COVINGTON

The EU-U.S. Privacy Shield: What's New and What's Next?

July 14, 2016

EU Data Protection

At a joint press conference on July 12, 2016 in Brussels, EU Commissioner for Justice, Consumers and Gender Equality, Věra Jourová and the U.S. Secretary of Commerce, Penny Pritzker, presented the Privacy Shield (see Press Release here, Adequacy Decision text here, Annexes here, Communication here, and Q&A factsheet here). The press conference followed the approval of the underlying adequacy decision by the College of EU Commissioners. This was the last step in the adoption of the Privacy Shield in the EU.

Background

Under Article 25 of the EU Data Protection Directive, personal data may only be transferred to third countries that ensure an "adequate" level of protection. In the absence of such protection, transfer is only permitted in certain situations: either on the basis of an exception to Article 25, or where adequate contractual safeguards have been provided. The European Commission has recognized a number of third countries as providing an adequate level of protection, and has also approved specific contractual clauses for overseas transfer. The Privacy Shield, much like the now defunct EU-U.S. Safe Harbor framework, is an alternative mechanism approved by the Commission to ensure this adequate level of protection for data transfers.

The predecessor of the Privacy Shield, the EU-U.S. Safe Harbor framework, was invalidated by the Court of Justice of the EU (CJEU) in October 2015 (Case C-362/14. Maximillian Schrems v Data Protection Commissioner). The EU-U.S. Safe Harbor framework had been criticised by many. Following the Snowden revelations, the Commission decided to review the Safe Harbor, issuing 13 recommendations for its improvement in November 2013. On this basis, negotiations commenced between the EU and U.S. and these negotiations were accelerated by the CJEU's Schrems judgment in October 2015.

On February 2, 2016, the European Commission and the U.S. Government reached a political agreement on the Privacy Shield, which is a new framework for transatlantic exchanges of personal data for commercial purposes. Later that month, on February 29, 2016, the European Commission published the draft text of the new Privacy Shield. This draft text was subsequently revised to reflect concerns raised by the Article 29 Working Party (composed of representatives of the data protection authorities of all the EU Member States, the European Data Protection Supervisor, and the European Commission, the European Data Protection Supervisor, and the European Parliament).

The finally adopted Privacy Shield consists of:

- an adequacy decision;

- Privacy Shield Principles (a detailed set of requirements based on principles such as notice, choice, access, and accountability for onward transfer) and details of the new arbitral model (Annex II);
- Official representations and commitments contained in separate letters from the:
  - International Trade Administration (ITA) of the Department of Commerce, which administers the program and an annex describing the new arbitral model available under the Privacy Shield (Annex I);
  - U.S. Secretary of State John Kerry, committing to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson (Annex III);
  - Federal Trade Commission Chairwoman Edith Ramirez (Annex IV);
  - U.S. Secretary of Transportation Anthony Foxx (Annex V);
  - General Counsel Robert Litt, Office of the Director of National Intelligence (Two letters, Annex VI); and
  - Deputy Assistant Attorney General and Counselor for International Affairs Bruce Swartz, U.S. Department of Justice (Annex VII).

Next Steps

Once translated and published in the Official Journal of the EU, the adequacy decision will enter into force. The U.S. Department of Commerce is now working on the implementation of the framework and will accept self-certifications from U.S.-based companies beginning on August 1, 2016.

On July 25, the Article 29 Working Party will meet to discuss their views on the Privacy Shield. Their assessment will be advisory. We understand that the European Parliament is planning to adopt a new resolution on the Privacy Shield in Fall 2016.

The U.S. Department of Commerce has released a Guide to Self-Certification (see here). Companies will need to (i) update their privacy policies, (ii) update their verification mechanisms, and (iii) identify an independent dispute resolution provider prior to self-certifying (and register with that provider where required). Private sector dispute resolution providers may enable companies to register through their programs prior to August 1. Once a company registers, certifying compliance with the Privacy Shield Principles, the commitment will be enforceable under U.S. law by the relevant enforcement authority, either the U.S. Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT). Any U.S. organization that is subject to the jurisdiction of the FTC or the DOT may participate in the Privacy Shield. The FTC and DOT have both committed to enforcing the Privacy Shield Framework.

The European Commission will also produce a citizens' guide to explain the redress options for EU citizens.

Obligations Under the New Privacy Shield

So, what are the new obligations for U.S. certified companies under the Privacy Shield? A number of the Privacy Shield principles are significantly more robust than the Safe Harbor. The

Privacy Shield's enforcement provisions, in particular, are rigorous. In addition to FTC enforcement under section 5 of the FTC Act, the Shield encourages individuals to bring their complaints directly to the signatory. If the complaint is not resolved, the consumer may bring a complaint before an independent dispute resolution body designated by the signatory, to the national data protection authority (DPA) or to the FTC. Signatories must comply with the results of these challenges within certain deadlines (for example, in the case of advice provided by the national DPAs, compliance must be achieved within 25 days of delivery of that advice). To the extent that there is a "persistent failure to comply" with any compliance decision, the matter may be escalated to the FTC or to the Department of Commerce for enforcement action. A signatory that is found to have persistently failed to comply with the Privacy Shield Principles, may be struck of the list of certified organizations. For unresolved complaints, however, the consumer may choose to invoke binding arbitration. For this, a specially-constituted "Privacy Shield Panel" of arbitrators, with expertise in both EU and U.S. data protection law, has been set up. Steps have been taken to ensure that this arbitration mechanism is as accessible as possible for EU data subjects.

Compared to the Safe Harbor, the Privacy Shield provides for a more thorough set of Principles to which signatories must adhere. For example, the privacy principles relating to onward transfer of personal data have been bolstered so that data may only be processed by third party data controllers for "(i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group), and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles." Onward transfer obligations will apply irrespective of the location of the third parties and the third parties will be contractually obliged to notify the signatory if they determine that they can no longer satisfy the Privacy obligations. If this happens, reasonable and appropriate steps have to be taken to remedy the situation or else the third party processor must cease processing.

In addition, there will be new restrictions on national security access. Once the data has been transferred to organizations located in the U.S. and self-certified under the Privacy Shield, U.S. intelligence agencies may only seek personal data where their request complies with U.S. law, such as the Foreign Intelligence Surveillance Act, or is made by the Federal Bureau of Investigation based on a so-called National Security Letter.

For further information on the differences between the Safe Harbor obligations and the new Privacy Shield obligations, see here.

Key Changes in the Privacy Shield Text

The Privacy Shield contains a much more robust set of commitments than those underpinning the Safe Harbor and will provide stronger protections to data subjects in the EU than its predecessor. The finalized Privacy Shield differs in some key respects from the draft published on February 29, 2016:

- Role of the Ombudsperson: The revised text provides further detail on the ombudsperson's ability to act "objectively and free from any improper influence," political or otherwise, and his or her responsibility to respond to Europeans' complaints.
- Bulk Data: There have been substantial clarifications on the bulk collection of data. The adequacy decision outlines that intelligence collection will be "as tailored as feasible" and will always relate to a foreign intelligence objective. U.S. intelligence gathering

practices are further explained in a detailed letter from the U.S. Office of the Director of National Intelligence (ODNI) (Annex VI). The ODNI explains that that bulk collection of personal data is neither "mass" nor "indiscriminate."

- Notice & Choice and Purpose Limitation: Data subjects can object to data transfers, for example when there is a "material" change of purpose for the use of the data that is either incompatible with the purposes for which the data was originally collected, or subsequently authorized by the data subject.
- Data Retention: The revised draft contains more explicit obligations on companies regarding limits on retention. Signatories may only retain personal information "for as long as it serves a purpose of processing" pursuant to the Privacy Shield's Data Integrity and Purpose Limitation. There are exceptions to this, for example when processing "reasonably serves the purposes" of one of the following: archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis.
- Automated decision-making: The new version of the adequacy decision references the protections that apply to "automated processing of personal data", also known as algorithmic treatment. Companies sometimes use automated processing to make decisions affecting the individual (e.g., credit lending, mortgage offers, and employment). U.S. law currently provides guidance on automated decision-making on a sector specific basis. Under the Privacy Shield, this area will be monitored closely by EU and U.S. authorities. A dialogue on this topic will form part of the Privacy Shield's annual review process.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Monika Kuschewsky	+32 2 549 52 49	mkuschewsky@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Dan Cooper	+44 20 7025 0820	dcooper@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Vera Coughlan	+32 2 549 52 34	vcoughlan@cov.com