„Krytyka Prawa", tom 9, nr 4/2017, s. 78–93, ISSN 2080-1084, e-ISSN 2450-7938, Copyright by Akademia Leona Koźmińskiego

RASTISLAV FUNTA[1]

A criticism of the "Safe Harbor" and the alternative data transfer methods[2]

Abstract

The transfer of personal data is a necessary and integral part of transatlantic trade relations between the European Union (EU) and the United States of America (USA) since the increase of large (big) data flow from the EU to the USA. This especially applies to social networks, as well as to providers and users of online services, including cloud computing services and online shops. The Safe Harbor annulmentand and the adoption of the General Data Protection Regulation (GDPR) create an opportunity to review the privacy protection within the EU and the US. The present article provides an overview of the legal and uncomfortable situation for businesses and data processors, and examines whether the alternative solutions may offer an escape from the current situation.

Keywords: CJEU, EU, Personal Data, Data Privacy, USA

[1] Dr Rastislav Funta PH.D., LL.M. – Assistant Professor, Danubius University Faculty of Law; e-mail: rastislav.funta@gmail.com; ORCID: 0000-0002-5624-814X.

[2] This article is part of the EU project of the Danubius University through which we support research activities in Slovakia [ITMS 26210120047].

„Krytyka Prawa", tom 9, nr 4/2017, s. 78–93, ISSN 2080-1084, e-ISSN 2450-7938, Copyright by Akademia Leona Koźmińskiego

RASTISLAV FUNTA

Krytyka „bezpiecznej przystani" oraz alternatywne metody przesyłania danych

Streszczenie

Wzrastający transfer danych osobowych z Unii Europejskiej (UE) do Stanów Zjednoczonych (USA) jest konieczną i integralną częścią transatlantyckich stosunków handlowych między nimi. Dotyczy to w szczególności portali społecznościowych oraz dostawców i użytkowników usług online, w tym usług przetwarzania w chmurze i sklepów internetowych. Unieważnienie tzw. bezpiecznej przystani oraz przyjęcie ogólnego rozporządzenia o ochronie danych (RODO) stwarzają okazję do oceny ochrony prywatności w UE i USA. W niniejszym artykule przedstawiono sytuację prawną, niewygodną dla biznesu i przetwarzających dane oraz zbadano, czy istnieją alternatywne rozwiązania, które mogłyby pomóc w obecnej sytuacji.

Słowa kluczowe: Trybunał Sprawiedliwości UE, UE, dane osobowe, prywatność danych, USA

 DOI: 10.7206/kp.2080-1084.166

Introduction

The transfer of personal data is a necessary and integral part of transatlantic trade relations between the European Union and the United States of America. It is due to the large amounts of data flow from the EU to the USA. This especially applies to social networks (e.g. Facebook), as well as to providers and users of numerous online services, including cloud computing services and online shops. Digital business models are essentially based on a worldwide exchange of personal data via Internet. In addition, subsidiaries of US companies in Europe or US subsidiaries of European companies frequently process personal data of their employees or customers in the USA. Many companies have handled such data on the basis of the so-called "safe harbor" system. In the "Schrems judgment"[3] of 6 October 2015, the Court of Justice of the EU (CJEU) annulled the decision of the European Commission (Commission) in regards to the "Safe Harbor" system. This means that the so called Safe Harbor is no longer a legal basis for the legal transfer of personal data from EU to US for the purposes of storage or other processing. This has created a dilemma for many companies. In particular, there are uncertainties as to whether and which alternative legal basis can be used for transfer of personal data to companies based in the USA. In order to replace the Safe Harbour, the Commission has agreed with the USA on a transatlantic "EU–US Privacy Shield". But this has become a challenge. An action for annulment[4] has been brought by Digital Rights Ireland, the privacy advocacy organization, before the General Court of the European Union (GCEU). Undoubtedly, political representatives in the EU and the US will achieve a compromise, which will replace Safe Harbor and the EU–US Privacy Shield. The current situation creates uncertainty in the transfer of personal data from the EU to the US and jeopardizes the extremely valuable transatlantic digital business relations. Many companies thus use the hybrid approach and accept combinations of various personal data transfer solutions, such as Binding Corporate Rules (BCRs). The present article provides an overview of the legal situation for businesses and data processors, and examines the alternative solutions that may be offered as a way out of this situation. The Commission's decision on the

[3] C-362/14, Maximillian Schrems vs Data Protection Commissioner.

[4] T-670/16, Digital Rights Ireland vs Commission.

legalization of the transatlantic data transfer and thus the creation of legal certainty is also being examined.

EU Data Protection Directive vs. the EU Data Protection Regulation and the key changes

The current data protection law, which is still valid in the EU, has been harmonized – in addition to other sector-specific regulations – by the Directive 95/46/EC (DPD)[5]. However, the divergent implementation of the DPD in the EU Member States has led to a fragmentation of the law within the EU. In 2012, the Commission launched a data protection package to create a new base for the digital economy, while taking into account the fundamental right of EU citizens to data protection. At the center of this package is the new general data protection regulation (GDPR). The GDPR will enter into force in the first half of 2018[6] and will then replace the DPD[7].

A transnational transfer of personal data is necessary for the development of international trade[8]. The problem is that there are often no identical or comparable data protection rules in third countries. In order to prevent a circumvention of the high level of protection within the EU and not to deny the rights of the individual concerned, personal data may only be transferred to a third country in accordance with Article 25 (1) DPD if this provides an "appropriate level of protection", as well as protection of privacy[9] and the freedoms and fundamental rights of individuals. Accordingly, Article 40 GDPR established the general principle that the transfer of personal data to third countries or international organizations must comply with the provisions on international data transfers. The Commission can determine whether a third country or an international organization offers an appropriate level of data protection by means of a so-called "adequacy decision" pursuant to Article 41 (3) GDPR (Article 25 (6) DPD). The GDPR regulates in detail a bulk of non-exhaustive check points which the Commission must take into account when assessing the adequacy of the level of protection. If a positive decision is provided,

---

5 D. Ježová, *Ochrana osobných údajov na internete a porušovanie práv s tým spojených*, "Bratislavské právnické forum" 2016, p. 49.

6 M. Rotenberg, J. Scott, J. Horwitz, *Privacy in the modern age: The search for solutions*, New York 2015, p. 55 and follows.

7 R. Funta, L. Golovko, F. Jurš, *Európa a európske právo*, Bratislava 2016, p. 473–474.

8 R. Funta, *EU–USA Privacy Protection Legislation and the Swift Bank Data Transfer Regulation: A Short Look*, "Masaryk University Journal of Law and Technology" 2011, p. 28.

9 R. Funta, *Ochrana súkromia v rámci prenosu osobných údajov medzi EÚ a USA*, "Justičná revue" 2017, p. 1–14.

 DOI: 10.7206/kp.2080-1084.166

this is binding for the EU Member States. The transfer of personal data to this country is then permitted in accordance with Article 41 (1) DPD "without adequacy decision". However, with regard to the United States, the Commission had taken an adequacy decision based on Article 25 (6) of the DPD, which was known as the Safe Harbor decision.

The GDPR will introduce many changes including transparency and consent. It means that, where consent is requested by means of a written declaration by a data subject, the request for consent has to be presented in an intelligible and easily accessible form, clear and plain language; and be clearly distinguished. While the DPD allows reliance on implicit consent of the data subject, the GDPR requires *a statement or clear affirmative action* from the data subject for the consent in order be valid. Because transparency remains a key principle under the GDPR, the GDPR is more explicit (in comparison to DPD) and provides for an extensive list of topics on which data subjects must be informed, e.g.contact details of the controller and its data protection officer, the purposes of and the legal basis for the processing;, the recipients of the data, ecc.

The GDPR has expanded the definitions of personal data and sensitive data. While the definition of personal data and sensitive personal data remained mostly unchanged under the GDPR, for some organisations, the explicit inclusion of location data or genetic data may result in additional obligations. Similar obligation may be imposed on organisations that process genetic or biometric data, which are expressly categorised as sensitive personal data, resulting in additional protections.

Pseudonymisation of data can allow organisations to satisfy their obligations in order to justify processing that would otherwise be seen as incompatible with the purposes for which the data were collected. The GDPR include a direct reference to the accountability principle in Article 5 (2) and require under Article 24 the implementation by controllers of appropriate technical and organisational measures to ensure and also demonstrate compliance (e.g. appropriate data protection policies, security risk management, data breach notifications, data protection impact assessments) with law appropriate policies.

The EU–USA "Safe Harbour"

Instead of a comprehensive adequacy decisions for the third country USA as a whole, the Commission recognized in the "Safe Harbor" decision[10] a system of

[10] 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

self-certification and self-evaluation of American data receivers, and adopted a adequacy decisions limited to the level of data protection by such certified companies. The Federal Trade Commission (FTC)[11] oversaw compliance with the Safe Harbor rules by companies in the US. The "Safe Harbor" system was used by numerous small and large companies as a legal basis for the transfer of personal data to the USA. "Safe Harbor", however, has repeatedly been criticized by the data protection authorities. Huge doubts about the "personal data security" finally aroused in regards to the global surveillance of digital communications by the US National Security Agency (NSA). The CJEU has pursued the opportunity to declare the Commission's "safe harbor" decision invalid in the "Schrems judgment". The decision of 6 October 2015, which had a major impact on the transatlantic economy, was the result of a complaint from the Austrian national Maximilian Schrems, a user of the social network "Facebook". Schrems opposed the practice of Facebook to transfer the personal data of the EU-resident Facebook user via the Dublin-based European Facebook to the US-based server of the US parent company Facebook Inc. He believed that his personal data flows in the US was surveilled for commercial purposes by the US intelligence agencies, especially the NSA, following the revelations of Edward Snowden. For this reason, he lodged a complaint with the Irish Data Protection Officer (Commissioner) and asked to inform Facebook Ireland Ltd. to prohibit the transfer of his personal data to the USA. The Commissioner dismissed the appeal as unfounded. On the one hand, there is no evidence that the NSA had access to Mr Schrems' data. Secondly, the Commission stated in the Safe Harbor decision that the US has ensured an appropriate level of protection of the personal data. He therefore was bound by this decision and prevented from carrying out his own investigations. On the other hand, Mr. Schrems brought an action before the Irish High Court. The court found that the massive and undifferentiated access of US security authorities to personal data was disproportionate and was contrary to the values protected by the Irish Constitution. However, the legality of the Commissioner's decision has also be assessed on the basis of the EU law. The Irish High Court therefore stayed the proceedings and referred to the CJEU two questions for a preliminary ruling. The core issue was how a national data protection authority, such as the Commissioner, should behave when a complaint is made that there is no adequate level of data protection in a third country such as in the USA. Is it bound by the implicit determination of an appropriate level of protection by the Commission in the Safe Harbor decision? Or has it, as

privacy principles and related frequently asked questions issued by the US Department of Commerce.

11 Ch. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge 2016, p. 96.

 DOI: 10.7206/kp.2080-1084.166

an independent national data protection authority, independently assess whether the transfer of personal data to the USA is in line with Articles 7 and 8 of the Charter of Fundamental Rights of the EU?[12] The CJEU largely followed the Opinion of the Advocate General Yves Bot. In order to answer the question referred, he first took a position on the powers of the national supervisory authorities. Subsequently, the Court considered the validity of the Safe Harbor decision. The Advocate General[13] particularly complained about the following essential shortcomings of the "Safe Harbor" system:

(a) the inadequate assessment and determination by the European Commission of an appropriate level of protection,
(b) the lack of effective monitoring and control mechanisms,
(c) the lack of limitation of the fundamental rights,
(d) the absence of effective judicial protection against such interventions and
(e) the illegal interference of the powers of national data protection authorities.

The CJEU first replied to the questions referred. It made it clear that the existence of a decision on adequacy of the European Commission, such as the "Safe Harbor", would not affect the control powers of the national data protection authorities that result from the DPD as well as from Article 16[14] (2) TFEU and Article 8[15] (3) of the Charter of Fundamental Rights of the EU. The task of the national supervisory authorities is to monitor the law of the Union on the protection of natural persons in the processing of personal data. The CJEU criticized the fact that the European Commission had not found in the "Safe Harbor" decision that the United States actually provides an appropriate level of protection. Instead, Article 1 of the Safe Harbor decision is limited to the assumption that Safe Harbor principles provide an appropriate level of protection within the meaning of the Directive. In the view of the CJEU it is therefore contrary to Article 25 (6) of the DPD in the light of the requirements of the Charter of Fundamental Rights of the EU. Article 1 is therefore invalid without a substantive examination of the "Safe Harbor" principles. It is true that a third country should ensure an appropriate level of protection according to the wording of Article 25 (6) of the DPD "on the basis of its national legislation

12 K.D. Borchardt, *Die Rechtlichen Grundlagen der Europäischen Union*, Heidelberg 2010, p. 110; L. Klimek, *Trestnoprávne záruky Charty základných práv Európskej únie: krok vpred alebo „nový obal" Dohovoru o ochrane ľudských práv a základných slobôd?*, [in:] V. Marková (ed.), *Aktuálne otázky trestného práva v teórii a praxi*, Bratislava 2015, pp. 339–349.

13 Opinion of Advocate General Bot delivered on 23 September 2015, Case C-362/14, Maximillian Schrems vs Data Protection Commissioner.

14 R. Funta, L. Golovko, F. Juriš, op. cit., p. 142.

15 R. Funta, *EU–USA Privacy Protection Legislation...*, 2011, p. 25.

or international obligations". However, as the CJEU expressly stated, the recourse of a third country to a system of self-certification as such does not contravene this requirement. According to the CJEU, a reliable self-certification system can play a role in assessing the appropriate level of protection. However, the observations suggest that the CJEU did not consider the existing supervisory and control mechanisms of the "Safe Harbor" system sufficient. He also criticized the fact that the "Safe Harbor" principles applied only to self-certified US organizations but were not met by American authorities. Furthermore, the CJEU criticized the Safe Harbor decision that allowed far-reaching fundamental rights interventions, in particular into the fundamental right to the private life of individuals as defined in Article 7 of the Charter of Fundamental Rights of the EU, as well as the fundamental right to protection of personal data guaranteed by Article 8[16] of the Charter of Fundamental Rights of the EU. According to the settled case-law of the CJEU, a European Union legislation regime which includes an intervention in the fundamental rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU must provide clear and precise rules on its scope and application and establish minimum eligibility criteria. This European Union legislation regime only then provides to those concerned sufficient guarantees if it ensures effective protection of their data against misuse and the risk of unauthorized access. This risk is very significant in case of automatic processing of personal data. The European Commission, in the "Safe Harbor" decision did not provide any finding that an effective judicial protection against fundamental rights infringements existed. The supervisory tools provided in the form of private arbitration and procedures before the Federal Trade Commission (FTC) served only to compliance with "Safe Harbor" principles by the US companies, but did not provide any legal remedy for violations of fundamental rights by government measures. Finally, the CJEU also declared invalid Article 3 of the Safe Harbor decision. This increases the threshold for interventions by the national supervisory authorities, such as the suspension of data transfers. It thus deprives the national supervisory authorities from the powers which they are actually entitled under Article 28 of the DPD in the light of the fundamental right to the protection of personal data pursuant to Article 8 of the Charter of Fundamental Rights of the EU. The exercise of the power of Article 25 (6) of the DPD does not authorize the European Commission to limit the powers of national supervisory authorities. The European Commission has in this regard exceeded its jurisdiction. Finally, the CJEU declared the entire "Safe Harbor" decision to be invalid.

16 P. Svoboda, *Úvod do Evropského práva*, Praha 2010, p. 278.

 DOI: 10.7206/kp.2080-1084.166

Alternative conditions for data transfers to the USA

According to the DPD, as well as in the future under the GDPR, personal data may be also transferred to a third country without an adequate level of data protection if sufficient guarantees are provided. Such guarantees may arise, in particular, from contractual agreements between the data exporter and data importer or from binding corporate rules. In addition, transatlantic data transfers may also be justified under exceptional circumstances by means of an exemption. Contractual agreements between the EU data exporter and the US data importer, which compensate for the lack of data protection level, can be negotiated individually and then approved by the national data protection authorities (NDPA) on a case-by-case basis. In order to simplify the contractual agreements between the data exporter and the data importer, the European Commission may issue, in accordance with Article 26 (2), (4) DPD, and Article 42 (1) (2) (c) GDPR so-called standard data protection clauses (SDPC). The European Commission has recognized three versions of SDPC which regulate the data protection obligations of EU data exporters and data importers in the third country as well as the rights of those concerned. According to this, companies can choose between "standard contract I" and "standard contract II". Pursuant to Article 1 of the respective Commission Decisions, the SDPCs shall be deemed to be sufficient guarantee in accordance with Article 26 (2) DPD. SDPCs must be adopted unchanged and integrated into a contract between EU data exporter and US data importer. This solution is therefore relatively easy to implement. International data transfers on the basis of such SDPCs do not require further authorization from the NDPAs. The disadvantage of the SDPC is, however, that a separate contract has to be concluded between each EU data exporter and each (US) data importer.

The European Commission decisions on the standard contract clauses are still valid. The CJEU has declared invalid in the "Schrems judgment" the "Safe Harbor" decision. In addition to the SDPCs, it is also possible for multinational corporations to introduce binding intra-company data protection rules (BCRs). BCRs are intra-company data protection rules for international data transfers. More specifically, these are self-imposed intra-company guidelines for dealing with personal data in international data transfers, which are legally binding for all members of a particular group of companies and must be followed by all employees. The company must first submit a draft of its BCR to the lead national data protection authority. The NDPA must examine the draft and agree with the authorities of all EU Member States, from whose territory companies wish to transfer data to third countries. Furthermore, an international data transfer pursuant to Article 26 DPD, Article 49 GDPR may be justified and thus be permitted without further authorization if the

conditions of one of the exceptions – which are to be interpreted strictly – are present. In such cases, the requirement of an appropriate level of protection may, in exceptional circumstances, be practically deviated. According to Article 26 1 (a) DPD, in the future Article 49 1 (a) GDPR, personal data may be transferred to a third country if and to the extent the data subject has given the consent. While the DPD requires a consent with no doubt, the GDPR requires an "explicit" or "unambiguous" consent for the data transfer. Pursuant to Article 2 (h) DPD a consent must be given without compulsion for the specific case. The prerequisite for effective consent means that the data subject has previously been adequately informed about the threat to his personal data when transferred to a state without adequate level of data protection. Article 7 GDPR regulates the conditions for an effective consent in more details. In addition, the transfer pursuant to Article 26 (b) and (c) of the DPD, and Article 49 1 (b) and (c) of the GDPR is admited in certain cases where the data transfer is necessary for the initiation or performance of a contract between the responsible body and the data subject or between the responsible body and a third party in the interests of the data subject. According to this, for example, data transfers can be justified to book a flight or hotel room in the USA or to carry out the transfers.

The applicability of the alternative transfer instruments according to the "Schrems Judgment" of the CJEU

Since the abandonment of the "Safe Harbor" companies have been recommended to conclude contracts on the basis of SDPCs or BCRs. Against the background of the practices of the American intelligence services and the statements of the CJEU, the protection of these instruments is, however, particularly questioned by national data protection authorities. The views on the admissibility of existing alternative data transfer instruments are widely divergent. The only consensus is that data transfers based solely on "Safe Harbor" are unlawful and are to be prohibited and sanctioned in the future. In view of the high requirements laid down by the CJEU in its judgment, a lasting solution could only be based on a substantial change in the US law, which would not be expected in the foreseeable future. The Article 29 Data Protection Working Party (which will be replaced from 2018 by the European Data Protection Board (EDPB)) also stated in its opinion from 2015 that the existing means of data transfers are "not a solution" in the case of massive and arbitrary surveillance. On 6 November 2015, the European Commission published a Communication to the European Parliament and the Council on the transfer of personal data from the EU to the USA under the "Schrems" judgment of the CJEU. It states

 DOI: 10.7206/kp.2080-1084.166

that alternative transfer instruments may be used further. In the aftermath of the CJEU "Schrems Judgment", the Article 29 Working Party clarified the meaning of 'essentially equivalent' wording where the key objective is to make sure that an essentially equivalent level of protection granted to individuals[17] is maintained when personal data is processed. The Article 29 Working Party also called the Member States and the EU institutions to find a solution to overcome the situation of uncertainty. Nonetheless, it is largely questioned that the European Commission decision on the SDPC can continue to exist in the context of the CJEU judgment. The reasoning of the CJEU is in large parts linked to the SDPC. The European Commission has not made any determination in the decisions concerning the SDPC as to whether the compulsory national legislation in the third country is appropriate for the protection of important interests which, according to the decisions, prevail over the principles of standard contracts. Whether the SDPC and BCR can continue to be used in the long term depends on whether the deficiencies mentioned by the CJEU also apply to these instruments. It is questionable whether the European Commission decision on the SDPC, as well as Article 3 of the "Safe Harbor" decision, would restrict the powers of the independent national data protection authorities. Article 4 (1) of the SDPC decision authorizes the Member State control authorities to prohibit the transfer of data to third countries in certain circumstances for the protection of individuals with regard to the processing of their personal data. This is possible, for example, if it is established that the data importer is obliged under his domestic law to deviate from the agreed data protection to a degree which goes beyond the necessary restrictions on data protection laid down in Article 13 of the DPD. It is unclear what options have the national supervisory authorities in regards to such transfers, which are based on SDPC or BCR. The national data protection authorities are not likely to take any countervailing measures on these decisions. But what would be a counter-measure? In this respect, the CJEU states that the national supervisory authorities are not empowered to determine the invalidity of such decisions. In the light of the above, the CJEU pointed out that the national authorities are not entitled to adopt a measure which makes it compulsory to establish that the third country does not provide an appropriate level of protection. Another alternative way is the concept of consent. As stated above, consent may be justified under the condition of Article 26 1 (a) DPD, Article 49 1 (a) GDPR in case of a transatlantic transfer of personal data. According to the European Commission and the Article 29 Data Protection Working Party, consent can only be obtained in cases where the data exporter has direct contact with the data subject, the necessary information can be easily provided and an unambiguous consent can be obtained.

[17] O. Lynskey, *The foundation of EU data protection law*, Oxford 2016, p. 177 and follows.

Prior to the transfer, the data subject has to be informed of the fact that, for what purposes and under what conditions his data are transferred to a third country in which there is no adequate level of data protection. Moreover, consent could be revoked at any time. After the invalidation of "Safe Harbor", no similar legal transfer of personal data to the USA is currently possible, except in the strictly defined exceptional cases of Article 26 DPD (Article 49 GDPR). Companies that are able to structure their data transfers on existing contracts with SDPC or BCR may in principle assume that the national supervisory authorities will continue to accept these transfer instruments as an interim solution. Cross-Border data transfers to a recipient in a third country may take place if the third country receives an Adequacy Decision from the European Commission. There are several factors that may affect an Adequacy Decision, e.g. the rule of law and protections for human rights and fundamental freedoms; existence of an effective functioning of DPAs; and international commitments to the protection of personal data. The current list of Adequate Jurisdictions is: Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay. Half of the current adequacy decisions (6) apply to territories in Europe. But obtaining a finding of legal adequacy basically requires the applicant territory to demonstrate that its domestic law adheres very closely to EU data protection principles. As stated in the GDPR the Cross-Border data transfer may take place on the basis of approved Codes of Conduct. Monitoring of compliance with Codes of Conduct will be carried out by the competent supervisory authority. The Code of Conduct will require a DPA approval.

Possible ways out of the dilemma

Companies could prevent legally uncertain transfers of personal data to the US by processing data from EU citizens exclusively on servers within the EU. Several American companies such as Amazon or Facebook have started to relocate their servers to Europe or open computer centers in Europe after the "Schrems judgment". The move of data processing to servers within the EU is probably the safest and most reliable solution, both at present and in the long term. The problem here is that moving the data to servers within the EU or even the construction of such a server takes time and is not considered for all companies due to the costs. Data on servers within the EU are, however, not fully protected from access by the USA. For example, US companies may be required to disclose personal data, even if stored by their subsidiaries and on servers within the EU, according to US law. The question has not yet been clarified in the USA.

 DOI: 10.7206/kp.2080-1084.166

In 2016 the European Commission has presented the "EU–US Privacy Shield" as a new framework for transatlantic data transfer. The materiality of EU–US Privacy Shield presupposes that the European Commission assessment of the level of protection in the USA appears to be justified as "adequate" by an overall consideration of the relevant circumstances. Furthermore, according to the CJEU, it is indispensable that the US restrict the access to data of EU citizens to what is "absolutely necessary". Access and processing by US authorities may only be done in a manner which is compatible with the objectives of its transfer and does not go beyond what is "absolutely necessary and proportionate" to protect national security. With the help of objective criteria, the access of the authorities to the data and its subsequent use must be restricted to very specific, strictly limited purposes which can justify such interventions. The EU–US Privacy Shield is neither an international agreement, nor is it expected that its contents are incorporated into the US in the form of a law. In view of the fact that all transatlantic data flows based on the EU–US Privacy Shield would have to be stopped without any substitute, a suspension will continue to be politically delicate and posing an immense problem to the companies involved. The use of SDPC, BCR and other legal instruments is, however, also problematic in view of the deficits shown in US law. The formal deficits are identical. The European Commission also failed to establish in the decisions relating to the SDPC whether the compulsory national legislation in the third country is appropriate for the protection of important interests which, according to the decisions, have a lump priority over the principles laid down in the standard contracts. In addition, personal data submitted by SDPC and BCR by EU citizens are also subject to (disproportionate) access by US authorities. The legal uncertainty for companies has also increased by the fact that the CJEU had been asked for its opinion about the validity of the EU–US Privacy Shield. The Article 29 Working Party provided strong concerns about the EU–US Privacy Shield and recommended a number of changes. The final version of the EU–US Privacy Shield addressed some, but not all, of the Article 29 Working Party concerns. The Article 29 Working Party welcomed significant improvements (e.g. the establishment of an Ombudsperson as a new redress mechanism) brought by the EU–US Privacy Shield compared to the Safe Harbour decision. However, the Article 29[18] Working Party had strong concerns (e.g. the application of the purpose limitation principle to the data processing is unclear or the data retention principle is not expressly mentioned in it) on both the commercial aspects and the access by public authorities to data transferred under the EU–US Privacy Shield. Subsequently, the Digital Rights

[18] Statement of the Article 29 Working Party on the Opinion on the EU–US Privacy Shield, Brussels, 13 April 2016.

Ireland[19] has filed the challenge with the General Court of the EU. In the claim it has been requested to invalidate the European Commission Adequacy Decision. This has approved and adopted EU–US Privacy Shield. In 2017 the Irish office of the Data Protection Commissioner asked the Irish High Court to make a preliminary reference to the CJEU in regards to the validity of the "standard contractual clauses" mechanism. Global businesses should follow the developments in this area, since the EU–US Privacy Shield is likely to be challenged before the CJEU, and other data transfer mechanisms are also under under proof. I would therefore urge in particular:

- additional checks, e.g. in the form of regular, unannounced inspections;
- dissuasive sanctions for US companies in accordance with the new GDPR;
- definition of the terms 'necessity and proportionality', etc.

It is questionable whether the European Commission's assessment of the US level of data protection is justified as "adequate" (i.e. substantially equivalent to the protection afforded by the EU's data protection principles[20] as well as to EU fundamental rights). In particular, the European Commission should have to examine all relevant circumstances. Pursuant to Article 25 (1) of the DPD, the European Commission must take into account, in assessing the adequacy of the level of protection, all circumstances which play a role in data transfer, in particular the nature of the data, the purpose and the duration of the intended processing, the country of origin as well as the regulations and security measures applicable in the USA.

In the US, the government authority may to a considerable degree obtain and process personal data (e.g. through the US Patriot Act, Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, Presidential Policy Directive 28, USA Freedom Act)[21]. The situation in the USA, and in particular the protection level offered by US law, can not be comprehensively examined at this point. Some points, like the inadequate limitation of US authorities' access powers under US law, have already been addressed.

19 T-670/16, Digital Rights Ireland vs European Commission.

20 P. Carey, *Data protection*, Oxford 2004, p. 51–64.

21 In regards to history of US Informational Privacy look at: C. Bowman, A. Gesher, J.K. Grant, D. Slate, E. Lerner, *The architecture of privacy*, Sebastopol 2015, p. 5–8.

 DOI: 10.7206/kp.2080-1084.166

Concluding remarks

Even without a thorough examination of the EU–US Privacy Shield and without a substantive examination of the privacy principles[22], the partial reforms in the US still have deficits. Despite numerous improvements there is stil evidence that the level of data protection in the US is not equivalent and therefore should not be considered appropriate. Since the EU "has and probably will have the most advanced data protection law in the world"[23] it is the task of the EU data protection authorities to provide feedback on the shortcomings of the EU–US Privacy Shield. As long as companies do not rely on a long term legally safe solution for future data transfers to the US, it is expected that the current trend to store data in the EU is continuing. But this may put pressure on the US economy. It is also clear that many of the problems that also affect the possibility to recourse on alternative legal bases, such as BCR or SDPC, are still not solved. As already stated, BCR which are comprehensively regulated in Art. 43 of the GDPR, as well as SDPC under the GDPR, can offer sufficient guarantees that can help overcome the lack of adequate protection levels in a third country such as the USA. However, the explicit prerequisite is now that the persons concerned have enforceable rights and effective legal protection options. SDPCs may be adopted by the European Commission (Article 42 (2) (c) of the GDPR). The same effect will, in the future, also be imposed by SDPCs which have been approved by a supervisory authority and approved by the European Commission (Article 42 (2) (d) GDPR). In the future, so-called approved codes of conduct are to contribute to compliance with the GDPR in accordance with Article 38 of the GDPR and provide adequate guarantees. However, some of the new instruments such as the certification or the codes of conduct are part of general principles in the GDPR. Therefore, the use of these instruments is likely to be expected at the earliest in 2018.

References

Borchardt K.D., *Die Rechtlichen Grundlagen der Europäischen Union*, 4. ed., Heidelberg 2010.

Bowman C., Gesher A., Grant J.K., Slate D., Lerner E., *The architecture of privacy*, Sebastopol 2015.

Carey P., *Data protection*, Oxford 2004.

22 B. Schneier, *Data and Goliath*, New York 2015, p. 125 and follows.

23 D.J. Svantesson, *The (Uncertain) Future of Online Data Privacy*, "Masaryk University Journal of Law and Technology" 2015, p. 130.

Funta R., *EU–USA Privacy Protection Legislation and the Swift Bank Data Transfer Regulation: A Short Look*, "Masaryk University Journal of Law and Technology" 2011, 1.

Funta R., *Ochrana súkromia v rámci prenosu osobných údajov medzi EÚ a USA*, "Justičná revue" 2017, 69.

Funta R., Golovko L., Juriš F., *Európa a európske právo*, Bratislava 2016.

Hoofnagle Ch., *Federal Trade Commission Privacy Law and Policy*, Cambridge 2016.

Ježová D., *Ochrana osobných údajov na internete a porušovanie práv s tým spojených*, "Bratislavské právnické forum" 2016.

Klimek L., *Trestnoprávne záruky Charty základných práv Európskej únie: krok vpred alebo „nový obal" Dohovoru o ochrane ľudských práv a základných slobôd?*, [in:] V. Marková (ed.), *Aktuálne otázky trestného práva v teórii a praxi*, Bratislava 2015.

Lynskey O., *The foundation of EU data protection law*, Oxford 2016.

Rotenberg M., Scott J., Horwitz J., *Privacy in the modern age: The search for solutions*, New York 2015.

Schneier B., *Data and Goliath*, New York 2015.

Svantesson D.J., *The (Uncertain) Future of Online Data Privacy*, "Masaryk University Journal of Law and Technology" 2015, 2.

Svoboda P., *Úvod do Evropského práva*, 3. ed., Praha 2010.

 DOI: 10.7206/kp.2080-1084.166