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 8 >>> AUGUST 2016

The Privacy Shield Gets the Green Light from the European Union

By Aaron Simpson and Anna Pateraki

After a long and twisting diplomatic process, the EU-U.S. Privacy Shield (Privacy Shield or Shield) formally became effective for companies to use on Aug. 1, 2016. The U.S. Department of Commerce has developed a website for the Privacy Shield framework and has announced that it will stop accepting new Safe Harbor framework (Safe Harbor) submissions as of Aug. 1, 2016 and re-certifications as of Oct. 31, 2016. In parallel, the European Commission has updated its website to include the Privacy Shield in its list of European Union adequacy decisions and has published a Guide for citizens explaining their rights and remedies in the context of the Privacy Shield.

Background

Similar to the Safe Harbor before it, the Privacy Shield is a legal mechanism that allows companies in the EU to comply with data transfer restrictions when they transfer personal data to entities in the U.S. that have publicly certified their adherence to the new framework. For a detailed description of Privacy Shield, see Aaron Simpson, "*European Commission Presents EU-U.S. Privacy Shield*," Pratt's Privacy & Cybersecurity Law Report, May 2016.

The Privacy Shield is comprised of seven principles and 16 supplemental principles inspired by EU data protection law that organizations must publicly proclaim their compliance if they intend to certify. The *seven principles* are: (1) Notice; (2) Choice; (3) Accountability for Onward Transfers; (4) Security; (5) Data Integrity and Purpose Limitation; (6) Access; (7) Recourse, Enforcement and Liability. The *16 supplemental principles* are: Sensitive data; Journalistic Exceptions; Secondary Liability; Performing Due Diligence and Conducting Audits; The role of Data Protection Authorities; Self-Certification; Verification; Access; Human Resources Data; Obligatory Contracts for Onward

Transfers; Dispute Resolution and Enforcement; Choice – Timing of Opt-Out; Travel Information; Pharmaceutical and Medical Products; Public Record and Publicly Available Information; Access Requests by Public Authorities.

When compared to its predecessor, the Privacy Shield imposes stricter obligations on companies with respect to onward transfers, redress mechanisms for individuals and data access by public authorities. The framework itself is also subject to enhanced supervision and is intended to result in more enforcement. In order to ensure the framework remains a living and breathing construct, it also includes an annual joint review mechanism by the EU and the U.S. that allows for continual improvements to be made to the framework.

The Privacy Shield was adopted on July 12, 2016, following an adequacy decision by the European Commission . The adequacy decision on the Privacy Shield replaces the EU-U.S. Safe Harbor adequacy decision which was invalidated by the Court of Justice of the EU on Oct. 6, 2015, primarily due to concerns in relation to law enforcement and judicial redress issues. The Privacy Shield is the result of an almost three-year negotiation process between EU and U.S. officials that was initiated in the aftermath of Edward Snowden's revelations in 2013.

The Article 29 Working Party will be focused on the necessity and proportionality of data access requests made by public authorities and the potential impact that such an assessment may have on other data transfer mechanisms.

The Statement of the Article 29 Working Party

On July 26, 2016, the Article 29 Working Party (Working Party) issued a short statement welcoming the improvements made on the Privacy Shield following its nonbinding opinion from April 2016 and outlining its remaining concerns, which include the following:

- **Commercial aspects:** The Working Party believes that further improvements should be made to introduce more specific rules on automated decision-making and a general right to object (according to point 25 of the EU Commission implementing decision on the Privacy Shield, automated decision-making will be re-examined in the course of the first annual joint review). The Working Party also would like to see more clarification on how the Privacy Shield Principles apply to data processors, which was also an issue under the Safe Harbor.

- **Data access by U.S. authorities:** The Working Party states that it expected stricter guarantees concerning the independence and the powers of the Ombudsperson under the Shield. The Ombudsperson is a function intended to sit within the U.S. Department of State. Its mission is to handle complaints and inquiries received from EU individuals regarding access to their commercial data by U.S. intelligence authorities. Furthermore, the Working Party acknowledged the commitment of the U.S. Office of the Director of National Intelligence (ODNI) to avoid mass and indiscriminate personal data collection, but the Working Party remained skeptical given no assurances were provided that the practice would not occur.

Despite these remaining concerns, the Privacy Shield is officially a legally valid data transfer mechanism for EU-U.S. data transfers. Therefore, the statement of the Working Party did not impact the Privacy Shield's implementation as a practical matter. That being said, such statements from the Working Party do have political value, and they likely will impact the annual review process that will be undertaken in accordance with the Shield. In its recent statement, the Working Party committed to await next year's first EU-U.S. joint annual review to further assess the effectiveness of the Shield. In particular, the Working Party will be focused on the necessity and proportionality of data access requests made by public authorities and the potential impact that such an assessment may have on other data transfer mechanisms.

In addition, the regulators participating in the Working Party have committed to proactively assist individuals with lodging complaints against Privacy Shield-certified organizations. The Working Party stated that it will provide guidance to data controllers about their obligations under the Privacy Shield. It also will provide suggestions on the composition of the "EU centralized body" to be created by the Shield to review individuals' law enforcement complaints, as well as the modalities of the joint review mechanism.

Implications for Businesses

For many businesses, the news of the Privacy Shield's formal adoption is a welcome relief. As a practical matter, the obligations for companies wishing to certify to the Shield are similar to the Safe Harbor framework, with a few key differences as described below:

- **Privacy notices:** The Privacy Shield's Notice principle requires companies to provide a privacy notice that includes specifically prescribed content across a range of areas, including with respect to the company's data processing activities, available recourse mechanisms, onward transfers and potential data disclosure to public authorities for national security and law enforcement purposes. Therefore, organizations wishing to join the Privacy Shield should have their privacy policies reviewed and updated as needed.

- **Choice to opt out:** Companies must offer individuals the choice to opt out if they will share personal data with a third party controller or if they use the personal data for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized. Individuals must be provided with clear, conspicuous and readily available mechanisms to opt out. Note that the opt out require-

   ISSN 1473-3579

ment only applies when personal data is being disclosed to a third party who uses the data for its own purposes. It does not apply when personal data is disclosed to an agent processing the data on behalf of the controller as long as an appropriate contract is in place.

- **Onward transfer agreements:** The Privacy Shield requires adherents to implement appropriate onward transfer agreements when personal data received from the EU is transferred onward to either agents (*i.e.*, data processors) or third-party controllers. Such agreements with data controllers should provide that EU personal data may only be processed for limited and specified purposes and that the third-party recipient will provide the same level of protection for the data as is provided by the Privacy Shield Principles. In addition, the Privacy Shield-certified organizations must conduct specific diligence when sharing EU personal data with agents and will need to be prepared to provide a summary or a copy of the relevant onward transfer agreements to the Department of Commerce upon request. Ultimately, the Privacy Shield adherent will remain liable if its agent processes personal data in a manner inconsistent with the Privacy Shield Principles. Therefore, businesses will need to review their onward transfer arrangements to ensure appropriate onward transfer provisions are in place.

- **Withdrawal:** An organization that certifies to the Privacy Shield and subsequently leaves the framework will continue to be bound by its Principles and will continue to be liable for the processing if it keeps and does not return or delete the personal data processed under the Privacy Shield. In such cases, the business is required to affirm to the Department of Commerce on an annual basis its commitment to continue to comply with the Privacy Shield Principles for the retained data for as long as it retains that data.

- **Redress mechanisms:** Organizations are required to establish redress mechanisms provided for in the Privacy Shield. For example, organizations will need to implement a process internally that allows them to review and respond to individuals' complaints within 45 days. In addition, organizations will need to set up an Alternative Dispute Resolution process which will be free of charge for individuals, and be prepared to bear additional costs when redress is sought by other means (such as when individuals lodge complaints with the regulator in their country which will then be forwarded to the Department of Commerce and the Federal Trade Commission in the U.S., or when the binding arbitration of the Privacy Shield Panel is triggered).

Although there is a significant effort that will go into a company's Shield certification to ensure the public representations can be made accurately, organizations that were previously certified to Safe Harbor will be in a relatively advanced position as a relative matter given the similarities between the two frameworks. These companies should be able to leverage their existing Safe Harbor compliance program to certify with the Privacy Shield without upending their current data practices.

Companies should be able to leverage their existing Safe Harbor compliance program to certify with the Privacy Shield without upending their current data practices.

The Role of EU Data Protection Authorities

The Privacy Shield contains a supplemental principle on "The Role of the Data Protection Authorities," according to which companies can select to cooperate with the EU regulators instead of another Alternative Dispute Resolution mechanism. In such cases, the company is required to respond promptly to inquiries from the handling authority designated by the panel of EU Data Protection Authorities (DPAs). This will be an informal panel of EU DPAs created in an effort to ensure a harmonized approach. The EU panel will provide advice to the U.S. organizations concerning unresolved complaints from individuals. It is not yet clear what the composition of the EU panel will look like, however, failure to comply with the advice of the EU panel can trigger enforcement by the Federal Trade Commission.

Overall, EU DPAs will be substantially involved in the monitoring of the Privacy Shield and in assisting individuals with lodging complaints. Individuals can always complain directly to their national DPA who will cooperate with the Department of Commerce and the Federal Trade Commission. Also, the EU DPAs are expected to play a significant role in the context of the Ombudsperson mechanism for reviewing complaints relating to law enforcement operations. As complaints from individuals steadily increase in number, enforcement by EU DPAs will also most likely increase in the future. It is expected that organizations will be subject to significantly more scrutiny and enforcement in the context of the Privacy Shield than they experienced under Safe Harbor.

Outlook

Although further tweaks and improvements will inevitably result from the annual review process, the Privacy Shield is officially a valid legal mechanism for EU-U.S. data transfers. Despite the remaining concerns of the Working Party, depending on a company's data flows, the Privacy Shield can be implemented by companies subject to the Federal Trade Commission's unfair competition authority either alone or in combination with other data transfer mechanisms.

It cannot be excluded that the Privacy Shield will be challenged before regulators or courts, however, the same is true for other data transfer mechanisms. Taken together, the challenges to data transfer mechanisms appear more focused on the foundational questions associated with cross-border data transfers generally and less focused on the specifics of a particular data transfer mechanism. Despite these ongoing challenges, the Pri-

vacy Shield's recent adoption constitutes a step in the right direction for both businesses and their customers and employees.

  WDPR ISSN 1473-3579

  WDPR ISSN 1473-3579