EU-U.S. Privacy Shield Now Available:

What impact will it have on personal data transfers?

Authored by: Bart W. Huffman, Alan D. Meneghetti, Mark E. Schreiber and Thomas J. Smedinghoff

August 2016

Beginning on August 1, 2016, U.S. companies have a new way to legally facilitate the transfer of personal data from the European Union to the U.S. Known as the EU-U.S. Privacy Shield, this new agreement between the EU and the U.S. was approved by the European Commission on July 12, 2016. It will facilitate the storage, sharing, retention and use of EU personal data by participating U.S. companies. Effective August 1, 2016, U.S. companies can join the Privacy Shield by self-certifying their compliance with its requirements.

The Privacy Shield promises to "impose stronger obligations on U.S. companies," as well as require greater monitoring by and cooperation between the U.S. and European Data Authorities.

1. What is Privacy Shield?

The EU-U.S. Privacy Shield is a set of principles agreed to by the European Union and the United States to enable U.S. companies that certify compliance with those principles to more easily receive personal data from the EU. It is a replacement for the U.S. – EU Safe Harbor program which was originally established in 2000 and declared invalid by the European Court of Justice in October 2015.

By certifying compliance with the Privacy Shield principles and its other requirements, a U.S. company satisfies the EU legal requirements necessary to receive and process personal data from the EU. A U.S. company also becomes subject to enforcement by the Federal Trade Commission under FTC Act section 5 if it subsequently fails to comply with any of those principles.

2. What Are the Privacy Shield Principles that U.S. Companies must comply with?

To join the privacy Shield, U.S. companies must commit to comply with seven principles governing the handling of personal data received from the EU. While those principles are similar to the principles adopted under the prior Safe Harbor agreement, the compliance obligations under each principle have been significantly expanded. The European Commission recently put out a Guide to the EU-U.S. Privacy Shield, and the Department of Commerce has a Fact Sheet for Interested Participants on its website. The principles are categorized as follows from the Guide:

(1) Notice: "Your Right to be informed"
(2) Choice: "Limitations on the use of your data for different purposes."
(3) Data Integrity and Purpose Limitation: "Data minimization and obligation to keep your data only for the time needed."
(4) Security: Obligation to secure your data.
(5) Accountability for Onward Transfer: "Obligation to protect your data if transferred to another company."
(6) Access: "Your right to access and correct your data."
(7) Recourse, Enforcement and Liability: "Your right to lodge a complaint and obtain a remedy."

U.S. participants must not only agree to adhere to the Privacy Shield principles, they must also reflect certain information in their privacy policies and they must advise EU citizens of their redress and other rights. When a participating U.S. company commits a potential breach under the Privacy Shield framework, the individual will have a number of options to enforce their rights against the company.

3. How Does Privacy Shield Compare with the old Safe Harbor?

The seven Privacy Shield principles are similar to the original seven Safe Harbor principles in name. However, several of the new Privacy Shield principles impose obligations on U.S. companies that go well beyond the obligations of the old Safe Harbor.

One of the core principles that is significantly expanded is the onward transfer principle – now referred to as the "accountability for onward transfer" principle. For example, U.S. companies that want to transfer personal information received from the EU to third-party controllers must now enter into a contract with the transferee (1) providing that the data may only be processed for limited and specified purposes consistent with the consent provided by data subject, and (2) obligating the recipient to provide the same level of protection for the data as required under the Privacy Shield principles. Companies that self-certify under Privacy Shield before October 2016, will have a nine-month window to bring their transfer contracts into compliance with these and other requirements. During this nine-month period individuals will have opt-out rights. After that, all such onward transfer contracts must be compliant at the time of self-certification.

Another core principle undergoing significant changes is the recourse, enforcement, and liability principle. U.S. companies are now required to provide independent recourse mechanisms to resolve complaints and disputes at no charge, commit to binding arbitration at the request of the data subject, and respond promptly to inquiries from the Department of Commerce relating to any disputes.

4. What are the Pros and Cons of Joining Privacy Shield?

- It will facilitate personal data transfers from EU to U.S. entities.
- It will not facilitate personal data transfers from EU to other non-EU countries.
- It will certainly require more work for companies, both in privacy policy changes and back end implementation processes.
- The Privacy Shield undertaking will be rigorous and monitored.
- There is some risk of challenges to the legal validity of Privacy Shield in the future.

The EC has announced that the new arrangement will require the U.S. Department of Commerce "to conduct regular updates and reviews" of all participating companies in the scheme. At the time of writing, we do not know how many companies will participate, although both Microsoft and Google have announced their intention to sign up to the proposal on 1 August 2016. It is highly likely that the U.S. Department of Commerce will require each company to keep updated records of personal data held and produce reports at regular intervals to the Department.

In addition, there are expected to be strict rules on the ability of companies to transfer or forward an individual's personal data to a third party company: the Privacy Shield is a 'self-certifying' mechanism whereby each company that signs up and its third party service providers that process personal data are expected to adhere to all the privacy principles, and the underlying contracts with third parties that process data must impose equivalent protections. The date of compliance for such third party providers, as explained earlier, will depend on the date the company signed up for the Privacy Shield, and whether the company can avail itself of the nine month grace period for those enrolling before 1 October 2016.

Clear safeguards and transparency obligations on U.S. government access

The U.S. has already made several promises (actually, "assurances") to the EU in this area: firstly, the U.S. government will not use transferred data to conduct mass-surveillance of European citizens and, secondly, the access of public authorities for security or legal purposes shall be limited by concepts of "necessity and proportionality." Until the terms of the Privacy Shield are clarified, we will not know exactly what this entails and under what circumstances data can be passed on in the national interest. A reassurance, perhaps, for European citizens is that the data is not to be reviewed on a blanket approach, but rather only used for specific instances or threats.

Another development in this area will be the introduction of a "redress possibility" whereby EU citizens will be protected by an independent ombudsman mechanism; a checks and balances approach which will handle complaints by European data subject. This role was clarified in the recently released, final version of the Privacy Shield.

Effective protection of individual rights

The EC recently published the final version of its "adequacy decision": the purpose being to ensure that the U.S. has an adequate level of data protection (in accordance with existing EU laws) before the Privacy Shield comes into force.

The complaint procedure has sequential ways of resolving a dispute between a U.S. company and an EU data subject, and the Guide has a detailed section on this. Each complaint option should be followed in turn (from 1 through to 6) with the parties only progressing to the next option once all previous options have been fully explored and exhausted:

(1) Firstly, the company will be given an adequate opportunity to resolve the dispute with the EU data subject. Under the proposed guidelines, a company will have 45 days to respond to any complaint made and to offer a resolution.

(2) If the company is unable to resolve the complaint, the individual will be offered Alternative Dispute Resolution (ADR) or independent resource mechanism – this will be designated by the US company and can take place either in the EU or the U.S.

(3) The European national Data Protection Authority (DPA) will then examine the matter, providing a response within 60 days.

(4) If the DPA requires assistance, the matter will be referred to the U.S. Department of Commerce.

(5) The EU data subject is then entitled to request the U.S. Federal Trade Commission to consider granting a consent order, obliging the company to comply with the contents of the order.

(6) If none of the above complaint procedures are effective, a 'last resort' option will be available: a 'Privacy Shield Panel' will be established to handle cases that advance to this last stage and the parties will select a panel of one or three arbitrators from a pool of at least 20 arbitrators appointed by the EC and U.S. Department of Commerce. The task of the Panel will be to hear the dispute in full and make a binding legal decision. The Privacy Shield Panel will have the authority to impose "individual-specific, non- monetary equitable relief" necessary to remedy non-compliance with the principles set out in the Privacy Shield. While the panel will take into account other remedies already obtained by other Privacy Shield mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient.

Naturally, it is hoped that most complaints will be settled at stage 1, with the EC encouraging transparent discussions between the company and EU data subject from the outset.

Annual joint review mechanism

This principle aims to do what it says: monitor and review how effectively the Privacy Shield is operating, both from a company and national government perspective. National intelligence experts from both the U.S. and EU Data Protection Authorities will produce their findings in the form of a public report for the review of the European Parliament and Council. The upcoming implementation of the GDPR, as well as any interim challenges or criticisms, will doubtless impact the annual review process.

The opinion of the European Data Protection Supervisor (EDPS)

In a recent opinion, the EDPS expresses a belief that the Privacy Shield takes important steps forward in establishing a trans-Atlantic framework for the 21st century, as well as resolving the issue of "instantaneous and unpredictable data flows". Firstly, the EDPS is critical of the lack of "safeguards to protect the EU rights of the individual" as well as ignoring the data protection principles that form a fundamental part of union law. Secondly, the EDPS express concerns that self-regulation by private organisations in a "globalized digital world where many countries are now equipped with data protection rules" is dangerously short-term and wrongly discourages "transatlantic dialogue".

Conclusion

As the Privacy Shield proceeds towards active implementation, there will be further instructions and guidance, and companies will begin to work through the implementation stages. The parties remain committed to a more cooperative approach that, on its face, involves a more EU-like framework for processing of data by participating U.S. companies.

ABOUT THE AUTHORS

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com

Bart W. Huffman is Chair of Locke Lord's Privacy and Cybersecurity Practice. He has a systems engineering background and experience in privacy and information security matters that spans the modern history of the practice area. Bart provides advice concerning a wide range of matters within his field, including cybersecurity program development, enterprise cloud computing and other IT services agreements, company policies, information security preparedness, and data breach response. He also has a proven track record in significant online copyright and litigation matters (including representation of some of the largest ISPs in various venues and appellate courts in matters involving Internet subscriber data).

Alan D. Meneghetti
Partner
London
+44 (0) 20 7861 9024
ameneghetti@lockelord.com

Alan D. Meneghetti is a Partner in the London office of Locke Lord LLP where he undertakes a full range of commercial and regulatory work in the general commercial, aviation and aerospace sectors. Alan's practice covers work which ranges from regulatory issues to the procurement of suppliers and responses to tenders, to data protection and privacy, IT, IP, and the drafting and negotiating of various commercial agreements (such as outsourcing, supply, service and R&D agreements). He has worked extensively on matters in Africa, Europe and the United Kingdom.

Mark E. Schreiber
Partner
Boston
617-239-0585
mark.schreiber@lockelord.com

Mark E. Schreiber practice is in cyber security, privacy, employment, and compliance matters, including numerous internal company investigations involving data breaches, health care, anti-kickback, alleged fraud, financial improprieties, and other misconduct. He often advises senior management, boards and special board committees in these cases. He has also handled a variety of multinational and cross-border matters in this context.

Thomas J. Smedinghoff
Of Counsel
Chicago
312-201-2021
tom.smedinghoff@lockelord.com

Thomas J. Smedinghoff is Of Counsel at the Firm, where his practice focuses on the new legal issues relating to the developing field of information law and electronic business activities. Tom is internationally recognized for his leadership in addressing emerging legal issues regarding electronic transactions, identity management, privacy, information security, and online authentication issues from both a transactional and public policy perspective.