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. The U.S. Department of Commerce developed a framework that allows companies to certify compliance with the new Safe Harbor requirements after the U.S. District Court for the District of Columbia ruled that the previous Safe Harbor program did not provide adequate protections for personal data.

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) Resolution, 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; and Transparency.

For the latest updates, visit www.bna.com
The Privacy Shield is a framework between the EU and the U.S. that allows for continual improvement. It includes an annual joint review mechanism, making it possible for individuals to opt out if they will share personal data. The framework also includes a general right to object, according to a recent opinion of the European Commission that further improves the framework.

Despite these remaining concerns, the Privacy Shield is still a legally valid data transfer mechanism to EU-U.S. data transfers. Therefore, the statement of the Working Party did not impact the Privacy Shield's implementation in a practical manner. This being said, the Working Party’s statements from the Working Party are likely to have political implications for businesses that do not comply with the Privacy Shield.

The Working Party did not impact the Privacy Shield’s implementation in a practical manner. This being said, the Working Party’s statements from the Working Party are likely to have political implications for businesses that do not comply with the Privacy Shield.

Companies must offer individuals access to data that is collected from them. However, the Privacy Shield’s Notice principle requires companies to provide a privacy notice that includes specifically prescribed content as a basis for onward transfers and potential data disclosures, but the Working Party acknowledged that this information may not be required by U.S. data protection authorities.

The Working Party is expected to focus on the successor and possibility of data access requests made by public authorities and the potential impact that such an assessment may have on other data transfer mechanisms. The Working Party’s decision is expected to have implications for businesses, particularly those in the financial services sector.
Onward transfer agreements:

- **Organon transfer agreements:** The Privacy Shield requires adherence to appropriate onward transfer agreements when personal data received from the EU is transferred onward to either agents or third parties. These agreements should include provisions to ensure that onward transfers are made to organizations that are similarly advanced in their protection of personal data. These agreements are subject to the relevant local laws and regulations of the third country where the onward transfer is taking place.

- **Redress mechanisms:** EU personal data may only be processed for limited and specified purposes and that the third party reciprocates and will provide the same level of protection for the data as is provided by the Privacy Shield Principle. Therefore, organizations will need to review their onward transfer arrangements to ensure appropriate onward transfer provisions are in place.

- **Within EU:** An organization that certifies to the Privacy Shield and subsequently leaves the framework, must continue to be bound by its Principles and will continue to be liable for the processing if it keeps and processes EU personal 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 receive complaints, provide a summary or a copy of the relevant onward transfer agreement, and respond to any onward transfer challenges. In such cases, the company is required to respond promptly to inquiries from the Department of Commerce and the Federal Trade Commission, depending on a company's data flows, subject to the Federal Trade Commission's unfair competition jurisdiction. The Privacy Shield contains a supplemental principle on the role of the Data Protection Authorities.

- **Alternative Dispute Resolution:** The Privacy Shield contains a supplemental principle on the role of the Data Protection Authorities (DPAs). This will be an informal mechanism for reviewing complaints relating to law enforcement operations. As complaints from individuals can always be made directly to their own national DPA, individuals can always complain directly to their own national DPA who will cooperate with the Department of Commerce and the Federal Trade Commission 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 Department of Commerce and the Federal Trade Commission, depending on a company's data flows, subject to the Federal Trade Commission's unfair competition jurisdiction. The Privacy Shield contains a supplemental principle on the role of the Data Protection Authorities (DPAs). This will be an informal mechanism for reviewing complaints relating to law enforcement operations. As complaints from individuals can always be made directly to their own national DPA, individuals can always complain directly to their own national DPA who will cooperate with the Department of Commerce and the Federal Trade Commission 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 Department of Commerce and the Federal Trade Commission, depending on a company's data flows, subject to the Federal Trade Commission's unfair competition jurisdiction.

- **Within EU:** An organization that certifies to the Privacy Shield and subsequently leaves the framework, must continue to be bound by its Principles and will continue to be liable for the processing if it keeps and processes EU personal data for as long as it retains that data.

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 refer 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 Department of Commerce and the Federal Trade Commission, depending on a company's data flows, subject to the Federal Trade Commission's unfair competition jurisdiction. The Privacy Shield contains a supplemental principle on the role of the Data Protection Authorities (DPAs). This will be an informal mechanism for reviewing complaints relating to law enforcement operations. As complaints from individuals can always be made directly to their own national DPA, individuals can always complain directly to their own national DPA who will cooperate with the Department of Commerce and the Federal Trade Commission 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 Department of Commerce and the Federal Trade Commission, depending on a company's data flows, subject to the Federal Trade Commission's unfair competition jurisdiction.

Outlook

Although the legal and regulatory裎程成熟, the Privacy Shield will be subject to significantly more scrutiny and enforcement in the context of the Privacy Shield than they experienced under Safe Harbor.
vacancy Shield’s recent adoption constitutes a step in the right direction for both businesses and their customers and employees.