ROPES & GRAY

ALERT

Privacy & Data Security

March 8, 2016

European Commission Releases Text of Proposed Privacy Shield Agreement for Transfer of European Union Citizen Data to the United States

Attorneys
Heather Egan Sussman
Rohan Massey
James S. DeGraw
David McIntosh
Mark Barnes
Ira Parghi
David T. Cohen
Matthew Coleman

On February 29, 2016, the European Commission released the full text of the proposed EU-U.S. Privacy Shield agreement, a data protection self-certification framework for companies transferring EU citizen data to the United States. The framework is based on seven core privacy principles ("Principles"): *Notice, Choice, Security, Data Integrity and Purpose Limitation, Access, Accountability for Onward Transfer, and Recourse, Enforcement and Liability*.

Privacy Shield's predecessor – the U.S.-EU Safe Harbor – was invalidated last November by the European Court of Justice ("ECJ"), leaving more than 4,000 companies without a legal mechanism to transfer data from the EU. One of the grounds on which Safe Harbor was invalidated was that the agreement did not adequately protect Europeans' fundamental right to data privacy in respect of the collection and processing of data by the U.S. intelligence community. In the draft released on February 29, the Commission extensively outlines the checks and balances that will limit the U.S. intelligence community, new commitments made by U.S. public officials, and the remedies available to EU citizens for any violations of their fundamental rights regarding the processing of personal information identifying them.

The Privacy Shield imposes several obligations on corporate entities that are more stringent than those that were imposed by Safe Harbor:

- A self-certified company is required to include data protection provisions within its sub-processor (i.e., vendor) contracts, including provisions to obligate its agents to process all transferred personal information in a manner consistent with the Principles, to take reasonable and appropriate steps to remediate unauthorized processing upon notice, and to provide relevant contractual provisions to the Department of Commerce (DoC) upon request. The company will be responsible for the processing of personal data by its vendors acting on its behalf, unless the company can prove it was not responsible for the event that led to a user's complaint.
- A self-certified company is only permitted to transfer personal information to non-vendor third parties if such transfer is pursuant to a contract providing that the recipient will only use the data for limited and specified purposes that are consistent with the consent provided by the individual upon initial collection and that the recipient will provide a level of protection consistent with the Principles.
- A self-certified company is required to include links to the DoC's Privacy Shield site and the DoC's whitelist of self-certified companies.
- If it does not obtain an outside compliance review of its practices, a self-certified company is required to conduct employee training on the implementation of organizational privacy policies.
- A self-certified company must make available a mechanism for users to submit complaints and must respond to privacy-related complaints by EU citizens within 45 days. The response must include "an assessment of the merits of the complaint" and "how the organization will rectify the problem."

- A self-certified company is required to obtain an independent dispute resolution service to which EU consumers can forward unresolved disputes at no cost. In its privacy policy, the company must link to the dispute resolution mechanism.
- A self-certified company must retain its records on the implementation of its privacy policies and make them available upon request by a U.S. authority or independent dispute resolution service.

Additionally, the agreement outlines an EU "data subject's" escalation measures to obtain redress for any privacy complaint:

- A user must first contact the self-certified company using the company's available feedback mechanism.
- If the data subject is not satisfied with the company's response, he or she may seek redress through the independent dispute resolution service.
- The DoC will conduct a verification of a company's practices during its certification and recertification, and additional reviews when it receives what it deems non-frivolous complaints.
- The Federal Trade Commission ("FTC") will accept complaints from dispute resolution providers, the DoC, and EU Data Protection Authorities ("DPAs") and determine whether to conduct an enforcement investigation or proceeding.
- The EU DPAs are entitled to investigate complaints on their own, and a self-certified company has an obligation to cooperate if it either transfers Human Resources data from the EU or if it voluntarily agreed to be subject to DPA authority as part of the self-certification process.
- Finally, a data subject may utilize a new arbitral model, newly minted as the *Privacy Shield Panel*. The panel consists of a pool of at least 20 arbitrators, of whom the parties may stipulate to one or three for a final binding adjudication.

It is not entirely clear how the Privacy Shield will be administered. For example, it is unclear how the principles will apply to data processors. The *access* principle, which requires a company to provide EU citizens access to their personal data, may not be possible for a data processor to comply with as data processors generally do not have the right to access the data themselves. Furthermore, it is not yet clear what steps companies that self-certified under the old Safe Harbor framework must take in order to be compliant under the new rules.

The next step is for the Article 29 Working Party (a group comprised of EU national data protection authorities) to accept or reject the Commission's proposed agreement. Afterwards, there will be an extensive process for the agreement to be ratified within the EU. If and when it is ratified, the agreement is widely expected to be challenged in national courts by the same groups that challenged the Safe Harbor agreement. Only the ECJ can find the agreement invalid once it has been ratified.

If you have any questions regarding the Privacy Shield agreement, please contact Heather Egan Sussman, Rohan Massey, James DeGraw, David McIntosh, Mark Barnes, Ira Parghi, David Cohen, Matthew Coleman or any other member of Ropes & Gray's leading privacy & data security team.