EU-U.S. Privacy Shield formally adopted, set to launch Aug. 1 for U.S. businesses

James J. Giszczak, Dominic A. Paluzzi | Wednesday, July 27, 2016

The European Commission formally adopted the EU-U.S. Privacy Shield on July 12, a framework designed to replace the previously-invalidated Safe Harbor program and to provide companies on both side of the Atlantic with a new mechanism to comply with EU data protection requirements when transferring personal data from the European Economic Area (comprised of all EU member states, plus Norway, Liechtenstein and Iceland) to the United States. In doing so, the European Commission issued an Adequacy Decision, confirming that the United States ensures an adequate level of protection for personal data transferred from the EU/EEA to U.S. organizations that participate in the Privacy Shield framework.

The European Commission's decision comes nearly nine months after the Court of Justice of the European Union (CJEU) struck down the Safe Harbor scheme amid concerns over the absence of adequate rights to judicial redress in the U.S. afforded to EU citizens for misuse of their data and the lack of transparency over the data-gathering activities of U.S. intelligence agencies in relation to EU data. The CJEU ruled that the extent of surveillance uncovered by Edward Snowden's revelations demonstrated that the U.S. did not guarantee an adequate level of protection for European citizens. The CJEU's ruling effectively left thousands of U.S.-based companies with European operations in legal limbo, anxiously scrambling to find alternative ways to legally import and process EU residents' personal data, and introduced new uncertainty regarding the long-term sustainability of other mechanisms such as binding corporate rules and model contractual clauses. The adoption of the Privacy Shield re-opens the door for U.S.-based

companies to once again receive, store, process, use and share personal data originating from the EU/EEA through a simpler mechanism to comply with EU data protection requirements in lieu of using binding corporate rules or model contractual clauses.

The self-certification process

Similar to the Safe Harbor framework, U.S. businesses wishing to import personal data from the EU/EEA under the Privacy Shield will be required to self-certify with the U.S. Department of Commerce on an annual basis that their privacy practices comply with the Privacy Shield principles. **Companies may begin self-certifying on Aug. 1, 2016**.

Companies must also publicly declare their commitment to complying with the Privacy Shield principles, and publicly disclose and fully implement their Privacy Shield compliant privacy policies. It is important to note that these companies must verify that their privacy policy is effective ***prior*** to self-certification. To ensure compliance, organizations must, for example, implement employee training procedures, conduct periodic compliance reviews, and provide means by which any complaints relating to their processing of personal data are dealt with effectively. The Department of Commerce will then maintain and publish an authoritative list of U.S. organizations that have self-certified to the Department of Commerce and declared their commitment to adhere to the framework's principles (the Privacy Shield List), as well as a list of companies that have been removed from the Privacy Shield List because of voluntary withdrawal or persistent failure to comply.

The Department of Commerce has published a guide to self-certification to assist companies as they review the framework and prepare to self-certify, which can be found here.

Key protections afforded by the Privacy Shield

The Privacy Shield was designed to address and improve on the issues raised by the CJEU in its landmark decision handed down last October. Although the Privacy Shield implements certain principles, similar to Safe Harbor, it differs in several respects. The new framework establishes seven Privacy Shield Principles (notice, choice, access, security, onward transfers, data integrity/purpose limitation and redress) and 16 Supplemental Principles, resulting in:

- Stronger obligations on U.S. companies handling personal data
- Defined means of redress available for EU citizens
- Enforcement commitments from U.S. agencies
- Clearer safeguards and transparency obligations imposed on possible access by U.S. government agencies to personal data transferred under the new arrangement
- Continued monitoring of the program itself

STRONG OBLIGATIONS ON U.S. ORGANIZATIONS HANDLING EUROPEANS' PERSONAL DATA

The Privacy Shield imposes strong obligations on companies that transfer EU citizens' data to the U.S. In particular, the Shield provides for regular reviews of companies' data protection practices, stricter conditions for the onward transfer of personal data and restrictions around data retention.

- **New Privacy Shield policy requirements.** A simple statement of participation in the program alone will no longer be acceptable. In addition to providing a declaration of a company's commitment to comply with the Privacy Shield Principles, the company's Privacy Shield policies must include:
  - A link to the Privacy Shield website and a link to the website or complaint submission form of the EU

data protection authority or independent US complaints-handling body appointed to help resolve disputes; and
    - Statements regarding (i) an individual's rights under the program, (ii) which enforcement authority has jurisdiction over the company's compliance with the Privacy Shield framework, (iii) a new arbitration right, (iv) disclosure to public authorities, and (v) the company's liability for non-compliant onward transfers.
- **Heightened restrictions on onward transfers**. The conditions and accountability for onward transfers of data to third parties have been tightened.
    - Privacy Shield-certified companies will be liable for any onward transfer of the data (for example, to an HR service provider) and must revise agreements with any third party recipients to ensure that they adhere to the same privacy safeguards that the certified company has put into place. The requirement to provide the same level of protection as guaranteed by the Privacy Principles applies equally to all parties involved in the processing, even when a third party recipient of personal data transfers such data to another third party (e.g., a sub-processor). The Department of Commerce also has the right to require a company to provide a summary of the company's onward transfer contractual provisions for its review.
    - Privacy Shield certified companies must contractually obligate the third party recipient of personal data to:
        - Notify the certified company if the recipient is unable to apply the same level of protection that the Privacy Shield certified organization has promised to provide (in such instances, the certified company must notify affected individuals); and
        - Delete or de-identify personal information if such information is no longer relevant to the purposes for which it was initially processed.
- **Grace period (exception)**
    - If a U.S. company already has pre-existing commercial relationships with third parties and self-certifies to the Privacy Shield within the first two months of the framework taking effect (i.e., until Sept. 12, 2016), it will be granted a ***nine-month grace period*** to ensure that its contracts with third party processors conform to the new Privacy Shield requirements.
- **Data retention limitations**. Privacy Shield companies may keep personal data only as long as this serves the purpose the data was collected for. Additionally, these program participants must contractually obligate third parties to delete or de-identify personal information if such information is no longer relevant to the purposes for which it was initially processed.

- **Restrictions when leaving the Privacy Shield.** A company leaving the Privacy Shield must delete the information collected under the framework or certify with the Department of Commerce that it will continue to process the information in accordance with the Privacy Shield Principles.

ROBUST OVERSIGHT AND ENFORCEMENT MECHANISMS

The intent behind the Privacy Shield is to transform the oversight system from self-regulating to one that is more responsive and proactive. As discussed above, companies wishing to import personal data from the EU/EEA will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The certification and annual recertification process will remain unchanged, but the Department of Commerce will actively monitor compliance and conduct ongoing audits of program

participants through detailed questionnaires and/or on the basis of specific complaints or other evidence of non-compliance. These reviews could lead to sanctions or removal from the Privacy Shield List by the Department of Commerce in case of non-compliance. Secondly, the Department of Commerce will maintain an updated list of current members and will ensure that U.S. organizations that are no longer registered on the list nonetheless continue to apply the Privacy Shield Principles to EU personal data received when they were registered for as long as they continue to retain such data.

While organizations included on the Privacy Shield List will be subject to "regular and rigorous monitoring" by the Department of Commerce, the Shield's Privacy Principles will be legally binding and enforceable by the FTC under U.S. law, specifically Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." Therefore, any Privacy Shield certified organization that fails to live up to the promises stated in its policy statement will run the risk of having an enforcement action brought against it by the FTC. Any organization that persistently fails to comply with the Privacy Principles will be removed from the Privacy Shield List and will be required to return or destroy any personal data collected under the Privacy Shield. Additionally, the FTC will maintain a "wall of shame" for companies that are subject to FTC or court orders in Privacy Shield cases.

EFFECTIVE PROTECTION OF EU CITIZENS' RIGHTS WITH SEVERAL VIABLE REDRESS MECHANISMS

EU citizens who believe that their data has been misused under the Privacy Shield framework will have access to a number of affordable and accessible dispute resolution mechanisms. These include the right of a data subject to:

- **Lodge a complaint with the U.S. self-certified organization itself**, which must respond to an individual within 45 days.
- **Lodge a complaint directly to an independent dispute resolution body** (i.e., alternative dispute resolution, "ADR") **designated by the U.S. organization to investigate and resolve individual complaints, and to provide recourse free of charge to the individual**, to the extent such complaint cannot be resolved by the organization itself. Participants must include the details of the independent dispute resolution body in their privacy policy and provide a link to the website of that ADR provider.
- **Lodge a complaint to their "home" (local) DPA**, who will then work with the Department of Commerce and/or the FTC to ensure that unresolved complaints are investigated and resolved expeditiously. Both the Department of Commerce and the FTC have committed themselves to work with European DPAs to receive, review, and respond within 90 days to complaints lodged in the EU. In addition, any U.S. self-certifying company handling human resources data from the EU/EEA must comply with any decisions from the competent DPA with respect to this type of data.
- **As a last resort, invoke binding arbitration by the "Privacy Shield Panel,"** which is made up of at least 20 arbitrators designated by the Department of Commerce and the Commission with experience in U.S. privacy- and EU data-protection law. The Panel will be able to take binding decisions against U.S. self-certified companies. Several "consumer-friendly" features (*e.g.*, no cost, possibility to participate by video-conference, free-of-charge translation and interpretation services) ensure that individuals are not discouraged from making use of the Panel.

Additional avenues for judicial redress may be available under the laws of the U.S., which provide for legal remedies under tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

CLEAR SAFEGUARDS AND TRANSPARENCY OBLIGATIONS ON U.S. GOVERNMENT ACCESS

The U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access to personal data by public authorities for national security purposes will be subject to clear limitations, safeguards, and oversight mechanisms. As part of the assurance, the U.S. also affirmed that:

- There will be no indiscriminate or mass surveillance of European citizens' personal data transferred to the U.S. under the Privacy Shield; and
- Bulk data collection may only take place in accordance with specific preconditions and should be as focused as possible, in particular through the use of filters and the requirement to minimize collection of non-pertinent information.

In addition, the U.S. Secretary of State has established an Ombudsperson, independent from U.S. intelligence authorities, to address and resolve complaints from EU individuals if they fear that their personal information has been used unlawfully by U.S. authorities in the area of national security. This redress mechanism will inform the complainant whether the matter has been properly investigated and that either U.S. law has been complied with or, in case of non-compliance, this has been remedied.

ANNUAL JOINT REVIEW MECHANISM / PERIODIC REVIEW OF ADEQUACY FINDING

The European Commission will check periodically on whether the findings relating to the adequacy of the level of protection ensured by the U.S. under the Privacy Shield are still factually and legally justified. In doing so, the Commission and the Department of Commerce – in association with U.S. national intelligence experts and European DPAs – will oversee an annual review of the Privacy Shield to monitor its functioning and to substantiate the commitments and assurances made by the U.S.

The European Commission will issue a public report to the European Parliament and the Council based on the annual joint review and other relevant sources of information. Furthermore, the Commission will hold an annual privacy summit with NGOs and stakeholders on developments in the area of U.S. privacy law and its impact on Europeans.

Is your company considering joining the Privacy Shield? **Click here for 5 ways your U.S. company can prepare**.

Or, to learn more about the Privacy Shield framework, contact one of the data privacy attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi