Cooley

Europe's Highest Court Invalidates the EU-US Privacy Shield, Casts Doubt on Viability of Model Clauses for Data Transfers to the US

July 17, 2020

On July 16, 2020, the Court of Justice of the European Union issued a decision that uprooted long-standing legal frameworks on which thousands of US and EU companies have relied to transfer personal data from the EU to the US.

First, the CJEU invalidated outright the EU-US Privacy Shield framework, which was put in place by the US Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US in support of transatlantic commerce.

Second, the CJEU upheld the European Commission's Controller-Processor Standard Contractual Clauses (Model Clauses) as a valid compliance mechanism for the transfer of personal data outside of the EU in general. However, the CJEU's rationale for invalidating the Privacy Shield raised questions about whether the Model Clauses remain a viable compliance mechanism for purposes of transfers from the EU to the US. Despite this, the Model Clauses may be the only practical alternative to Privacy Shield for many companies.

Privacy Shield invalidated

CJEU decision

In invalidating the Privacy Shield, the CJEU determined that the Privacy Shield did not afford EU individuals the protections equivalent to those afforded by EU law, including the General Data Protection Regulation.

Specifically, the CJEU cited (a) the ability of US public authorities to obtain wide-ranging access – including under surveillance programs such as PRISM – to personal data transferred to the US under the Privacy Shield, and (b) the deficiency of the Privacy Shield's Ombudsperson function in that it neither provided individuals with any cause of action before a body offering guarantees substantially equivalent to those required by EU law, nor was it empowered to adopt decisions that are binding on the US intelligence services.

Possibility of enforcement grace period

Following the CJEU decision, the UK ICO signalled that it "will be working with UK Government and international agencies to ensure that global data flows may continue," indicating the possibility of a grace period during which European authorities will not take action against companies that rely on the Privacy Shield. Businesses are expected to call for such a grace period given the unexpected decision. A grace period would be consistent with EU regulators' reaction to the CJEU's 2015 invalidation of the Privacy Shield's predecessor – the Safe Harbor framework. At that time, EU regulators announced a grace period of approximately four months, during which they agreed not to enforce that decision.

Will Privacy Shield come back?

The Privacy Shield itself was already an attempt to address concerns that the CJEU raised around the US government's access to personal data, which caused the CJEU to invalidate the Safe Harbor in 2015. The establishment of the Ombudsperson function, for example, was an attempt to offer EU residents additional protections, but was dismissed as inadequate by the CJEU in yesterday's decision. Given that history – and in light of the somewhat fundamental nature of the perceived conflicts between the US laws concerned and EU laws governing privacy – it is unclear how the issues CJEU raised in the decision could be solved without material concessions by either or both of the US or the EU.

Applicability of the decision to the UK and Switzerland

The UK is bound by the CJEU's decision until at least December 31, 2020. Under the EU-UK Withdrawal Agreement, EU data protection legislation (including the GDPR) will continue to apply to and in the UK until that date. It is not yet clear what arrangements regarding data protection laws the UK will have with the EU starting in 2021. However, material deviations from the CJEU's decision may adversely affect the UK's efforts to have the European Commission find the UK "adequate" for purposes of receiving personal data from the EU. Any such adequacy decision would likely have to address the potential nature of any onwards transfers of personal data from the UK to the US.

Swiss authorities are not legally bound by the CJEU's decision because Switzerland is not a member of the EU or the EEA. As a practical matter, however, Switzerland is unlikely to adopt a different stance in respect of the validity of the Swiss-US Privacy Shield framework to that outlined in the CJEU decision. When the CJEU invalidated the Safe Harbor, the Swiss Federal Data Protection and Information Commissioner quickly followed suit and effectively invalidated the US-Swiss Safe Harbor.

Validity of Model Clauses for data transfers to the US called into question

The CJEU's rationale for invalidating the Privacy Shield may also put Model Clauses on shaky ground as a solution for EU to US data transfers.

On the one hand, the CJEU (a) concluded that Model Clauses remain theoretically valid as a potential data transfer mechanism, and (b) did not find that Model Clauses could not be used to transfer personal data to the US. The CJEU, however, emphasized that Model Clauses' validity is not absolute.

Specifically, for a particular data transfer, the validity of Model Clauses will be premised on the determination of the EU exporter, in consultation with the US importer, that those clauses, in the context of that particular transfer, are sufficient to ensure a level of protection at least "essentially equivalent" to that guaranteed within the EU by the GDPR. The CJEU was clear that this will need a case-by-case analysis of both: (a) the terms and conditions of the Model Clauses themselves, and (b) the relevant aspects of the legal system in the recipient's country – specifically as they relate to rights of public authorities to access the transferred personal data and any relevant remedies available to affected individuals.

If – in light of all relevant circumstances of a particular transfer and local law considerations applicable to the importer – the Model Clauses do not/cannot operate to ensure a level of protection equivalent to that guaranteed by the GDPR, then the data importer and/or data exporter should stop the relevant transfer. In such circumstances, where the parties to such transfer do not themselves cease the transfer, EU data protection regulators are required to intervene to suspend or prohibit that transfer.

The CJEU's findings in invalidating the Privacy Shield – in relation to certain public authorities' apparently excessive rights to access transferred data – would be expected to weigh heavily on the analysis of the same equivalency question when considered by exporters/importers and EU data protection regulators in the context of use of the Model Clauses. Indeed, the Irish Data Protection Commission commented following the CJEU decision that "in practice, the application of [Model Clauses] transfer mechanism to transfers of personal data to the United States is now questionable."

Industry on both sides of the Atlantic will now look to the European Commission and the US government to develop a new transatlantic data transfer regime, and in the meantime, companies will look to the EU data protection regulators for guidance on the use of Model Clauses.

The flow of data across the Atlantic will continue, and for the moment, transfers under Model Clauses appear to remain valid, including for purposes of EU to US transfers. In the absence of the Privacy Shield or other practical alternatives, many organizations will have no choice but to either cease EU US data transfers or rely on Model Clauses.

Next steps for companies

Consider alternative basis for cross-border data transfer

Although we expect EU data protection regulators to offer a grace period, companies that have relied on the Privacy Shield to transfer data from Europe to the US should promptly begin work on establishing an alternative legal basis for those transfers under Chapter V of the GDPR, where possible. Depending on the circumstances, possible transfer mechanisms include:

- Executing Model Clauses (which should continue to be valid for transfers to the US, at least in the near term)
- Obtaining individuals' consent to the transfer (which can work in limited circumstances)
- Implementing Binding Corporate Rules (which is resource-heavy and time consuming)
- Relying on another Article 49 derogation that might be available for nonrecurring transfers

Check Privacy Shield compliance commitments

Companies that relied on the Privacy Shield or committed to comply with it in contractual relationships with customers, vendors, partners or other third parties should revise those contracts as appropriate.

Business-to-business service providers that relied on the Privacy Shield should consider proactively contacting customers to get ahead of the inevitable questions about their plans for adapting to the CJEU decision.

Companies that committed to Privacy Shield compliance in privacy notices or other public disclosures should revise those disclosures as appropriate.

Address cross-border data transfer risks in SEC disclosures and investor prospectuses

US-listed public companies should update, or consider adding, specific risk factor disclosures in SEC filings regarding EU cross-border data transfer restrictions to address the potential impact of the CJEU decision. Other companies disclosing risks in investor prospectuses should consider similar disclosures.

For assistance, contact a member of the Cooley c/d/p team.

Follow our blog at cdp.cooley.com for more coverage of this development and additional guidance.

Primary sources

Read the press release.

Learn more about the judgement.

Key Contacts

Ann Bevitt **London**	**abevitt@cooley.com** **+44 (0) 20 7556 4264**
Chris Coulter London	ccoulter@cooley.com +44 (0) 20 7556 4262
Leo Spicer-Phelps London	lspicerphelps@cooley.com +44 (0) 20 7556 4334