SEYFARTH SHAW

International Data Privacy Client Alert

Safe Harbor - Not so Safe After Schrems

By John P. Tomaszewski

Yesterday, October 6, 2015, the European Court of Justice ("ECJ") issued its Judgment in the Schrems case, and in doing so, continued along the seismic shift happening in law related to cross-border privacy. The two major elements of yesterday's Judgment are 1) The Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the US Safe Harbor framework (the "Safe Harbor Decision") is invalid, and 2) even if the Safe Harbor Decision were otherwise valid, no decision of the Commission can reduce the authority of a national data protection authority ("DPA") to enforce data protection rights as granted by Article 28 of the data protection directive ("DP Directive").

Clearly, the first element brings a more immediate concern for all the companies participating in the Safe Harbor framework. However, the second element will have much longer term consequences for the stability of US-EU commerce and privacy law.

Validity of the Safe Harbor Decision

Over 4,000 companies rely on the Safe Harbor Decision as the legitimate basis for transfers of data from the EU to the US. The unfortunate result of yesterday's Judgment is that such a basis for transfer is no longer valid as the ECJ has a direct and retroactive effect on how the DP Directive should be interpreted. Therefore, companies need to determine an alternative basis for lawfully transferring their data to the US. Fortunately, there are ways to do this. Unfortunately, until such measures are taken, companies moving data between the US and the EU may be in breach of EU law.

Derogations to Transfer Prohibition

The Directive provides for certain "derogations", or exceptions, which legitimize cross-border transfers of personal data. More specifically, cross-border transfers are permitted where:

- the individual has given his unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the individual and the business (which is the "data controller");
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the business (again, the "data controller") and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject.

Companies who use these exceptions still need to properly document how and why they are using these exceptions, and should work with their legal counsel to do so. This is particularly important because the exceptions are usually narrower in scope than a plain reading would suggest, due to the way the data protection regulators have interpreted them.

Data Transfer Agreements

Data transfer agreements that use Model Clauses (developed by the European Commission) are another means to legitimize cross-border transfers. While there are challenges with the implementation of Model Clauses, their use is the most obvious solution to this issue where the consent exception should not be used.

Binding Corporate Rules

From a more strategic perspective, Binding Corporate Rules ("BCR") can be a mitigation strategy to avoid the risk of another ECJ judgment invalidating a Commission decision. However, BCRs are time consuming and not inexpensive to put in place.

New Safe Harbor Agreement

While the ECJ invalidated the Safe Harbor Decision, it did give instruction on how to correct the deficiencies of the decision. In fact, the ECJ found the Safe Harbor Decision deficient not in the data protection principles, per se. One can take this to mean that the underlying concept of the data protection principles are not defective, merely the means by which the Commission issued its decision.

While it would seem that developing a Safe Harbor 2.0 might take an inordinate amount of time, work on this issue is already underway. In a press release yesterday, the UK Information Commissioner's Office ("ICO") noted that "…negotiations have been taking place for some time between the European Commission and US authorities with a view to introducing a new, more privacy protective arrangement to replace the existing Safe Harbor agreement… [and] that these negotiations are well advanced." Clearly, the Court has provided a roadmap to resolving the noted deficiencies in the Safe Harbor Decision.

While the Judgment is going to create challenges in the short term, most businesses will have a way to ensure their data can still legally flow between the EU and the US. However, businesses who relied on the Safe Harbor Decision are going to need to take some action to make sure their data flows are legitimized outside the Safe Harbor Decision framework until a new agreement is reached between the European Commission and the US.

National Data Protection Authority Jurisdiction

The second element of the Judgment, which will continue to have farther reaching effects than just the invalidity of the Safe Harbor Decision, is the inability of the Commission to limit the ability of individual national data protection regulators ("DPAs") from making a determination of "adequacy" (or lack thereof) for any transfer of data. The effect of this element of the decision is poised to render any Safe Harbor agreement inconsistent in its enforcement.

As the DPAs and the Commission are deemed to have concurrent jurisdiction in making adequacy determinations, it is quite possible that even when a new Safe Harbor agreement is in place, there is still the possibility that the individual DPAs will make determinations that the Safe Harbor will not be operative in that particular nation.

This inconsistency in application would seem to make it advisable to businesses to start to develop a blended approach to their data transfer practices -- for example, use of consent for consumer data, and use of model contracts for workforce data. Additionally, the development of BCR is going to take on a much more prominent role as a means of legitimizing cross-border transfers of personal data.

Regardless of the solution a business decides to take, the ECJ's Judgment yesterday will require a thorough review of how a business enables its data flows between the EU and the US.

John P. Tomaszewski is Senior Counsel and Team Co-Lead of Seyfarth's Global Privacy & Security (GPS) Team. If you have any questions, please contact your Seyfarth attorney or John P. Tomaszewski at jptomaszewski@seyfarth.com.

www.seyfarth.com