Privacy Alert: European Data Protection Board Releases FAQ on the Ruling Invalidating the EU-U.S. Privacy Shield

Related Professionals

Marcel C. Duhamel

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 7.27.2020

Leaving businesses scrambling, the European Union Court of Justice invalidated the EU-U.S. Privacy Shield on July 16, 2020. Late last week, the European Data Protection Board (EDPB) published 12 Frequently Asked Questions on the judgment. Unfortunately, they provide little direction to U.S. businesses attempting to assess how to react to the decision. In particular, many businesses have relied on Privacy Shield to permit the transfer of HR data from their EU operations to a centralized U.S.-based HR function. While the EDPB points to the continued vitality of "standard contractual clauses" in the short term, those clauses appear susceptible to the same perceived deficiency that doomed Privacy Shield: they may not be capable of providing UE data subjects an effective judicial remedy against surveillance by U.S. intelligence services. Below is a brief summary of these FAQs.

1. What did the Court rule in its judgment?

The Court of Justice reviewed the European Commission's Decision 2010/87/EC on "Standard Contractual Clauses" (SSCs), by which the European Commission can determine that SCCs offer sufficient safeguards for data protection for data to be transferred internationally. Although the Court confirmed the validity of SCCs, that validity depends on whether the 2010/87/EC Decision includes effective mechanisms to ensure compliance with the level of data protection guaranteed within the EU by the General Data Protection Regulation (GDPR). The Court determined that the EU-U.S. Privacy Shield did not guarantee equivalent protections as the GDPR, especially with respect to access to personal data transferred from the EU to the U.S. by U.S. public authorities for national security purposes.

2. Does the Court's judgment have implications on transfer tools other than the Privacy Shield?

Yes. The judgment applies to any electronic transfer of data to the U.S. that falls under the scope of Section 702 FISA and EO 12333, regardless of the transfer tool.

3. Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

No.

4. I was transferring data to a U.S. data importer adherent to the Privacy Shield, what should I do now?

Transfers on the basis of the Privacy Shield are illegal. A different mechanism must be used.

5. I am using SCCs with a data importer in the U.S., what should I do?

Whether or not transfers can be made on the basis of SCCs will depend on the circumstances of the transfers and supplementary measures put in place. Following a case-by-case analysis of the circumstances, the supplementary measures and SCCs must ensure that U.S. law does not impinge on the adequate level of protection guaranteed by the SCCs.

6. I am using Binding Corporate Rules (BCRs) with an entity in the U.S., what should I do?

Whether or not transfers can be made on the basis of BCRs will depend on the circumstances of the transfers and supplementary measures put in place. Following a case-by-case analysis of the circumstances, the supplementary measures and SCCs must ensure that U.S. law does not impinge on the adequate level of protection guaranteed by the BCRs.

7. What about other transfer tools under Article 46 GDPR?

The standard for appropriate safeguards in Article 46 GDPR is that of "essential equivalence."

8. Can I rely on one of the derogations of Article 49 GDPR to transfer data to the U.S.?

Yes, following the guidelines set forth by the EDPB. Some of these guidelines include: (1) requiring the explicit, specific, and informed consent of the data subject to the data transfer; (2) transfers that are necessary for the performance of a contract between a data subject and the controller may take place only where the transfer is occasional and necessary in relation to a contract; and (3) transfers that are necessary for important reasons of public interest must be restricted to specific situations and meet the strict necessity test.

9. Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?

Yes, so long as such SCCs or BCRs and supplementary measures ensure an essentially equivalent level of protection as provided by the GDPR and the law of the third country will not impinge on the effectiveness of such supplementary measures.

10. What kind of supplementary measures can I introduce if I am using SCCs or BCRs to transfer data to third countries?

Supplementary measures are to be provided on a "case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to

check if it ensures an adequate level of protection." The EDPB intends to provide further guidance concerning these supplementary measures.

11. I am using a processor that processes data for which I am responsible as controller, how can I know if this processor transfers data to the U.S. or to another third country?

Contracts with processors in accordance with Article 28.3 of the GDPR must provide whether transfers are authorized or not. Authorization must also be provided concerning processors to entrust sub-processors to transfer data to third countries.

12. What can I do to keep using the services of my processor if the contract signed in accordance with Article 28.3 GDPR indicates that data may be transferred to the U.S. or to another third country?

If data is transferred to the U.S., and neither supplementary measures nor derogations under Article 49 GDPR apply, the only solution is to negotiate an amendment or supplementary clause to your contract to forbid transfers to the U.S. If data is transferred to another third country, the legislation of that third country must be compliant with the requirements of the Court and with the level of protection of personal data expected. If no suitable ground for transfers to a third country can be found, personal data should not be transferred and or processed outside the EU.

Conclusion

U.S.-based businesses—and employers in particular—may have hoped for a "grace period" similar to the one that followed the invalidation of the Safe Harbor. Unfortunately, the EDPB has made clear that no such grace period will be extended. While the EDPB does point to standard contractual clauses as a possible transfer mechanism, there may be strong reason to believe that this mechanism will fall victim to the same perceived deficiency that led to Privacy Shield's demise. U.S.-based businesses who have been relying on Privacy Shield to effect cross-border data transfers now face difficult, case-by-case assessments of how to proceed.