Client Update
EU-U.S. Privacy Shield Open for Self-Certification on August 1

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

WASHINGTON, D.C.
Jeffrey P. Cunard
jpcunard@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

On August 1, 2016, U.S. organizations can finally begin to submit self-certification requests to the U.S. Department of Commerce under the new EU-U.S. "Privacy Shield." This opens a new era for the lawful transfer of personal data from the European Union westward across the Atlantic. The Commerce Department has published a practical guide, "How to Join Privacy Shield: Guide to Self-Certification," that sets out the steps to participation.[1]

WHAT CLEARED THE WAY FOR THE PRIVACY SHIELD TO BECOME OPERATIONAL?

On July 12, 2016, the European Commission adopted an "adequacy decision"[2] ("Decision") under the EU Data Protection Directive,[3] approving the final form of the Privacy Shield. The Decision entered into force the same day.[4]

The adequacy decision ended, at least for now, a process of negotiation and debate that began after the Snowden revelations in 2013 and culminated in the October 2015 European Court of Justice ("CJEU") *Schrems* decision striking down the Privacy Shield's predecessor, the Safe Harbor.[5] The Privacy Shield, too,

---

1 *See* http://tinyurl.com/jpm3zm6.

2 *See* http://tinyurl.com/hc26oqs.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 *See* EU Commission press release dated July 12, 2016, http://tinyurl.com/jeg3doq.

5 *See* the Debevoise Client Update "Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid," dated October 6, 2015, http://tinyurl.com/hvad4zm, and Debevoise FCPA Update November 2015, http://tinyurl.com/hjzxklk.

could yet face challenges in the CJEU or elsewhere. Subject to that possibility, however, the adequacy decision means that EU personal data can now flow freely from the 28 EU Member States (and the three European Economic Area members, Norway, Liechtenstein and Iceland) to U.S. organizations that self-certify adherence to the Privacy Shield Principles. The Privacy Shield framework will be published in the Federal Register, and the self-certification process with the U.S. Department of Commerce will start on August 1, 2016.[6]

WHAT ARE THE PRIVACY SHIELD PRINCIPLES AS FINALLY ADOPTED?

The following Privacy Shield Principles ("Principles") form the cornerstones of EU data protection compliance for transatlantic data transfers:

- Notice. A participating U.S. organization handling EU personal data must inform individuals about the scope of the organization's participation in the Privacy Shield, the type of personal data collected, the purpose of processing that data, and the individual's access to legal redress.
- Choice. The organization must offer the individual the opportunity to opt out of having their personal information either disclosed to third parties or used for a materially different purpose than that for which the data was originally collected. In the case of sensitive information (medical or health conditions, racial or ethnic origin, etc.), organizations generally must obtain opt-in consent.
- Security. The organization must take reasonable and appropriate security measures to protect personal information from loss, misuse, unauthorized access, etc. Specific security measures are not dictated by the terms of the Privacy Shield.
- Data Integrity and Purpose Limitation. Personal information collected must be limited to that which is relevant for the purposes of the processing. The organization must take reasonable steps to ensure that the personal data collected is reliable for its intended use, accurate, complete and current. Personal information can only be retained as long as it serves the purpose for which it was collected.
- Access. Individuals have the right to access their personal information held by the organization, and the right to correct, amend or delete information that is inaccurate or has been processed in violation of the Principles.

---

6 *See* the U.S. Department of Commerce press release dated July 12, 2016, http://tinyurl.com/zh26mvj.

- Accountability for Onward Transfer. In case of an onward transfer from the self-certifying organization to a third-party controller or an agent, the organization has to contract with the data recipient to provide the same level of protection as under the Shield.
- Recourse, Enforcement and Liability. The organization must provide for a mechanism that assures compliance with the Principles. In the case of human resources data collected in the context of an employment relationship, the organization must commit to cooperate with European data protection authorities and to comply with those authorities' advice.

The Privacy Shield also includes a set of Supplemental Principles, which flesh out the above Principles by specifying such detailed steps as the performance of due diligence and audits, the means of processing of human resources data, and the terms of data processing contracts for onward transfers.

WHAT ROLE WILL THE U.S. GOVERNMENT PLAY?

To obtain the protections of the Privacy Shield, a U.S. organization must self-certify adherence to the U.S. Department of Commerce. Participants must (a) subject themselves to the investigatory and enforcement powers of the U.S. Federal Trade Commission or the U.S. Department of Transportation; (b) publicly declare their commitment to comply with the Principles; (c) publicly disclose a privacy policy consistent with the Principles; and (d) fully implement the Principles. The certification must be renewed annually.

The Principles provide for several carve-outs, providing that a U.S. organization may limit adherence to the Privacy Shield to the extent necessary (a) to meet U.S. national security, public interest, or law enforcement requirements or (b) to comply with U.S. statutes, government regulations, or case law. The organization must indicate in its privacy policy if it expects that exceptions under (b) will apply on a regular basis.

A self-certifying organization's failure to comply can lead to enforcement measures under Section 5 of the Federal Trade Commission Act,[7] which prohibits unfair and deceptive acts, or under other laws or regulations prohibiting such acts.

The Department of Commerce will maintain a public list of U.S. organizations that have self-certified. Privacy Shield protections are assured from the date that the Department places the organization on the list. The Department will remove

[7] 15 U.S.C. § 45(a).

an organization from the list if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification. The Department will also remove organizations that persistently fail to comply with the Principles. Such organizations must return or delete any personal information of European data subjects they received under the Privacy Shield.

WHAT LEGAL REDRESS WILL BE AVAILABLE TO EU DATA SUBJECTS?

EU data subjects who believe that their data has been misused will have several redress possibilities:

- Filing of a complaint with the self-certified organization. Organizations must respond within 45 days of receiving a complaint.
- Use of a free Alternative Dispute Resolution process through an independent ADR provider. The organization will be required to include information in its published privacy policies about the independent dispute resolution body to which European data subjects may address complaints.
- Filing of a complaint with the U.S. Department of Commerce.
- Filing of a complaint with the data subject's "home" data protection authority. The authority will refer the complaint to the U.S. Department of Commerce, which will respond within 90 days, or the Federal Trade Commission, if the Department of Commerce is unable to resolve the matter.
- If a case is not resolved by other means, there will be an arbitration mechanism. Individuals may file a notice to the U.S.-seated Privacy Shield Panel, a dispute resolution body that can issue binding decisions against U.S. self-certified organizations, providing non-monetary equitable relief.
- Individual complaints based on a fear that personal information has been accessed in an unlawful way by U.S. authorities in the area of national security will be handled by an Ombudsperson independent from the U.S. intelligence services.

WHAT ARE THE MAIN DIFFERENCES COMPARED TO SAFE HARBOR?

The Privacy Shield was drafted against the backdrop of perceived shortcomings in the Safe Harbor regime, especially the perception that the Safe Harbor had left European data subjects unduly exposed to U.S. government surveillance. The Privacy Shield addresses these concerns by requiring companies to disclose certain mandatory content in their privacy policies, and by adding obligations for U.S. data importers, including tightened conditions and stricter liability provisions for onward transfers to third parties outside the framework. The

Federal Trade Commission is expected to increase its enforcement efforts against participating companies to counter the argument of prior lax Safe Harbor oversight. The new variety of EU data subjects' accessible and affordable avenues to individual redress also promises greater scrutiny and compliance under the Privacy Shield as compared to Safe Harbor.

IS THE PRIVACY SHIELD STILL SUBJECT TO REVIEW AND CHALLENGE?

Yes, in a number of ways. The European Commission will continuously monitor the functioning of the Privacy Shield. There will also be an annual joint review by the European Commission and the U.S. Department of Commerce, focusing in particular on the safeguards relating to national security access—*i.e.*, the Snowden-inspired concerns, regarding arguably excessive U.S. intelligence access to personal information, that drove the *Schrems* decision. If U.S. organizations or public authorities do not abide by their commitments, then the European Commission can suspend, amend or repeal the Privacy Shield or limit its scope.

The *Schrems* decision leaves open the possibility that a similar legal challenge to the Privacy Shield could emerge in the CJEU. *Schrems* also leaves open that an individual country's data protection authority may seek to question or limit the application of the Privacy Shield to its country's citizens' data. The Article 29 Working Party—a group of representatives of national data protection authorities within the European Union, which has been notably skeptical towards the Privacy Shield thus far—has advised that it will conduct a coordinated analysis of the final form of the Privacy Shield, and will publish a statement as soon as possible.[8]

Also relevant is the new General Data Protection Regulation ("GDPR"),[9] which will replace the current Data Protection Directive on May 25, 2018 as the overall privacy law directly binding within the European Union. Adequacy decisions issued during the life of the Directive will be respected once GDPR comes into force.[10] Nonetheless, the Article 29 Working Party has advised that, once the GDPR enters into force, it will review the adequacy decision regarding the

---

8 *See* Article 29 Working Party press release dated July 1, 2016, http://tinyurl.com/jmyqr7d.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10 *See* Article 45 paragraph 9 GDPR.

Privacy Shield with a view to the higher level of data protection that the GDPR offers.[11]

Time will tell how robust the Privacy Shield proves to be in the face of any of these potential reviews and challenges. For today, the headline news is that U.S. organizations finally have a specific new option for data transfers to replace the Safe Harbor.

* * *

Please do not hesitate to contact us with any questions.

[11] *See* Article 29 Working Party statement dated April 13, 2016, http://tinyurl.com/h9hbd2o.