Norbert Bernsdorff*

Transfer of Personal Data to Third Countries - "Safe Harbour", "EU-US Privacy Shield" and "Trans-Atlantic Data Privacy Framework"

The new „Trans-Atlantic Data Privacy Shield Framework“-Agreement is the successor of the „EU-US Privacy Shield“-Agreement. The European Commission’s adequacy decision, which was based on the latter, was declared invalid bei the Court of Justice of the European Union in July 2020 in the sensational „Schrems II“ judgement. Prior to this, the judges in Luxembourg had already criticised the adequacy decision, which was based on the predecessor agreement known as „Safe Harbour“-Agreement. The reason in both cases was the far-reaching surveillance and intervention powers of the US security authorities with regard to the personal data of citizens of the European Union. These two judgements meant that, according to the Court of Justice, the level of data protection in the USA was not equivalent to that in the European Union.

Keywords: *Data privacy, data protection, transfer to third countries, „Safe Harbour“-Agreement, „EU-US Privacy Shield“-Agreement, „Trans-Atlantic Data Privacy Shield Framework“-Agreement, Facebook, Court of Justice of the European Union, case law, General Data Protection Regulation.*

1. Introduction

Personal data may only be transferred to third countries if the level of protection guaranteed by the General Data Protection Regulation (GDPR)[1] is not "undermined". Third countries are countries in which the GDPR does not apply. As the GDPR is only binding for the member states of the European Union (EU), third countries are therefore all countries that are not members of the EU. This means that the countries of the European Economic Area, Iceland, Liechtenstein and Norway, also belong to the group of third countries as long as they have not decided to apply the GDPR. A particular transmission problem exists in relation to the United States of America (USA). These do not have a level of data protection equivalent to that in Europe.

* Doctor of Law, Professor at the Philipps University of Marburg; Retired Judge of the German Federal Court of Social Affairs; Former Data Protection Commissioner of the Lower Saxony Judiciary. The Author is a Member of the Editorial Board of the “Journal of Personal Data Protection Law“.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.

Since the "*Edward Snowden*" case and his surveillance by the US secret service, trust in American data protection has been lost. EU citizens can also be monitored in the USA, for example when they send messages via the US network Facebook (Meta).

Following the failure of the "Safe Harbour" and "EU-US Privacy Shield" data protection agreements between the European Union (EU) and the USA before the Court of Justice of the European Union, the EU and the USA have now attempted for the third time to find a compromise between the high standard of protection provided by European data protection law and the mass surveillance that continues to be politically desirable in the USA with the "Trans-Atlantic Data Privacy Shield Framework"-Agreement.

2. History and Significance

The former Data Protection Directive (95/46/EC; DPD)[2] correctly recognised the cross-border movement of personal data as a necessity for the development of international trade. The cross-border flow of data and thus also the cross-border transfer of personal data is a matter of course in a digitally networked world and not least due to the possibilities of using the Internet. However, an equal level of data protection or even just an equal concept of data protection does not exist globally.[3]

The DPD had two effects: On the one hand, it created an EU-wide framework for national data protection laws and thus harmonised the level of data protection in the EU. In doing so, it created the framework conditions for a fundamentally unhindered transfer of personal data within the EU. On the other hand, it demarcated the EU from other countries in terms of data protection law. This is because it stipulated the conditions under which data could be transferred to countries other than EU member states.

The GDPR continued this approach in Articles 44 to 50. However, the depth of its provisions goes beyond the depth of the provisions of the former DPD. The GDPR thus takes account of developments in the reality of life since 1995. The following should be pointed out: EU data protection law should not be a "brake block" for economic development.[4] Cross-border data traffic with third countries is essential for business and trade; however, it is risky for data protection.

3. The System of the General Data Protection Regulation

The transfer of personal data to third countries is regulated in Articles 44 to 50 of the GDPR. The GDPR thus creates a standardised level of data protection within the EU; at the same time, it distinguishes the EU from other countries by setting limits on the processing of personal data in third countries.

Article 44 GDPR sets out the general principles for the transfer of personal data to third countries. Articles 45 to 49 regulate various instruments for justifying the transfer of personal

[2] 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 1995 L 281, 31.

[3] See: *Wuermeling U.*, Handelshemmnis Datenschutz - Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.

[4] For more information see: *Rüpke G.*, *von Lewinski K.*, *Eckardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, Munich 2018, § 18. On the requirements of a "European internal data market" *Brink St.*, *Oetjen St.*, *Schwartmann R.*, *Voss K.*, So war die DSGVO nicht gemeint, Frankfurter Allgemeine Zeitung (FAZ) v. 17 July 2022.

data to a third country. Article 50 GDPR standardises international cooperation for the protection of personal data. The admissibility criteria in Articles 45 to 49 GDPR are not legally related to each other. According to Article 45, the adequacy of the level of data protection is recognised for a specific third country. With the mechanisms of Articles 46 and 47 GDPR, an adequate level of data protection is created for certain companies in third countries with regard to certain data processing. Individual specific transfers of personal data are permitted on the basis of Articles 48 and 49 GDPR.

The assessment of the permissibility of a transfer of personal data to a third country requires a two-stage examination.[5] Article 44 GDPR expressly clarifies that, in addition to Articles 44 et seq. GDPR, the other provisions of the GDPR must also be complied with. These are the provisions in Articles 6, 9 and 10 GDPR.[6] At the first stage, in accordance with the general prohibition with the reservation of permission anchored in Articles 6, 9 and 10 GDPR, it must be checked whether there is a legal basis for the transfer of the data to the recipient. In the second stage, it must be checked whether the requirements of Articles 44 et seq. GDPR are met. This is because only then is the transfer of personal data to the third country permitted.

This two-tier structure also results from the purpose and system of the GDPR. It creates a standardised data protection legal framework in the EU. Therefore, cross-border processing as such does not pose a risk to the data subject. The risk therefore only arises from a transfer from one data controller to another data controller. Articles 6, 9 and 10 GDPR take this risk into account.[7] A data transfer outside the area of the harmonised legal framework poses an additional risk.

Onward transfer by the recipient in the third country to another third country is also only permitted if Articles 44 et seq. GDPR and the other provisions of the GDPR are complied with.

4. The Case Law of the Court of Justice of the European Union

The transfer of personal data to the USA has already been criticised twice by the Court of Justice under data protection law. Firstly, it declared the "Safe Harbour"-Agreement negotiated by the EU and the USA invalid, and then the "EU-US Privacy Shield"-Agreement, including the respective adequacy decisions of the European Commission (EU Commission).

a. Judgement of the Court of Justice in Case C-362/14, Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd, 6 October 2015 ("Schrems I")[8]

The decision of the Court of Justice of 6 October 2015 on the EU Commission's „Safe Harbour“ Principles was of crucial importance for the transfer of personal data to third countries and in particular for data transfers to the USA. In this judgement, the Court of Justice laid down fundamental cornerstones for the former DPD. The decision had an influence on the design of Articles 44 to 50 of the later GDPR.

[5] Likewise: *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017, Part 6.
[6] *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017, 239.
[7] See *Rüpke G.*, *von Lewinski K.*, *Eckardt J. (eds.)*, Datenschutzrecht- Grundlagen und europarechtliche Umgestaltung, Munich, 2018, § 18, 266.
[8] ECLI:EU:C:2015:650.

Facts of the case: *Schrems*, an Austrian citizen, lodged a complaint with the Irish data protection supervisory authority with the aim of preventing Facebook Ireland from transferring his personal data to Facebook Inc. in the USA. At that time, all persons resident in the Union territory who wished to use Facebook had to sign a contract with Facebook Ireland, a subsidiary of Facebook Inc. based in the USA, when they registered. The personal data of Facebook users resident in the Union territory were transferred in whole or in part to Facebook Inc. servers located in the USA and processed there. The Irish data protection supervisory authority rejected the complaint as unfounded. Among other things, it stated that all issues relating to the adequacy of the protection of personal data in the USA had to be clarified in accordance with the EU Commission's adequacy decision 2000/520/EC[9] and that the Commission had found in this decision that the USA guaranteed an adequate level of protection if the requirements of this decision were met („Safe Harbour" Principles). The Irish data protection supervisory authority considered itself to be bound by the adequacy decision of the EU Commission without its own review competence. The complainant *Schrems* then took legal action. The Irish High Court made clear its concerns about the admissibility of the data transfer to the USA. It ultimately referred the question to the Court of Justice for a preliminary ruling as to whether the Irish data protection supervisory authority was bound by the finding made by the EU Commission in its decision that the USA guaranteed an adequate level of protection or whether Art. 8 of the European Charter of Fundamental Rights[10] would have authorised it to override such a finding if necessary.

The question of the legality of the EU Commission's Decision 2000/520/EC on the "Safe Harbour" Principles was not the subject of the Irish High Court's referral. Nevertheless, the Court of Justice also ruled on it. It pointed out that the complainant *Schrems* was de facto questioning this legality with his complaint. The Court of Justice thus extended the subject matter of its decision.

With regard to the question referred by the Irish High Court, the Court of Justice comes to the conclusion that the national data protection supervisory authorities are not limited in their review competence by a decision of the EU Commission under the DPD; there is an independent review competence of the national supervisory authorities. However, the authority to declare a decision of the EU Commission invalid lies solely with it; the Court of Justice has a monopoly on rejection. The national data protection supervisory authorities would therefore have to take legal action before it after exercising their review competence.

The Court of Justice considered that where a claim is lodged with national supervisory authorities, they can examine whether the transfer a person's data to a third country complies with the requirement of the EU legislation on the protection of the data, even in those cases which the EU Commission adopted decision finding a third country affords an adequate level of protection of personal data and even considered that the Court of Justice alone has jurisdiction to declare an EU act invalid.

On the merits, the Court of Justice stated word-by-word:

„In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 39).

[9] Decision 2000/520/EC of the European Commission of 26 July 2000.
[10] Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.

Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him , or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (…).“

With its ruling, the Court of Justice not only established the invalidity of the "Safe Harbour"-Agreement between the EU and the USA. With its judgement, it also laid down criteria for assessing the adequacy of the level of data protection.[11] This also had an impact on the successor agreement - the "EU-US Privacy Shield"-Agreement - which came under increased scrutiny in terms of data protection law and data protection policy.

b. Judgement of the Court of Justice in Case C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, 16 July 2020 ("Schrems II")[12]

In order to once again take into account the importance of data traffic to the USA, the "EU-US Privacy Shield"-Agreement on data exchange with the USA was implemented on 12 July 2016 as a successor agreement to the "Safe Harbour"-Agreement on the basis of the EU Commission's adequacy decision 2016/1250[13]. The content of this adequacy decision by the EU Commission was that companies that made a voluntary commitment in accordance with the „EU-US Privacy Shield“ Mechanism had an adequate level of data protection.

The "EU-US Privacy Shield" Mechanism was therefore comparable to the "Safe Harbour" Mechanism. US companies made a voluntary commitment to the US Department of Commerce to process data transferred to them from the EU only in accordance with certain "principles"; there was a voluntary commitment to maintain the level of data protection in the EU. The Federal Trade Commission and the US Department of Transportation monitored compliance with this voluntary commitment. The "EU-US Privacy Shield" Mechanism was therefore only open to companies that were subject to the supervision of these authorities. The Department of Commerce was primarily responsible for monitoring compliance with the voluntary commitment. Penalties could be imposed by the Federal Trade Commission in the event of violations. From the outset, there were considerable doubts about the effectiveness of data protection supervision by US authorities.

Facts of the case: The complainant in the "Safe Harbour" proceedings, *Schrems*, complained to the Irish data protection supervisory authority that Facebook Ireland was forwarding his data to the parent company in the USA. In further proceedings, an Irish court turned to the Court of Justice to decide whether the standard contractual clauses and the „EU-US Privacy Shield“ are compatible with the European level of data protection. The Luxembourg judges declared the „EU-US Privacy Shield“ Mechanism invalid. In view of the US authorities' access options, the data protection requirements are still not guaranteed. In

[11] Likewise *Kühling J.*, *Heberlein J.*, EuGH "reloaded": "unsafe harbour" USA vs. "Datenfestung" EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7,9.
[12] ECLI:EU:C:2020:559.
[13] Decision (EU) 2016/1250 of the European Commission of 12 July 2016.

addition, the legal protection for data subjects - the right to an effective legal remedy - is still inadequate.

A particular problem after all of this was the US authorities' authorisation to access data transferred from the EU and the question of legal remedies against this access. This was a key aspect of the Court of Justice's decision to declare the "Safe Harbour" Mechanism invalid.

The Court of Justice word-by-word formulated:

„In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52 (1) of the Charter.

Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

It follows, that Article 1 of the Privacy Shield Decision is incompatible with Article 45 (1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.“

What is the role of the EU Commission and what is the role of the national data protection supervisory authorities when data is transferred to third countries?

The EU Commission is not obliged to review the level of data protection in third countries when adopting standard contractual clauses. Rather, the Court of Justice emphasises the responsibility of the data exporter to check the level of protection in the third country for each data transfer and to provide suitable guarantees for the protection of the data transferred to a third country. It may be necessary to provide additional safeguards over and above the standard contractual clauses by means of additional measures.

The data exporter is obliged to suspend or terminate the data transfer if the protection of the transferred data cannot be adequately ensured even by additional measures.

The national data protection supervisory authorities have a very important role to play in the application of appropriate safeguards such as the standard contractual clauses. They are obliged to review the application of the appropriate safeguards, in particular if a complaint is lodged against a data transfer on the basis of an appropriate safeguard that casts doubt on the effectiveness of an adequacy decision by the EU Commission.

According to Art. 58 GDPR, the national supervisory authorities must prohibit the data transfer or order its suspension if there is no valid adequacy decision by the EU Commission, neither the appropriate guarantee nor additional measures sufficiently ensure the protection of the data transferred to a third country and the data exporter does not suspend or terminate the data transfer itself.

In their assessment of the level of protection existing in the third country, the supervisory authorities are ultimately bound by adequacy decisions of the EU Commission if these are valid.

5. The New "Trans-Atlantic Data Privacy Framework"-Agreement

A few years after the Court of Justice ruling of 16 July 2020 ("Schrems II"), the EU Commission and the USA have made a new attempt at a data protection agreement. A new

adequacy decision by the EU Commission should finally put the transfer of personal data to US companies on a legally secure footing.

a. Preparations

On 25 March 2022, US President *Biden* and EU Commission President *von der Leyen* announced their agreement in principle on a "Trans-Atlantic Data Privacy Shield Framework" Mechanism. The content of this agreement is set out in a press release from the US government, among other things.[14]

This results in the following:[15]

Instead of the ombudsperson of the previous "EU-US Privacy Shield"-Agreement, the "Trans-Atlantic Data Privacy Shield Framwork"-Agreement is to create a quasi-judicial, two-tiered body that will decide on complaints from data subjects in the EU. The body would be authorised to investigate comprehensively and order binding remedies. Although it should not be part of the judiciary, it should be as independent as possible. In particular, it should be composed of persons who are not members of the US government.

Furthermore, new measures are being established at the US security authorities in order to reduce surveillance to a proportionate level and enforce constitutional standards. It remains unclear what these measures will be. The USA will not implement these changes by means of a parliamentary act, but only by means of a new administrative regulation (so-called Executive Order) issued by the US President.

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement is intended to build on the previous "EU-US Privacy Shield" Mechanism. The requirements for US companies will remain the same and previous certifications will continue to apply. Accordingly, even the term "Privacy Shield" will continue to be used for the certification. The US government had continued the "Privacy Shield" certification unchanged even after the ruling of the Court of Justice on 16 July 2020.[16]

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement contains certain principles for the self-certification of US companies that are based on European data protection law. They appear to be a kind of GDPR "light".[17] Self-certification is carried out by registering a US company on a Department of Commerce website in return for a registration fee. The corresponding website has been available since 17 July 2023.[18] From this date, the approximately 2,600 "Privacy Shield"-certified US companies will also be considered "Trans-

[14] For more information see: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states and european commission-announce-trans-atlantic-data-privacy-shield framework.pdf> [10.05.2024]. Also *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

[15] *Glocker F.,* EU-US Data Privacy Framework: Beschluss der EU-Kommission, <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024] Also: *Glocker F.,* Politische Lösung für Datentransfer in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

[16] For more information see: <https://www.privacyshield.gov/article?id=EU-US-Privacy-Shield-Programm.html> [10.05.2024].

[17] Thus expressly *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

[18] The website can be found at <https://www.dataprivacyframework.gov/s.html> [10.05.2024].

Atlantic Data Privacy Framework"-certified. These include all major US cloud providers, SaaS providers and IT service providers.

b. So-called. Executive Order and Adequacy Decision of the EU Commission

On 10 July 2023, the EU Commission adopted the "Trans-Atlantic Data Privacy Shield Framework"-Agreement and announced the corresponding adequacy decision in the Official Journal.[19] The US government has also published the US President's so-called Executive Order. Due to the improvements in the law of the US security authorities, the EU Commission now considers the US level of data protection to be equivalent to that of the EU if US companies have self-certified under the new mechanism.[20]

6. Conclusions - "Schrems III"?

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement has a decisive advantage: it offers legal certainty! The EU Commission's new adequacy decision binds national data protection supervisory authorities. They may not prohibit data transfers to self-certified US companies, but must treat them as authorised. This eliminates the great uncertainty surrounding standard contractual clauses, which the data protection supervisory authorities previously regarded as insufficient protection for data subjects in some cases.

The transfer to non-self-certified US companies is also effectively facilitated. It is true that data controllers must continue to conclude standard contractual clauses with non-self-certified companies. In such cases, national data protection supervisory authorities would actually be obliged to examine the law of the third country for compatibility with European data protection law (so-called transfer impact assessment). Instead of carrying out their own so-called transfer impact assessment, the parties can therefore now refer to the existing assessment of US law by the EU Commission in the adequacy decision.[21]

It is doubtful whether the "Trans-Atlantic Data Privacy Shield Framework" - Agreement and the EU Commission's adequacy decision really fulfil the requirements of the Court of Justice. Resistance to this is already very strong:

The establishment of an independent, quasi-judicial body to examine complaints is indeed skilful and could possibly meet the Court of Justice's requirements for a judicial remedy. However, it remains unclear whether the very generally formulated so-called Executive Order of the US President, on which the extensive surveillance activities of the US security authorities are based, will fulfil the requirements of the Court of Justice for clear and precise rules on the scope and application of the measures in question. Furthermore, it is not clear from the published documents how the surveillance by US security authorities can be limited to what is "absolutely necessary" as required by the Court of Justice.

The fate of the "Trans-Atlantic Data Privacy Shield Framework"-Agreement could once again be decided before the Court of Justice. Civil rights organisations such as the *NOYB*[22] -

[19] Decision (EU) 2023/4745 of the European Commission of 10 July 2023.

[20] On this in detail *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

[21] *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-dereu-kommission.html> [10.05.2024].

[22] „None Of Your Business".

European Center for Digital Rights, which is led by the complainant *Schrems,* have already announced their intention to bring an action against the EU Commission's new adequacy decision. French member of the European Parliament *Latombe* has also expressed this intention. However, the Court of Justice is not expected to rule on this quickly.[23]

Note: For the transfer of personal data to other third countries for which - unlike the USA - there is no adequacy decision by the EU Commission, the ruling of the Court of Justice of 16 July 2020 remains relevant.[24]

Bibliography:

1. Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.
3. 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 1995 L 281, 31.
4. Decision 2000/520/EC of the European Commission of 26 July 2000.
5. Decision (EU) 2016/1250 of the European Commission of 12 July 2016.
6. Decision (EU) 2023/4745 of the European Commission of 10 July 2023.
7. *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017.
8. *Bernsdorff N.*, „EU-US Data Privacy Shield Framework“ und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210.
9. *Eichenhofer E.*, „e-Privacy“ im europäischen Grundrechtsschutz: Das „Schrems“-Urteil des EuGH, Europarecht (EuR) 2016, 76.
10. *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].
11. *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].
12. *Kühling J.*, *Heberlein J.*, EuGH „reloaded“: „unsafe harbor“ USA vs. „Datenfestung“ EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7.
13. *von Lewinski K.*, Privacy Shield – Notdeich nach dem Pearl Harbor für den transatlantischen Datenverkehr, Europarecht (EuR) 2016, 405.
14. *Rüpke G.*, *von Lewinski K.*, *Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, Munich, 2018.
15. *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017.

[23] See *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210, 213.

[24] *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210,214; *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024]; also *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

16. *Schreiber G.*, *Kohm W.*, Rechtssicherer Datenschutz unter dem EU-US Privacy Shield? – Der transatlantische Datenverkehr in der Unternehmenspraxis, Zeitschrift für Datenschutz (ZD) 2016, 255.
17. *Schwartmann R.*, Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2016, 864.
18. *Weichert Th.*, EU-US Privacy Shield – Ist der transatlantische Datenverkehr nun grundrechtskonform?, Zeitschrift für Datenschutz (ZD) 2016, 209.
19. *Wuermeling U.*, Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.
20. CJEU, Case C-362/14, *Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd.* („Schrems I"; 2015).
21. CJEU, Case C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd., Maximillian Schrems* („Schrems II"; 2020).