AmCham GERMANY

American Chamber of Commerce in Germany e.V.

EU-US Privacy Shield Agreement Invalid: Recommendations for Action

The EU-US Privacy Shield was declared invalid. For businesses in Europe using US cloud services, the ruling of July 16, 2020 has significant consequences. They can no longer rely on the guarantee of an adequate level of data protection under the Privacy Shield when using US services.

What Is the Privacy Shield and What Has It Regulated?

The EU-US Privacy Shield is an informal agreement between the US and the EU, which was designed to regulate transatlantic data exchanges in accordance with an adequate level of data protection. US businesses under the Privacy Shield have committed themselves to respecting established restrictions and principles to protect the data of EU citizens.[1]

The privacy shield thus served as a basic requirement for the use of US tools and the transfer of data to the United States in order to comply with the EU's basic data protection regulation (GDPR).

GDPR, Cloud Act and Patriot Act: Criticism of the Privacy Shield

American law stands in contrast to the EU GDPR, which lays down strict rules for the protection of personal data within the EU. However, the assurances given by the Privacy Shield are not compatible with the Cloud Act of 2018 and the Patriot Act of 2001. These guarantee the American authorities extensive rights in connection with all data stored on American servers and by American companies. That means: The authorities can oblige US providers to release all data (including personal data).[2]

EU-US Privacy Shield Agreement Invalid but Standard Contractual Clauses Still Valid

The Austrian lawyer and data protection activist Maximilian Schrems has therefore gone to court and in 2015 firstly brought down Safe Harbour (the predecessor of the Privacy Shield) and finally the previously valid privacy shield. Safe Harbour and the Privacy Shield were set up on the same legal basis.

In its ruling of 16 July 2020 (Case C311/18), the ECJ declared Decision 2016/1250 of the European Commission on the transfer of personal data to the US (Privacy Shield) to be invalid. At the same time, the ECJ found that Commission Decision 2010/87/EC on Standard Contractual Clauses (SCC) is in principle still valid.[3]

---

[1] https://www.privacyshield.gov/welcome
[2] https://www.stackfield.com/de/blog/privacy-shield-alternative-114
[3] https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

The ruling has the following consequences for the transfer of personal data to the US and other third countries[4]:

1. The transfer of personal data to the US on the basis of the Privacy Shield is not permissible and must be stopped immediately. The ECJ has declared the Privacy Shield invalid because the US law assessed by the ECJ does not provide a level of protection that is substantially equivalent to that in the EU.
2. For a transfer of personal data to the US and other third countries, the existing standard contractual clauses of the European Commission can continue to be used. However, the ECJ stressed the responsibility of the controller and the recipient to assess whether the rights of data subjects in the third country enjoy a level of protection equivalent to that in the Union.
3. The judgement's findings also apply to other guarantees under Article 46 of the GDPR, such as binding corporate rules (BCRs), on the basis of which personal data are transferred to the US and other third countries. Therefore, complementary measures must also be agreed for data transfers based on BCRs, unless the rights of data subjects in the third country do not enjoy an equivalent level of protection as in the Union.
4. The transfer of personal data from the EU to the US and other third countries under Article 49 of the DPA continues to be permissible, provided that the conditions of Article 49 of the DPA are met in the individual case. The European Data Protection Committee has published guidelines on the application and interpretation of this provision.
5. Data controllers who wish to continue transferring personal data to the US or other third countries must immediately verify whether they can do so under the conditions set out above. The ECJ has not granted any transitional or grace period. Although the ECJ has at various points in its ruling emphasized the primary responsibility of the transferor of personal data and the recipient, it has also assigned a key role to supervisory authorities in enforcing the DPAs and further decisions on data transfers to third countries.[5]

Consequences for Businesses: Which Businesses Are Affected?[6]

US tools are widely used in German businesses. The ruling is relevant…

- for companies that exchange data of users, customers, employees, but also device data that can be related to individual users, with partners or affiliated businesses in the US or other non-European countries.
- Most affected by the decision are international cloud services and social media platforms where cross-border data transfer – especially with regard to personal data – is part of the business model.

[4] https://www.datenschutz.de/urteil-des-europaeischen-gerichtshofs-zur-uebermittlung-personenbezogener-daten-in-drittlaender-schrems-ii-staerkt-den-datenschutz-fuer-eu-buergerinnen-und-buerger/
[5] https://www.datenschutz-bayern.de/dyn/virtdsb.html
[6] https://www.lexology.com/library/detail.aspx?g=c85ab6a9-bd29-4c64-9cb1-83ff9aac6ef6

- However, this also applies to SMEs that use, for example, newsletter systems or CRM (customer relationship management) systems from US providers or have personal data processed by companies in the US or other third countries.
- Pure business correspondence between businesses and US customers or US partners is not affected.[7]
- Anyone who transfers personal data from Europe to the US or other third countries outside the EU and the European Economic Area will have to check even more closely in future whether the recipient's data protection is guaranteed.

The ECJ has ruled that the EU-US Privacy Shield for data transfer to the US can no longer form a legal basis with immediate effect. At the same time, it questions the extent to which companies can base their data transfers to the US and other third countries on the standard contractual clauses of the European Commission. The ruling thus has massive implications for the legality of data transfers to all non-European countries. There is legal uncertainty in EU businesses that have relied on the Privacy Shield so far and continue to use US cloud services.[8]

Recommendations for Action: This Needs to Be Reviewed

Companies should take measures to bring international data transfers in their area of responsibility in line with the GDPR and the ECJ ruling.

The most important questions that businesses must now ask themselves are[9]:

1. Which tools are in use?
2. Where is the headquarter located?
3. Where are the servers located or where is the data stored/hosted?

Location of supplier	Location of group headquarters (if different)	Server location	Classification
GER/EU	GER/EU	GER/EU	unproblematic
GER/EU	US	GER/EU	Inspection required!
GER/EU		US	Urgent need for action!

[7] https://www.hoganlovells.com/de/news/privacy-shield-urteil_was-unternehmen-jetzt-tun-muessen
[8] https://www.debevoise.com/insights/publications/2020/07/schrems-ii-privacy-shield-invalid-and-severe
[9] https://www.stackfield.com/de/blog/privacy-shield-alternative-114

US	GER/EU	Urgent need for action!
US	US	Urgent need for action!

(Source: https://www.stackfield.com/de/blog/privacy-shield-alternative-114)

Possible Steps to Reduce Risk Include the Following Measures in Particular:

- **Data Mapping:** If not already done, businesses should identify the international data transfers and implemented transfer mechanisms in their area of responsibility. This includes both data transfers between individual Group companies, including the transfer of employee data within the Group, and transfers to service providers, business partners or other third parties. It is best for businesses to make a list of all the tools that are in use and get an overview of the tools that could potentially be dangerous.[10]
- **Reviewing the level of protection in individual cases**: In accordance with the requirements of the European Court of Justice, companies must assess and document for each individual case whether sufficient guarantees have been implemented to safeguard international data transfers. In this respect, the extent to which the data recipient is subject to the powers of intervention of the US secret services will be particularly relevant in the case of data transfers to the US.[11]
- **Switching to alternative guarantees:** If data mapping reveals that only the privacy shield was used to legitimize the transmission, businesses will have to switch to other guarantees due to the ineffectiveness of the privacy shield. In order to have legal certainty, companies can fall back on providers from Germany (or Europe). A German provider whose server is located in Germany is subject to German jurisdiction. Such a provider is not affected by the Cloud Act and must be able to guarantee sufficient data protection. In this case the Privacy Shield is not required from the outset.
- **Implementation of additional protective measures:** Even in the case of data transfers based on the standard contractual clauses, it must be examined whether the implementation of additional protective measures, including the conclusion of further contractual guarantees, can adequately safeguard the level of protection at the recipient's end.
- **Monitordata protection authorities:** The opinions of the supervisory authorities at national level and the European Data Protection Committee expected in the near future should be taken into account. Individual opinions of data protection authorities have already been published.

[10] https://fortune.com/2020/07/16/privacy-shield-eu-us-companies-business/
[11] https://www.computerweekly.com/news/252486477/Privacy-Shield-Companies-face-new-hurdles-to-legally-transfer-data-to-the-US

Data Processing Operations Are Particularly Problematic

The ruling of the ECJ makes things even more complicated in practice on the Internet. Particularly problematic are data processing operations which have so far been based on the legitimate interest of the website operator and which have entailed the involvement of a body in the US with which no standard contractual clauses have been concluded. In many of the constellations described above, it must now be examined whether one of the exceptions of Art. 49 GDPR is applicable. In many cases, all that will remain is to obtain consent. Content banners will therefore have to be used even more frequently than before. Since the transfer to a site without an adequate level of data protection is a central point in the user's decision, this will probably have to be pointed out in the banner text itself. It is therefore to be expected that the banners will also have more text in the future. Website operators who want to prevent this must try to make their website as data-efficient as possible and should, if possible, limit themselves to the integration of European services. In practice, however, this will often be difficult.[12]

Communications & Government Relations

Ann-Cathrin Spranger
T +49 69 929104-43
E aspranger(at)amcham.de

[12] https://www.datenschutz-notizen.de/das-urteil-zum-eu-us-privacy-shield-und-seine-auswirkungen-auf-internetseiten-und-cookie-banner-1926622/