ECJ: Privacy Shield Decision invalid, but EU standard clauses still valid: What this now means!

In its decision of 6 October 2015, the European Court of Justice (ECJ) had already declared the so-called "predecessor regulation" – the Safe Harbour Principles – to be invalid, and now in its decision of 16 July 2020 (Case C-311/18), it also declared the "successor concept" – the EU-US Privacy Shield (EU Commission Decision 2016/1250) – to be so. The ECJ in the meanwhile also addressed the EU Commission Decision 2010/87 which concerns standard contractual clauses for the transfer of personal data to processors in third countries. While it has not declared this decision to be invalid, the grounds for the invalidity of the Privacy Shield also have an impact here – at least with regard to data transfer to the USA.

Invalidity of the Privacy Shield
The EU-US Privacy Shield no longer constitutes a basis for data transfer to the USA. This has implications for data transfer within companies, online applications, social media, cloud services, etc.

Why is this so critical?
According to Articles 13 and 14 of the GDPR, every data subject must also be proactively informed about data transfer to third countries. This means that, in contrast to how the legal situation previously stood with the Safe Harbour Decision, the issue is now on everyone's plate. In addition, as a result of the GDPR, there is a heightened focus on the matter and, above all, the sanctions are greater. Both fines and claims for damages must be considered here.

Why is the response now more complicated than it was in 2015 with the ECJ's Safe Harbour Decision?
In the previous "Schrems I" decision of 5 October 2015, the ECJ limited its grounds for invalidity to the fact that the EU Commission had not sufficiently examined the adequacy of the level of protection – particularly with regard to access powers of the US security authorities. At the time, this went far enough for invalidity to be declared.

In its ruling of 16 July 2020, the European Court of Justice has now, on the basis of the findings of the EU Commission in Decision 2016/1250, dealt with the legal framework and – to put it plainly – considered a sufficient level of protection in the USA to be non-existent. This difference between the two decisions is crucial and will also affect the evaluation of alternatives for data transfer to the USA – because this assessment by the ECJ must also be taken into account when evaluating other legal bases for data transfer to the USA.

In declaring the EU-US Privacy Shield invalid, the ECJ stated that the US does not provide an adequate level of protection for data subjects due to the lack of judicial legal protection options available to EU citizens, particularly in view of the extensive access available to the US authorities. Special protective measures must therefore be taken for the transfer of data to the USA.

General validity of standard contractual clauses for third country transfers
The ECJ made it clear that the EU Commission's decision on the standard contractual clauses is not invalid. The standard contractual clauses thus continue to be eligible for the transfer of personal data to a third country.

The background: The standard contractual clauses are valid as the legal basis for any data transfer to a third country, whereas the EU-US Privacy Shield only applies to data transfer to the USA.

BUT: In this context, the ECJ clarifies that when EU standard clauses within the meaning of Article 46(1) and (2) of the GDPR are used, whether there are indeed adequately enforceable rights and effective legal remedies in the third country concerned must be verified. If this is not the case, the competent supervisory authorities may – and indeed must – suspend or prohibit corresponding data transfers.

In this regard, the ECJ is reinforcing European data protection principles and the role of data protection supervisory authorities. It also makes it clear that international data traffic is still possible, but that the fundamental rights of European citizens must be respected.

Relevant not only for data transfer to the USA
The requirement for the examination of a transfer to a third country to be the responsibility of the controller as data exporter and the recipient as data importer is not limited to the USA.

The examination required by the ECJ applies to any data transfer to a third country unless the EU Commission has recognised an adequate level of data protection in the third country by means of a decision.

In other words, the mere signing of an EU standard contract alone is also no longer sufficient for other third countries.

In concrete terms: what does this mean for data transfer to the USA?
The EU-US Privacy Shield no longer constitutes a legal basis for data transfers to the USA. The data transfer must therefore be made on a different basis within the meaning of Art. 44 et seq. GDPR. In this context, the ECJ's statements on the Privacy Shield must again be taken into account.

If a third country – such as the USA – does not offer an adequate level of data protection due to the absence of an adequacy decision by the EU Commission, a data transfer is permissible under Art. 46 GDPR, subject to appropriate guarantees. Art. 46 GDPR regulates one of the ways in which it can be ensured that the level of protection provided by the GDPR is guaranteed in data transfers to third countries and international organisations. This includes in particular

- so-called binding corporate rules, but these must be approved by the competent data protection supervisory authority and are therefore ruled out as a quick alternative,
- approved codes of conduct and certification; this possibility was added when the GDPR came into force and to date has seldom been used or approved,
- or the EU standard contractual clauses.

The ECJ determined that the US does not provide an adequate level of protection for data subjects due to the lack of judicial remedies for EU citizens, especially in view of the extensive access possibilities of the US authorities.

This means that, even with the alternative legal bases, what now must be assessed is whether and how sufficient protection can be ensured in such a way that an adequate level of data protection is guaranteed for data recipients in the USA. This seems – at least at present – difficult to quantify.

What should be done in compliance with the ECJ if a legal basis does not apply?
As a consequence, the controller is obliged to suspend the transfer of data and/or to rescind the contract. If the controller does not comply with this obligation, the supervisory authority is in turn obliged under Article 58(2)(f) and (j) of the GDPR to suspend or prohibit the transfer of personal data to a third country. The European Data Protection Board refers to this in its FAQ of 23.07.2020 (paragraph 1).

What authorisation still remains?
The only apparent option for data transfer to the USA in compliance with data protection law is currently likely to be Art. 49 GDPR. In the absence of an adequacy decision and suitable guarantees, data can therefore only be transferred to the USA in exceptional cases under Article 49 of the GDPR. This applies in particular if

- the data subject has explicitly consented to the data transfer after having been informed of the possible risks of such data transfers to the data subject due to the absence of an adequacy finding and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
- the transfer is necessary for the establishment, exercise or defence of legal claims.

The consent of the data subject as a solution?!
Consent under Art. 49 GDPR can also be considered as the basis for transfer to third countries. This is pointed out both by the European Data Protection Board in its FAQ of 23.07.2020 and by the German data protection supervisory authorities in their press release.

The German data protection supervisory authorities refer to the guidelines of the European Data Protection Board on Art. 49 GDPR. In its FAQ of 23.07.2020 (paragraph 8), the European Data Protection Board sets out certain requirements for such consent.

The effectiveness of such consent depends on its transparency and completeness. It therefore needs to be based on careful advice and must be meticulously constructed.

What's to be done?

The European Data Protection Board explicitly states in its FAQ of 23.07.2020 that there is no transition period. Therefore, immediate action must be taken. Even if the decision means that data transfer to the USA will be necessary, there is a need for action for every third country!

Talk to us! We're here to support you!

Here's how you can proceed: **Checklist from the law firm *dmp Derra, Meyer & Partner Rechtsanwälte PartGmbB 2020***				
Sequence			**Step**	**Checkbox**
1.			**Identify all transfers of personal data to countries outside the EU.**	☐
	1.1		**Distinguish between data transfer to the USA and other third countries.**	☐
	1.2		**Also check whether your service providers involve (other) companies in third countries as subcontractors.**	☐
2.			**Check whether personal data is being transferred.**	☐
	2.1		**Is personal data being transferred to companies in third countries?**	☐
	2.2		**Do companies from third countries have access to personal data at your company?**	☐
	2.3		**Can a transfer or access be restricted by, for example, encryption?**	☐
3.			**Identify the legal basis for the data transfer.**	☐
	3.1		**Is the transfer based on the EU-US Privacy Shield?**	☐
		3.1.1	**Identify the relevant companies.**	☐
		3.1.2	**Encourage the relevant companies to agree on alternative arrangements.**	☐
		3.1.3	**Check the alternative arrangements (see point 3.3).**	☐
	3.2		**Is the transfer based on the EU standard contractual clauses or on binding corporate rules (BCR)?**	☐
		3.2.1	**If a transfer is made to the USA, the ECJ's statements on the appropriate level of data protection must also be observed on EU standard contractual clauses or BCRs.**	☐
		3.2.2.	**If a transfer is made to another third country, the adequacy of the level of data protection there must also be examined.**	☐

		3.2.3.	**For assessment purposes, you should also contact the data recipient in the third country. This is also obligatory.**	☐
	3.3		**Is the transfer based on one of the authorisation provisions of Article 49 of the GDPR?**	☐
		3.3.1	**Check the prerequisites for authorised data transfer.**	☐
		3.3.2	**Especially with consents: Check the legal requirements for valid consent.**	☐
4.			**Check and, if necessary, amend privacy notices in accordance with Art. 13, 14 GDPR.**	☐