Safe Harbor: The Decision of the European Court of Justice

Andreas Börding

Abstract Currently, the transfer of personal data to the USA raises several problems, since the Safe Harbor agreement between the European Commission and the US is no longer in effect. By now, companies can use the subsequent agreement called Privacy Shield. In the future, contractual arrangements are expected to become increasingly relevant. Whether this is a realistic long-term solution depends on the implementation of the ECJ's guidelines.

1 Unrestricted Data Collection[1]

The transfer of personal data has no boundaries. The internet provides the possibility to send, copy, and process large data sets within fractions of a second.

Thereby, various law systems with different requirements collide. Germany and the European Union deal critically with the handling of personal data. According to that, the principle applies that personal data may only be collected, processed and used on the basis of a legally defined framework. Moreover, the collection of this data is restricted to its purpose and necessity. As a general rule, this requires a comprehensive balancing of interests of the people and authorities involved.

This understanding originates in the Census Act of the German Federal Constitutional Court from 1983, which determined criteria for the governmental handling of personal data of citizens.[2] As a result of a permanent development of this general rule, a harmonization of the European data protection standards arose. This started with the inception of the European Data Protection Directive in 1995 and continues with the European General Data Protection Regulation, which

[1]This article deals primarily with the Safe Harbor-agreement and the decision of the ECJ due to the date of the first draft. The succeeding Privacy Shield is therefore only marginally considered.
[2]BVerfG, NJW 1984, p 419.

A. Börding (✉)
Institute for Information, Telecommunication and Media Law (ITM), University of Münster, Münster, Germany
e-mail: andreas.boerding@uni-muenster.de

T. Hoeren and B. Kolany-Raiser (eds.), *Big Data in Context*,
SpringerBriefs in Law, https://doi.org/10.1007/978-3-319-62461-7_5

provides a broad full harmonization of data protection law. In contrast to that, the United States of America has a more generous understanding of data protection. A consistent data protection concept for personal data does currently not exist.[3] On the contrary, there are only area specific rules without a central data protection authority.[4] Only a few federal states have legal provisions for dealing with personal data.[5] Moreover, most of the US-American data protection rules do not apply or only apply restrictedly to EU-citizens.[6]

The differences between the legal areas require that the export of personal data from the European area may only be declared to be permissible under a guarantee of a high level of protection.

In the end, the biggest data processing companies, such as Facebook, Google, and Amazon, have its corporate seat in the United States of America. Thereby, apart from safe basic conditions for private companies, it has to be kept in mind that public authorities in the US have far-reaching competences regarding the disclosure of stored and processed personal data and that they substantially make use of it.[7]

Even if the previous "USA Patriot Act" has been replaced by the "USA Freedom Act" in 2015 and the intelligence services are thus subject to stricter formal requirements,[8] it remains to be seen which practical approach and which data protection developments will make their entry into the US. Therefore, it is necessary that the European Union determine safe and transparent regulations on the data transfer between Europe and the US. Thereby, the EU Data Protection Directive, the Federal Data Protection Act and the single State Data Protection Acts function as a legal basis.

2 The Safe-Harbor Agreement of the European Union

In 2000, the European Commission decided that the US guarantees an adequate level of protection for transmitted personal data.[9] The foundation for this decision has been that the EU Data Protection Directive only allows transfer of data for the purpose of data processing in exceptional cases.

---

[3]Börding, CR (2016), p 434.

[4]Börding, CR (2016), p 434.

[5]Hoofnagle 2010, Country Studies—USA, p 15.

[6]Böhm, A comparison between US and EU Data Protection Legislation for Law Enforcement, 2015, p 69 et seqq.

[7]See Electronic Frontier Foundation 2015, Who Has Your Back? https://www.eff.org/who-has-your-back-government-data-requests-2015.

[8]Byers 2015, USA Freedom Act vs. USA Patriot Act, http://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469.

[9]European Commission, Decision of 26.07.2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

According to this, neither the intended purpose of the data processing, nor legal provisions, nor an inappropriate safety level in the recipient country may be contrary to the protection of privacy and the fundamental rights of the data subject. The US-Ministry of Commerce therefore arranged a legal framework to establish "Principles of safe harbors for data protection" (Principles) and summarized frequently asked questions (FAQ) dealing with the specific realization of the principles mentioned above.[10]

According to the regulations of the Ministry, organizations, which wanted to transmit personal data out of the European Union for data processing, could join these principles. Thus, an appropriate protection level between the European Union, the US and the data processing offices in the US should be guaranteed.

Pursuant to the principles, information obligations, transfer and safety regulations and rights to information for the affected people were provided.[11] Thereupon, the Commission determined that the measures would be sufficient to ensure the rights of European citizens—especially the right to informational self-determination.[12]

3 The Decision of the European Court of Justice

In the sequel, the Austrian Mr. Max Schrems submitted a complaint at the Irish Data Protection Authority against the activity of Facebook. After the disclosures of Edward Snowden, he was convinced that Facebook's transfer of his personal data into the US was unlawful. Finally, the data were not adequately protected against inspections of US public authorities.

After the Irish Data Protection Authority had disallowed his complaint by reference to the Safe Harbor agreement, Mr. Schrems filed a suit before the Irish High Court. The Irish High Court submitted the question, whether the decision of the European Commission in 2000 is opposed to a decision of the own national data protection authority, to the European Court of Justice.[13]

The European Court of Justice stated that the decision of the commission did not hinder national data protection authorities to carry out own appropriateness tests regarding the data protection level in the third country. Rather, according to the Articles 7, 8 and 47 of the EU Charter of Fundamental Rights, the right to private life, protection of personal data and the right to effective judicial protection determine that the member states had to carry out inspections by their own.

[10]European Commission, Annex I, II to the Decision 2000/520/EC of 26.07.2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

[11]European Commission, Annex I to the Decision 2000/520/EC of 26.07.2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

[12]European Commission, Art. 1 No. 1 Decision of 26.07.2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

[13]Considering the legal procedure see EuGH, Decision of 6 Oct 2015, C-362/14, MMR 2015, p 753 et seqq. with notes from Bergt.

Nevertheless, only the European Court of Justice stayed entitled to judge on the effectiveness of the legal act of the Union.

The European Court of Justice criticizes that the Commission did not determine whether the US legal system or international agreements ensure a comparable data protection level. Furthermore, the provisions of the agreement must also refer to public authorities in the US. A provision, which principally permits public authorities to examine the content of electronic communication, was incompatible with the essence of the fundamental right to private life.

Beyond, the ECJ determined that the powers of intervention of public authorities in the United States and the lacking ability to legal protection are opposed to the necessary level of protection for the transfer of personalized data. The Safe Harbor agreement would not eliminate these problems.[14]

4 Consequences of the Decision

As an immediate consequence of the decision, companies can no longer refer to the Safe Harbor agreement when they transfer data into the US. Serious doubts about the effectiveness of the following agreement—the so-called "Privacy Shield"[15]—are advisable. Especially the legal requirements of the European data protection law are not or only insufficiently respected.[16] Therefore, the following part will focus on alternative instruments.

According to the Federal Data Protection Act, the transfer of data must be avoided in particular when the data processing authority does not ensure an appropriate degree of protection. At this, especially the data protection provisions at the place of destination have to be taken into account. Admittedly, there is no requirement that the level of protection is congruent to the German or European standard.[17] However, general principles of local data protection provisions must not be disregarded.[18] Insofar, already the assumption of an appropriate level of protection in the US should be precluded by the fact that a consistent data protection concept on a federal level is lacking.

Among others, exceptions were made when the affected person consented to the transfer of data or if it is necessary to fulfill a contract or to protect public interests. As an amplification of this exception, the competent supervisory authority is still entitled to approve the data transfer, if the protection of the right to privacy and the exercise of the therewith-involved rights are guaranteed.

[14]ECJ, Decision of 6 Oct 2015, C-362/14, MMR 2015, p 753 et seqq. with notes from Bergt.

[15]Press Statement of the EU-Commission of 12 Jul 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

[16]See Börding, CR 2016, pp 438–440.

[17]Börding, CR 2016, p 433.

[18]Börding, CR 2016, p 433.

5 Practical Implementation

Based on the aforementioned exceptions, three solutions seem to be practical for the transfer of personal data into the US: the consent of the affected person, data protection safeguards, and mandatory company corporate policies.

5.1 Consent

In individual cases, the consent of the affected person might be requested. For that, the law requires a free, indubitable and concrete previous admission. Beyond, the data processing authority has to enlighten the data subject about the purpose, extent and consequences of the data transfer. It is necessary that the affected person is enlightened about the risk of a data transfer in a third country with an inappropriate level of protection.[19]

5.2 Data Protection Safeguards

An additional option is the conclusion of a transfer contract.[20] Thereby, the transmitting authority agrees with the data receiver that essential basic ideas of the European Data Protection Directive will be respected.[21] As a general rule, standard contractual clauses, adopted by the EU-Commission, are used.[22] There is an ongoing debate about whether transfer contracts require the authorization of the supervisory authority as long as they assume the unchanged standard contractual clause. Contrary to the seemingly clear legislative language, the major scientists reject this approach.[23] It remains to be seen whether the authorities will follow this approach in the future.

Beyond, some argue that the transmitting authority has to provide evidence to the supervisory, which shows that the data receiver may not be forced by the US authorities to breach the data protection guarantee. Hereafter, missing or impractical evidence was opposed to the approval for data export.[24]

[19]Gola et al. 2015, in: Gola/Schomerus, Kommentar zum BDSG, section 4c Ref. 5.
[20]Gola et al. 2015, in: Gola/Schomerus, Kommentar zum BDSG, section 4c Ref. 5.
[21]Gola et al. 2015, in: Gola/Schomerus, Kommentar zum BDSG, section 4c Ref. 10.
[22]Gola et al., in: Gola/Schomerus, Kommentar zum BDSG, section 4b Ref. 16.
[23]Deutlmoser/Filip 2015, part. 16.6., Ref. 4.
[24]Deutlmoser/Filip 2015, part. 16.6., Ref. 46.

5.3 *Binding Corporate Rules*

Finally, companies can issue so-called binding corporate rules (BCR). These binding company policies have to contain guarantees governing personal data.[25] It is essential that an appropriate protection level be ensured inside the company as well as outside.[26] Legal provisions concerning the extent of the directive are lacking. Nevertheless, the directives should orientate themselves towards the legal regulations of national and European level to guarantee legal certainty. Thereby, the aforementioned standard contract clauses can be used.[27]

6 State of Debate

After the Safe Harbor judgment of the CJEU, various voices for the further course of action were raised.

In Germany, the statement of the Independent Centre for Privacy Protection Schleswig-Holstein is remarkable. According to the position paper,[28] absolutely no transfer in the US is admissible in the future, so far as no international law agreement is concluded between the US and the EU or respectively the national states. Thereby, especially the consent of the affected person is not sufficient since the individual is unable to dispose the essential core of the fundamental right to privacy.

This solution gives rise of massive objections, because thereby one denies every autonomy and freedom of action of the data subject concerning the personal data from the outset. However, one must agree to the reservations regarding the effectiveness of data protection guarantees and the conclusion of binding company policies. The reference upon this could be hindered by the possibility that the offices in the US might be forced to disclose the data by the US authorities and thus break the contract.[29] Insofar, the legal provisions would widely miss their purpose.

Apart from that, the data protection authorities of the federal government and the states currently do not consider the transfer of data on the basis of data protection guarantees or company policies as a sustainable solution.[30] New approvals would

[25]Deutlmoser/Filip 2015, part. 16.6., Ref. 46.

[26]Deutlmoser/Filip 2015, part. 16.6., Ref. 46.

[27]Gola et al. 2015, in: Gola/Schomerus, Kommentar zum BDSG, section 4c Ref. 15.

[28]ULD, Position Paper of 14 Oct 2015, https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html.

[29]Kühling/Heberlein, NVwZ 2016, p 10; Schuster/Hunzinger, CR 2015, p 788 et seqq.; Moos/Schefzig, CR 2015, p 632; see furthermore Borges, NJW 2015, p 3620.

[30]Der Hessische Datenschutzbeauftragte 2015, Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen: Datenschutz-Richtlinie im Bereich von Justiz und Inneres, https://www.datenschutz.hessen.de/ft-europa.htm.

not be granted on these foundations. It remains to be seen, if and how to proceed with already awarded permissions. However, the permission of the affected person could be obtained in particular cases and in narrow limits.

The so-called Article 29 Working Party, which compiles statements concerning data protection on behalf of the European Commission, draws a vague conclusion.[31] After that, the problem of data transfers shall be solved primarily on a political level. Concurrently, national supervisory authorities shall still consider contractual regulations as a suitable instrument for data exports. Finally, a decisive action of the European authorities is necessary if a sustainable solution is still lacking in January 2016.

Meanwhile, the business association BITCOM published a guideline for companies. According to this, the export of personalized data shall basically be based on data protection guarantees, whereby the standard contractual clauses of the European Commission shall be used. Beyond, it is possible to make recourse to consents of affected people.[32]

7 Outlook

As shown before, there is considerable uncertainty concerning the handling with the judgment of the European Court of Justice. Because of this, the solution of all legal questions can be expected the earliest in months ahead. Especially the Privacy Shield seems to be unsuitable to remove the uncertainties.[33]

On this occasion, a common European action is certainly advisable. Finally, it is conceivable that the national supervisory authorities develop different solutions to deal with the variety of contractual agreements. Thereby, the harmonization of the data protection level in the European Union calls for determination and compliance with common standards. It is important to avoid that the question of compliance with the data protection level depends primarily on the conduct of the respective member state. At the same time, it would stand for a great progress, if the United States of America carries out a levelling of the data protection law with more possibilities for legal protection.

Regarding the General Data Protection Regulation, the need for regulation is not omitted either. According to the European Council's draft framework of 15. June 2015 (Art. 44, 45 Para. 1), the regulation will be based on the adequacy of the data protection level in the third country. Contractual agreements in accordance with Art. 46, 47, guarantees to compliance with the data protection level, as well as the

[31]Statement of the Article 29 Working Party 2015, http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf.

[32]BITKOM 2015, Das Safe-Harbor-Urteil des EuGH und die Folgen: Fragen und Antworten, p 10.

[33]Börding, CR 2016, p 432 et seqq.

obtaining of the consent of the person concerned are possible simultaneously (Art. 49 Para. 1 a).

The whole discussion shows: Anyone who wants to protect himself against data abuse should consider every data transfer carefully from the outset.

References

Article 29 Working Party (2015) Statement of the Article 29 Working Party. http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf. Accessed 4 Apr 2017

BITKOM (2015) Das Safe-Harbor-Urteil des EuGH und die Folgen: Fragen und Antworten. https://www.bitkom.org/Publikationen/2015/Leitfa-den/Das-Safe-Harbor-Urteil-des-EuGH-und-die-Folgen/151110_SafeHarbour_FAQ.pdf. Accessed 4 Apr 2017

Böhm F (2015) A comparison between US and EU Data protection legislation for law enforcement: study for the LIBE committee. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf. Accessed 4 Apr 2017

Börding A (2016) Ein neues Datenschutzschild für Europa—Warum auch das überarbeitete Privacy Shield den Vorgaben des Safe Harbor-Urteils des EuGH nicht gerecht werden kann. CR 2016 (7):431–441

Borges G (2015) Datentransfer in die USA nach Safe Harbor. NJW 2015(50):3617–3620

Byers A (2015) USA freedom act vs. USA patriot act. http://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469. Accessed 4 Apr 2017

Der Hessische Datenschutzbeauftragte (2015) Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen: Datenschutz-Richtlinie im Bereich von Justiz und Inneres. https://www.datenschutz.hessen.de/ft-europa.htm. Accessed 4 Apr 2017

Deutlmoser R, Filip A (2015). In: Hoeren et al. (ed) Handbuch multimedia-Recht. C. H. Beck, Munich, part. 16.6, Ref. 4, 46

Electronic Frontier Foundation (2015) Who has your back? Protecting your data from Government. https://www.eff.org/who-has-your-back-government-data-requests-2015#results-summary. Accessed 4 Apr 2017

European Commission (2016) Press release of 12 July 2016. http://europa.eu/rapid/press-release_IP-16-2461_en.htm. Accessed 4 Apr 2017

Gola P et al. (2015) In: Gola P, Schomerus R (eds), Kommentar zum Bundesdatenschutzgesetz, 12th edn. C. H. Beck, Munich, section 4b, Ref. 16, section 4c, Ref. 5, 10, 15

Hoofnagle C (2010) Comparative country studies, B. 1 United States of America, Brussels

Kühling J, Heberlein J (2016) EuGH "reloaded": "unsafe harbor" USA vs. "Datenfestung" EU. NVwZ 35(1):7–12

Moos F, Schefzig J. (2015) "Safe Harbor" hat Schiffbruch erlitten. CR 2015 (10):625–633

Schuster F, Hunzinger S. (2015) Zulässigkeit von Datenübertragungen in die USA nach dem Safe-Harbor-Urteil. CR 2015 (12):787–794

Unabhängiges Landeszentrum für Datenschutz (2015) Positionspapier des ULD zum Safe-Harbor-Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14. https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html. Accessed 4 Apr 2017

Author Biography

Andreas Börding Ass. iur., research associate at the Institute for Information, Telecommunication and Media Law (ITM) at the University of Münster. He holds a law degree from the University of Münster and completed his legal clerkship at the District Court of Dortmund.