Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 3 >>> MARCH 2016

The EU-U.S. Privacy Shield—Challenges and Observations



By Rohan Massey, Heather Sussman and Matthew Coleman

On Feb. 29, 2016, the European Commission (EC) released the full text of the proposed EU-U.S. Privacy Shield agreement (16 WDPR 02, 2/25/16). The agreement sets forth a proposed data protection self-certification framework for companies transferring EU personal data to the U.S. It is the result of lengthy negotiations between the U.S. and the EU seeking to establish an alternative to the Safe Harbor Framework that was invalidated by a decision of the Court of Justice of the European Union (CJEU) in 2015 (15 WDPR 31, 10/23/15). That decision left nearly 4,000 U.S. companies that had previously self-certified to the Safe Harbor as well as thousands more EU companies questioning how to lawfully transfer personal data of European citizens to the U.S. While the Privacy Shield certainly appears to address many of the concerns articulated by the CJEU, the agreement contains many provisions that, when taken together, may lead far fewer companies to sign up for the Privacy Shield than expected.

This article examines the challenges that U.S. and EU regulators encountered in reaching this agreement, the additional privacy protections companies will be re-

Rohan Massey is a partner at Ropes & Gray LLP, London.

Heather Sussman is a partner at Ropes & Gray LLP, Boston.

Matthew Coleman is an associate at Ropes & Gray LLP, Boston.

quired to commit to under the agreement, and those aspects of the Privacy Shield framework that might cause a company previously self-certified under the Safe Harbor to consider alternative mechanisms.

Background

The Privacy Shield 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.* The Principles find a very close analogue in EU data protection law, which is of course by design. The Privacy Shield is intended to bridge the gap between the level of privacy protection afforded to EU citizens within the EU and the level provided under U.S. law. Within the EU, citizens are provided legal protection for their personal data under both their constitutional right to data privacy and the Data Protection Directive (95/46/EC) (DPD), which required all EU Member States to enact an equivalent or stronger data protection law, applicable to all those processing personal data for their own purposes (including all public and private organizations).

The U.S. takes a different approach. Instead of one, all-encompassing *omnibus* law, the U.S. has opted to pass data protection laws based on the nuances of particular contexts where the processing of data may be more sensitive. This *sectoral* approach to legislation has resulted in a patchwork of laws that apply depending on the type of data processed, or the type of business processing the data. This is back-stopped by federal and state consumer protection laws that generally prohibit unfair or deceptive business practices and these laws have routinely been applied to ensure basic privacy and data security protections.

The Privacy Shield imposes several obligations on both certifying entities and the government bodies tasked with oversight of the Privacy Shield that are more stringent than those imposed under Safe Harbor.

Under the DPD, however, personal data is not permitted to be transferred to any country outside of the European Economic Area (EEA) that does not provide an "adequate" level of protection, meaning a legal standard of data protection substantially similar to or stronger than the DPD. The U.S., of course, does not fit into the category of "adequate," which gives rise to the need for a mechanism like Privacy Shield aimed at ensuring an "adequate" level of protection for EU personal data.

Privacy Shield's predecessor—the U.S.-EU Safe Harbor—was invalidated on 6 Oct. 2015 by the CJEU, leaving more than 4,000 companies out of compliance with any legal mechanism to transfer data from the EEA. There are other data transfer mechanisms that may be used to ensure compliance with the adequacy requirements of the DPD, e.g. Standard Contractual Clauses and Binding Corporate Rules (which have extensive operational costs to set up and maintain) and, in other jurisdictions such as the U.K., self-assessed adequacy (which runs the risk of not being found sufficient in some jurisdictions). However, Safe Harbor was a clear favorite as it provided a gateway for all parties to transfer all relevant personal data to the Safe Harbor certified entity.

While the use of the Privacy Shield is voluntary once certified, compliance is compulsory, with failures to comply being enforceable under the Trade Commission Act, unless the company has committed to co-operate with the European Data Protection Authorities.

One of the grounds on which Safe Harbor was invalidated was that it 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. The CJEU found that the U.S. government's alleged processing of personal data was incompatible with the purposes for which it was transferred, disproportionate to the needs of national security, and without any measure of judicial redress available to EU citizens. In the draft of the Privacy Shield agreement released on 29 Feb. 2016, the Commission extensively outlines the checks and balances that limit the U.S. intelligence community, new commitments made by U.S. public officials, and the new remedies made available to EU citizens by virtue of the newly enacted Judicial Redress Act, which provides the same rights of redress to EU citizens as Americans under the Privacy Act of 1974.

The Privacy Shield will come into effect once the EC approves its adequacy decision. For self-certifying companies the Principles will apply upon certification. However, companies that certify to the Privacy Shield in the first two months following it coming into force will have nine months to ensure that all commercial relationships with third parties conform with the Accountability for Onward Transfer Principle. During this interim nine-month period, where the company transfers data to a third party, it must still (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles. While the use of the Privacy Shield is voluntary once certified, compliance is compulsory, with failures to comply being enforceable under the Trade Commission Act prohibiting unfair and deceptive practices unless the company has committed to co-operate with the European Data Protection Authorities (DPAs), in which case their interpretation of compliance will take precedence.

   ISSN 1473-3579

Enhanced Obligations

The Privacy Shield imposes several obligations on both certifying entities and the government bodies tasked with oversight of the Privacy Shield that are more stringent than those imposed under Safe Harbor.

Most notably, the Privacy Shield includes additional obligations surrounding the "onward transfer" of data. For instance, 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 data 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 self-certified company will be responsible and remain liable for the processing of personal data by vendors acting on its behalf, unless the company can prove it was not responsible for the event that led to an individual's complaint.

Furthermore, a self-certified company may only transfer personal data 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 of the personal data and that the recipient will provide a level of protection consistent with the Principles.

There are a number of additional obligations that have no equivalent in the Safe Harbor agreement, including:

- 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.

- To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews. 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.

- Where a self-certified company wishes to transfer human resources-related personal data from the EEA for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims arising out of the processing of such data. In addition, the company must indicate this in its self-certification submission and declare *inter alia* its commitment to cooperate with the EU authority or authorities concerned in conformity with supplemental Principles on HR Data and that it will comply with the advice given by DPAs. The company must also provide the DoC with a copy of its HR privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

- 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 designate 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.

- A self-certified company will be removed from the Privacy Shield List if: it voluntarily withdraws from the Privacy Shield; it fails to complete its annual re-certification; or where it is found to be in persistent breach of the Principles. Once removed the company may no longer benefit from the EC's adequacy decision to receive personal data from the EU, but it must continue to apply the Principles to the personal data it received while it participated in the Privacy Shield, and affirm to the DoC on an annual basis its commitment to do so, for as long as it retains such personal data. However, where removal is for persistent failure to comply with the Principles personal data must be deleted and cannot be retained.

- The EC and DoC data will undertake an annual joint review to monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes, and the EC will issue a public report of its findings to the European Parliament and the Council.

- The EC will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans.

However, there is good news for professional advisors engaged in due diligence, or auditors conducting an audit, as they may process personal data without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of the Principles would prejudice the legitimate interests of the company. Legitimate interests in these circumstances include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions.

Specific Issues Arising With Regard to the Principles

Notice. In addition to the information provided on data collection and use, individuals must be informed in clear and conspicuous language when first asked to pro-

vide personal data of inter alia: the company's processing of personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (i) the panel established by DPAs, (ii) an alternative dispute resolution provider based in the EU, or (iii) an alternative dispute resolution provider based in the U.S.

Choice. Companies must offer individuals a clear, conspicuous, and readily available mechanism to opt out of their personal data, or opt in in relation to sensitive personal data, being disclosed to a third party, other than the company's data processor, or to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals.

Access. Individuals must have access to personal data held about them and be able to correct, amend or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Recourse. The Privacy Shield outlines an EU individual's options to obtain redress for any privacy-related complaint. The options are designed to operate sequentially, with the individual escalating the matter to additional authorities if they are not satisfied with the response they have received.

First, an individual must contact the self-certified company using the company's available feedback mechanism. It is compulsory for the company to provide a feedback mechanism and make it available for no or nominal cost to the individual. With the imposed requirements of an expedient response (45 days), most cases will be directly resolved by the company without any need for outside involvement.

If the individual is not satisfied with the company's response, he or she may seek redress through the independent dispute resolution service. The dispute resolution service is also a compulsory aspect of a company's self-certification. There are a number of independent dispute resolution providers, such as TRUSTe or the Better Business Bureau.

Next, if the dispute resolution provider cannot resolve the complaint, 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 also accept complaints from dispute resolution providers, the DoC and DPAs, and determine whether to conduct an enforcement investigation or proceeding.

The EU DPAs are also 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 the new arbitral model, the "Privacy Shield Panel." The Privacy Shield Panel will consist of a pool of at least 20 arbitrators, of whom the parties may stipulate one or three such arbitrators for a final binding adjudication.

Enforcement and Liability. Unless the self-certified company proves that it is not responsible for the event giving rise to the damage, the company has responsibility and remains liable for the processing of personal data it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf.

Next Steps

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 don't have the right to access the data themselves. Furthermore, it isn't yet clear what steps companies that self-certified under the old Safe Harbor framework must take in order to be compliant with the new rules.

The next step is for the Article 29 Working Party (a group comprised of EU DPAs) to publish its opinion on the EC's proposed agreement, which should happen by 14 April 2016. Afterwards, there will be an extensive process for the agreement to be ratified within the EU, including a comitology procedure from EU Member State representatives, and adoption procedure by the College of the EC. 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 CJEU can find the agreement invalid once it has been ratified.

Reconciling Differences

The question still remains as to whether the Privacy Shield has the support it needs to be sustainable on both sides of the Atlantic. The answer, of course, may depend on who is responding.

The Privacy Shield is a substantial investment in U.S. resources above and beyond what would otherwise be required by law.

U.S. businesses and regulators have similar stakes in the matter. The agreement allows U.S. businesses to conduct commerce and offer services in EU markets and bring data and other resources back to the United States for processing, which makes U.S. businesses more competitive and better able to innovate. Without the agreement, a number of U.S. businesses run the risk of having their data streams from the EU cut unceremoniously if they have not implemented one of the other (arguably more

   ISSN 1473-3579

burdensome), cross-border transfer mechanisms. The agreement very strongly promotes U.S. economic interests.

On the other hand, U.S. businesses and regulators will be the first to point out that the standards within the Privacy Shield agreement are more onerous than any other privacy requirement in the U.S. outside of a regulated industry. In order to comply with the requirements of the Privacy Shield, a company must invest in, among other things, robust policy development and execution, renegotiation of vendor agreements, independent dispute resolution providers and annual checks to ensure it can competently re-certify. Similarly, the U.S. government has committed additional resources to conduct ongoing monitoring, enforcement, and provide redress mechanisms to meet the requirements of the agreement. The Privacy Shield is a substantial investment in U.S. resources above and beyond what would otherwise be required by law.

On the EU side, there is a more significant division of interests. EU DPAs often fall into one of two camps. The first camp appreciates the existence of an agreement like the Privacy Shield because it removes the burden of bringing enforcement action against U.S. based companies. DPAs will have the ability officially under the Privacy Shield to petition the FTC to pursue investigation against companies allegedly in violation of the Privacy Shield. This lowers the operational costs and increases the efficacy of the rules for the EU DPAs.

The second camp believe that any agreement obligating U.S. companies to standards of data protection will not be sufficient unless those standards are the same or stronger than the DPD. Their primary concerns still lie in the U.S. intelligence community's broad ability to collect and use personal data for "national security purposes" and that there is no proportionality to the need to process such data.

The published texts of Privacy Shield and the information provided by lawmakers on both sides of the Atlantic appear to be progress away from the void left by the CJEU's finding of invalidity of Safe Harbor. However, there is still much work to be done to bring the mechanics of the Privacy Shield to life and to ensure that it offers the protection and clarity that many organizations transferring personal data out of Europe are looking for to satisfy current (and proposed) legal requirements. Although legislators on all sides hope that the provisions within the Privacy Shield reflect a more stringent alignment with the DPD than was found under Safe Harbor, there is still concern that the Privacy Shield may be open to similar challenges to those that undermined Safe Harbor from individuals concerned about the protection of their personal data once it leaves Europe.

For organizations that relied on Safe Harbor, the message from the French and German DPAs, who are now taking enforcement action against those that have not yet put in place an alternative mechanism legitimizing international data transfers, is clear: the time to act is now. Unfortunately for those looking to take immediate action, until it is adopted by the EC, the Privacy Shield remains an interesting but future potential alternative that cannot yet be relied upon. If and when it is adopted, the next step will be to see how many companies elect to self-certify. The most likely candidates are large technology companies and other data controllers for whom alternative mechanisms are administratively, politically or technologically infeasible. The remainder will need to seriously consider the cost versus benefit of the enhanced Principles, which in many respects will require certifying companies to go well beyond what a typical EU company has already put in place. Organizations should now consider and determine if the benefits of the Privacy Shield for their business outweigh its burdens when compared to other options for legitimization.