

16.07.2020

DATA PROTECTION

EUROPEAN COURT OF JUSTICE STRIKES DOWN PRIVACY SHIELD – DATA EXCHANGE WITH THE US WILL BECOME MORE DIFFICULT

On 16 July 2020, the European Court of Justice (ECJ) again rendered a spectacular judgment on the transfer of personal data to the US. Effective immediately, companies in the EU will no longer be able to rely on the Privacy Shield programme negotiated between the EU Commission and the US government when transferring data to the US. Although the widely used “standard contractual clauses” will essentially continue to be applicable as an alternative basis for data transfers to third countries, the ECJ has imposed stringent requirements on contracting parties seeking to base their data exchange on these contractual clauses.

According to the General Data Protection Regulation (GDPR), the exchange of employee, customer and supplier data with group companies, service providers and business partners outside of the EU is only permissible if an “adequate level of data protection” is ensured in the third country. In the assessment of the ECJ, this is not the case in the US due to the far-reaching powers of the US security authorities to access electronically stored data of foreigners and the lack of available legal remedies. The ECJ has declared the derogating “adequacy decision” of the EU Commission, according to which a sufficient data protection level is ensured for data transfer under the Privacy Shield, invalid with immediate effect.

The Privacy Shield had been in effect since 2016 and was intended to replace the Safe Harbour Agreement, which the ECJ struck down in 2015 for near-identical reasons. Both programmes provided that US companies wanting to process EU partners’ data would undertake to comply with certain data protection standards, thus being able to certify themselves as “compliant with data protection”. In the ECJ’s view, however, the improved standards of the Privacy Shield do not represent an adequate level of data protection either: firstly, because far-reaching data access by US security authorities remains possible, and secondly, because data subjects’ legal protection options are limited to an ombudsman procedure that does not correspond to the European understanding of an independent judge.

The direct consequence of today’s judgment is that **undertakings which to date have relied solely on their US partner’s Shield certification for data exchange with the US no longer have a basis for such data transfers**. In such cases, therefore, there is a need for rapid action.

To date, a frequently employed alternative to Privacy Shield has been to conclude what are termed standard contractual clauses with US recipients. In these clauses, the parties undertake to process personal data on an adequate level of data protection. The EU Commission passed these standard contractual clauses on the basis of the EU Data Protection Directive, and they will continue to be valid after today’s evaluation by the ECJ.

When using these standard contractual clauses, however, the parties have a duty to check whether the national legal situation in the recipient’s country does indeed permit the data protection obligations under the contractual clauses to be met, the ECJ states. Even after standard contractual clauses have been concluded, the Court continues, data transfers will not be permissible if the recipient is bound by applicable national law to tolerate state actors’ access to EU citizens’ data where this access is disproportionate according to European standards. Should the parties find that it is impossible to comply with the standard contractual clauses’ data protection guarantees, given the actual circumstances in the recipient’s country, then according to the ECJ they are obliged to cease the data exchange. If they fail to comply with their duties of verification and action, the data transfer will be in breach of the GDPR.

How exactly and in what depth companies wanting to use standard contractual clauses for data transfer to a third country are to check the level of data protection there, the ECJ does not say. This is unfortunate, not least because despite the legal expertise available to the EU Commission, it is now the second time that the Commission has failed to accurately evaluate how appropriate the level of data protection in the US is. The ECJ is also ducking out of a clear answer to the question of whether it is in fact conceivable that data recipients in the US are able to ensure compliance with the standard contractual clauses' data protection guarantees, despite the deficiencies the ECJ has found in the US legal framework.

It can be assumed that data protection supervisory authorities will be dealing with these issues in the near future. The ECJ has expressly called upon the supervisory authorities to verify that compliance with standard contractual clauses is in fact possible in a third country when data subjects file complaints. Should the finding be negative, then the public authorities must prohibit the data transfer.

On the day of the decision itself, the EU Commission announced that it would be starting the process of introducing new standard contractual clauses. Until such time, EU undertakings that regularly transfer personal data to third countries and rely on the current standard contractual clauses should keep a close eye on how matters develop. In any event, they should ensure that they document their endeavours to verify the framework conditions in the recipient's country and check that their contracting partner is complying with the terms and conditions of the contract.

EXPERTISE

Data Protection

EXPERTS

Dr. Christian Hamann

Dr. Manuel Klar

Luca Maria Thieme

Simon Clemens Wegmann