transferred to the USA and the legal remedies connected therewith at the current US establishment?

Transfers of personal data under GDRP

Let´s imagine a situation when an account is created in order to receive some goods from a company based in Europe. That company has its branch in Latin America and servers in the USA. The server companies have a maintenance established by a company in India with employees working remotely in Africa. All of a sudden, within couple of clicks, personal data may travel all over the world.

The understanding of a fast technological development and its inevitable link to protection of personal data has been clearly understood and portrayed in the General Data Protection Regulation [3]. It is its recital 6 which explains that technology is transformed in various fields of life and the free flow of personal data with the Union and the transfer should be indeed facilitated. In addition, Article 44 of the GDPR determines that a transfers of personal data to third countries is possible under the conditions of being in compliance with the GDPR

[2] Judgment of the Court (Grand Chamber) of 16 July 2020 (request for a preliminary ruling from the High Court (Ireland) — Ireland) — Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (Case C-311/18), OJ C 249, 16.7.2018.
[3] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88

rules. If these conditions are not kept, such a transfer of personal data should be prohibited. As a consequence, GDPR provides with the possibility to transfer personal data to third countries in case of a compliance with the GDPR and the guarantee to safeguard data subject´s rights.

When it comes to the protection tools with regards to transfers of personal data to third countries, Chapter V of GDPR applies. Chapter V recognizes two systems: adequacy decisions or appropriate safeguards (including specified tools, i.e. corporate binding rules, standard contractual clauses etc.). Adequacy decisions are implementing acts adopted by the European Commission after a thorough assessment of personal data protection safeguards of a specific territory, a specified sector or a third country, where the personal data is to be transferred. In contrast to Decisions on adequacy, the system of appropriate safeguards is applicable in the absence of a Decision on adequacy and it is up to the controller and processor to make sure that data subject rights are enforceable and their legal remedies are sufficiently put in place. So far, there are 12 Decisions on adequacy adopted by the European Commission. And it was not long ago that there were still 13 of them.

Schrems II case-law

In 2018, Mr. Schrems, requested from the title of a data subject to prohibit or suspend the transfer of his personal data from Facebook Ireland to Facebook Inc., because he deemed that the law and practice in the United States did not provide with a sufficient protection against access by the public authorities to the data transferred thereto. As his request was refused, he lodged a complaint at the national supervisory authority in Ireland, which brought proceedings before the High Court in order to able to pose preliminary questions to the European Court of Justice. Once the proceeding has started, the European Commission adopted Commission Implementing Decision (EU) 2016/1250 (in this text as "Privacy Shield Decision")[4]. The preliminary questions not only concerned the validity of the Privacy Shield Decision, but also the Commission Decision 2010/87[5] relating to standard contractual clauses.

[4] 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, p. 1–112

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

Ruling concerning Privacy Shield

While providing responses to preliminary questions in the Schrems II judgment, the European Court of Justice, amongst other, decided on the question whether the Privacy Shield Decision provided sufficient protection of personal data when transferred to the territory of the US. It took into consideration the explanatory assessment of the Privacy Shield as such, as well as the assessment of the High Court of Ireland and it came to the following conclusions:

- *applicability*: European Court of Justice ruled that any adequacy decision has an overall binding effect, i.e. it is binding to private entities, as well as public authorities;
- *doubts about adequate level of protection in the US*- European Court of Justice found that the US national legislation failed to ensure adequate level of protection as it deemed that no effective judicial protection was at place on national level in case of interference by legally determined authorities;
- *no sufficient competence of Ombudsperson*- European Court of Justice ruled that the Ombudsperson established under the Privacy Shield Decision could not have presented equal replacement for a tribunal, therefore judicial remedies as requested in Article 47 of the Charter of Fundamental Rights were not put in place. In addition, by assessing that the Ombudsperson is appointed by the Secretary of State and was an integral part of the EU State Department put the Ombudsperson independency in question;
- *interference with fundamental rights*- European Court of Justice was of the opinion that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights[6];
- *disproportionality*- European Court of Justice came to a conclusion that the US interference arising from the surveillance programs based on Section 702 of the Foreign Intelligence Surveillance Act of 1978 (in this text as "FISA") on Executive Order 12333 were not proportionate to the level of protection to be guaranteed. It found out that the surveillance program under the Section 702 of the FISA does actually have no limitations to guarantee that foreign intelligence would not target

[6] See paragraph 171 of Case C-311/18, OJ C 249, 16.7.2018

non-US persons. Therefore, it concluded that the protection of personal data was unsatisfactory and the essential equivalence under the EU law failed to be provided;

- *lack of actionable rights for data subject*- as stated in recitals 69 and 77 of the Privacy Shield Decision, the US government has accepted that in fact Presidential Policy Directive 28 (in this text as "PPD-28") does not grant data subjects actionable rights before the courts against the US authorities;
- *lack of possibility for an individual to pursue legal remedies*- European Court of Justice ruled that there was a lack of redress for individuals with regards to the fundamental rights and that civil rights remedies were not a sufficient;
- *invalidity*- the Privacy Shield Decision was declared to be invalid.

Ruling concerning standard contractual clauses

With regards to the tool of standard contractual clauses, the European Court of Justice ruled that they were valid, however binding only to the entities which rely on them within their contract. Public authorities are thus excluded from this binding effect[7]. In addition, the Court declared that the mere existence of standard contractual clauses are not sufficient and additional safeguards need to be established by the controller established in the European Union, mutually with the recipient and any processor. Such additional safeguards are necessary in order to ensure the processing of personal data in line with the applicable personal data protection law.

Practical implications

On 10 November 2020, the European Data Protection Board (in the text as "EDPB") adopted Recommendations on measures concerning transfer tools[8]. Apart from some specific examples on additional safeguards, the text itself includes a 5-step roadmap to be applied before a transfer of personal data is to take place. Interestingly enough, the text of the Recommendation

[7] See paragraph 132 of Case C-311/18, OJ C 249, 16.7.2018
[8] Recommendation 1/2002 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

does not really use the terminology of controller and processor, but rather "exporter-importer". Like that, any potential confusion of accountability stemming from a more complicated establishment of a controller-processor relationship, have been avoided.

The 5-step roadmap includes the following parts:

1. Know your transfers- any potential transfer should be well known to the exporter before the processing takes place.
2. Identify the transfer tools you are relying on – assessment of personal data protection transfer should be done.
3. Assess whether the Article 46 GDPR transfer tool you are relying on is effective- in collaboration with importer, it is necessary to define all actors involved in the transfer and the characteristics of the transfer, as well as information whether the law and practice of the third country, where the personal data is to be transferred, may impinge the effectiveness of the transfer tools determined in Article 46 of GDPR.
4. Adopt supplementary measures- supplementary measures need to be identified on the case-by-case basis and can be of either contractual, organizational or technical character. As examples of supplementary measures, the EDPB mentions stronger encryption, pseudonymisation, split or multiply the processing, etc..
5. Procedural steps once effective supplementary measures identified- establish the processing on the basis of the results set up in points 1 to 4 above.

Last but not least, the EDPB concluded that when it comes to transfer of personal data to clouds or in case of remote access to data for business purposes (i.e. typically if a controller/processor established in the territory of the EU transferring personal data to a controller/processor in a third country of the same group of enterprises, undertakings etc.), there exist no effective technical measures to prevent from infringing data subject rights. The last two scenarios might change in the future upon an eventual technological progress.

Conclusion

The judgment left many societies in a delicate situation. Coping with additional safeguards for the already existing transfers to the US definitely represents constraints that are difficult to overcome. In addition, the COVID-19 pandemics exposed us all to more usage of digital platforms which are for the most cases US based. While one may still question whether the outcomes of the judgment do not really base grounds that under the current US regime concerning the legal framework on surveillance, effective legal remedies stemming from personal data breach cannot be established, it can be only hoped that further instructions will arrive from competent authorities. In addition to these, the phenomenally fast technological development could be used in favor of establishing more safeguards.

No matter what would be the following steps, one is sure…this judgment is a breaking point in the area of personal data protection leading to more awareness of the personal data protection and definitely contributed in further shaping of relatively new legal framework.

BIBLIOGRAPHY

EUROPEAN DATA PROTECTION BOARD: Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

EUROPEAN DATA PROTECTION SUPERVISOR: Strategy for EU institutions to comply with the "Schrems II" Ruling, available at: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2020-11_strategy_shremsii_judgement_en.pdf.

FENNESSY, C.: The "Schrems II" decision: EU-US data transfers in question, available at: https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

KUNER, Ch- BYGRAVE, Lee A.- DOCKSEY Ch.- DRECHSLER L.: The EU General Data Protection Regulation (GDPR), a commentary: Oxford University Press 2020. ISBN 978-80-1988-264-91.

PUBLICATION OFFICE OF THE EUROPEAN UNION: Handbook on European data protection law, Luxembourg, 2018 edition, ISBN: 978-92-9491-903-8.