Digital and data

EU-US Privacy Shield: What you need to know

OLSWANG

What is the US-EU Privacy Shield?

The EU-US Privacy Shield is a replacement arrangement for the previous Safe Harbour Agreement which was held to be invalid in 2015. In February 2016, the European Commission and the United States Government reached a political agreement on this new framework which provides a mechanism to enable the transfer of personal data from entities in the European Union to the US. It is intended to provide a robust new system to protect the personal data of Europeans through safeguards and commitments deemed to be adequate from a European data protection regulatory perspective.

European data rules prevent the transfer of personal data out of the European Economic Area except in certain limited circumstances. The US-EU Privacy Shield is one such permitted circumstance enabling companies to transfer personal data out of the European Economic Area to a Privacy Shield certified entity in the US. However, Privacy Shield does not cover transfers to any country other than the US.

Is it in force yet?

Yes, the European Commission launched Privacy Shield in July 2016 and the US Department of Commerce has started operating it. Certification was opened from 1 August 2016 and some companies, including Microsoft, have already signed up.

Do I have to certify for Privacy Shield if I transfer personal data to the US?

No, it is not a mandatory system. There are other ways to transfer personal data from the European Union to the US in a manner which is compliant with European data protection rules, for example the use of the EU model clauses or binding corporate rules.

What do I need to do if I want to certify?

US entities need to sign up to the framework with the United States Department of Commerce and commit to certain principles. The United States Department of Commerce is responsible for managing and administering the Privacy Shield. In order to become certified, companies must have a privacy policy in line with the Privacy Principles. They must renew their membership to the Privacy Shield on an annual basis. If they do not renew, they can no longer receive and use personal data from the European Union under that framework.

What are the Privacy Shield Principles?

Privacy Shield provides a number of rights to data subjects and companies must protect personal data in line with the principles:

Notice Principle: companies are bound to provide information on data subjects on a number of key elements relating to the processing of their personal data, such as the type of data collected, purpose for the processing of data, rights of access and choice, conditions for onward transfers and liability. Additional safeguards apply, specifically the requirement for companies to make public their privacy policies; and even provide links to the

United States Department of Commerce's website, the Privacy Shield list and the website of an appropriate alternative dispute settlement provider.

Data Integrity and Purpose Limitation Principle: personal data must be limited to what is relevant for the purpose of processing, reliability for its intended use, accuracy, and completion. An organization may not process personal data in a way that is incompatible with the purpose for which it was originally collected or authorised by the data subject.

Choice Principle: this gives data subjects the right to opt out. Special rules allows for Opt out at any time from the use of personal data applicable to direct marketing. In case of sensitive data, companies must normally obtain the data subject's affirmative express consent (Opt in).

Data Integrity and Purpose Limitation Principle: personal information may be retained in a form identifying or rendering an individual identifiable only as long as it serves the purposes for which it was originally collected or authorised.

Security Principle: companies creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures, taking in consideration the risks involved in the processing and the nature of the data. In case of subcontracting the data processing, companies must conclude a contract whereby the processor guarantees the same level of protection as provided under the Principles of Privacy Shield, and even take steps for ensure its implementation.

Access Principle: data subjects have the right, without the need of justification and only against an excessive fee, to obtain from the company, proper confirmation of whether such company is processing personal data related to them and have the data communicated in reasonable time.

Recourse, Enforcement and Liability Principle: companies must provide robust mechanisms to ensure compliance with other principles and recourse for European Union data subjects, whose personal data have been processed in a non-compliant manner, including effective remedies. Companies must also take measures to verify that their published privacy policies conform to the principles and are in fact complied with.

Accountability Principle for Onward Transfer Principle: any onward transfer can only take place for limited and specified purposes, on a basis of a contract, and only if that contract provides the same level of protection as the one guaranteed by the principles, which includes the requirement that the application of the principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes. In application of the choice principle, according to which data subjects must be informed about the type and identity of any third party recipient, the purpose of the onward transfer, as well as the choice offered and the possibility of objecting (Opt out), or in the case of sensitive data, subjects have to give "affirmative express consent" (Opt in) for onward transfers.

Finally, Privacy Shield provides the obligation to provide the same level of protection as required by the principles applied to any and all third parties involved in the processing of the data transferred, irrespective of their location, in the United States or other third country, as well as when the original third party recipient itself transfers those data another third party recipient, for sub-processing purpose.

How is Privacy Shield enforced?

Privacy Shield provides data subjects with different ways to help make a complaint about a company that is possibly using the personal data in an incorrect way or that is not in compliance with the rules:

A. **United States Privacy Shield Company:** a company must provide details of someone data subjects may contact directly for any inquiries or complaints, to which the company must respond in 45 days.

B. **Independent Alternative Dispute body:** this applies in case the Privacy Shield Company has chosen an Alternative Dispute Resolution body as its independent recourse mechanism. The Privacy Shield company's website must provide information and a link to the website of the ADR body.

C. **National Data Protection Authority:** a Privacy Shield company is in principle free to opt for an European Union Data Protection Authority to act as its independent recourse mechanism. However, when a company handles human resources data, submission to the relevant Data Protection Authority oversight is compulsory?.

D. **United States Department of Commerce:** Even if the Data Protection Authority does not have oversight powers over the Privacy Shield company that the complaint is against, it can still refer complaints to the United States Department of Commerce, through a new established dedicated contact point responsible for liaising directly with local Data Protection Authorities.

E. **Federal Trade Commission:** Anyone can still file a complaint directly with the United States Federal Trade Commission under the same complaint system for United States citizens. Similar to the Department of Commerce, the Federal Trade Commission has a dedicated point of contact to liaise with the relevant European Union Data Protection Authority to facilitate referrals and increase cooperation to handle individual complaints.

F. **Privacy Shield Arbitration Panel:** if the complaint is still wholly or partially unresolved after using other mechanisms, data subjects always retain a right to seek redress through the mechanism of binding arbitration.

Finally and worth noting, the Privacy Shield establishes a new mechanism to obtain independent redress in the area of national security: the Ombudsperson Mechanism. The Privacy Shield Ombudsperson is a United States senior official with the United States State Department who is independent from United States intelligence agencies. The Ombudsperson office will ensure complaints are properly investigated and addressed in a timely fashion, and to inform the data subject that relevant United States laws have been complied with, or, if the laws have been violated, that the situation is remedied.

Is the Privacy Shield robust or is it also at risk of being held invalid like safe harbour?

There have already been some challenges to the Privacy Shield arrangements and challenges also in relation to model clauses. More future challenges cannot be ruled out but in practice these could take years to work through as for safe harbour. At the moment, it is a legal and valid mechanism.

Useful Resources

European Commission Factsheet (1 page) http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

European Commission FAQs http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm

Text of European Commission's Adequacy Decision dated 12 July 2016 http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Annexes to the Adequacy Decision http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf

European Commission Communication: Transatlantic Data Flows: Restoring Trust Through Strong Safeguards (February 2016) http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf

Contacts

Elle Todd
Partner
London
+44 20 7067 3105

Dr Andreas Splittgerber
Partner
Munich
+49 89 206028-404

Christian Leuthner
Rechtsanwalt/Associate
Munich
+49 89 206 028-414

Diego Gonzalez Crespo
Paralegal
London
+44 (0) 20 7067 3292

Brussels
+32 2 647 4772

London
+44 20 7067 3000

Madrid
+34 91 187 1920

Munich
+49 89 206 028 400

Paris
+33 1 70 91 87 20

Singapore
+65 6720 8278

Thames Valley
+44 20 7071 7300

OLSWANG

Olswang:
Changing Business

www.olswang.com