GT GreenbergTraurig

Privacy & Cybersecurity | Alert

March 2016

Details of EU-U.S. Privacy Shield Revealed – What Does the Future of Transatlantic Data Transfer Look Like?

On Feb. 29, 2016, the EU Commission and the U.S. government published the long-awaited legal documentation that will put in place the new EU–U.S. Privacy Shield. Once enacted, the EU–U.S. Privacy Shield will replace the former Safe Harbor regime for the transfer of personal data from the EU[1] to the U.S., which the **Court of Justice of the European Union (CJEU) previously invalidated Oct. 5, 2015**.

The new 132 page documentation follows a **joint announcement by the EU Commission and the U.S. Department of Commerce** made Feb. 2, 2016, that an agreement on the new data transfer framework had been reached. While the announcement stayed short on details of the new Privacy Shield program, such details have now been revealed in these documents so that an in-depth analysis can now be made on how personal data may in the future be transferred from the EU to the U.S. The key points of the future Privacy Shield are as follows:

Self-Certification and Commitment to Privacy Principles

U.S. companies that wish to receive personal data from the EU under the Privacy Shield would have to register with the **Privacy Shield List** and commit to comply with **seven Privacy Principles**:

1. **Notice Principle** - Companies would be required to provide certain mandatory information to data subjects relating to the processing of their data, and to make their privacy policy public.

2. **Choice Principle** – Data subjects would have the ability to object to the disclosure of their personal data

[1] In fact, the same applies to the other member states of the EEA, which, in addition to the EU member states, also includes Norway, Iceland, and Liechtenstein.

to third parties, and to the use of their data for materially different purposes.

3. **Security Principle** – Companies would be obliged to take reasonable and appropriate security measures. In the case of sub-processing, a contract would have to be entered into with the sub-processor that would guarantee the same level of protection.

4. **Data Integrity and Purpose Limitation Principle** – Personal data processed would be limited to what is relevant for the purpose of the processing and its intended use, and must also be accurate, complete, and concurrent. The data may not be processed if the processing is incompatible with the purpose for which it was collected, or for which it was authorized by the data subject.

5. **Access Principle** – Data subjects would have the right to obtain from the company confirmation on whether it is processing data that is relevant to them, and will have the opportunity to correct, amend, or delete personal information where it is inaccurate, or where it has been processed in violation of the Privacy Principles.

6. **Accountability for Onward Transfer** – The onward transfer of personal data would only be permissible for limited and specified purposes, and only on the basis of a contract that provides the same level of protection as the one guaranteed by the Privacy Principles.

7. **Recourse, Enforcement, and Liability Principle** – Companies would be required to annually re-certify their participation in the Privacy Shield framework and take measures to verify that their published privacy policies conform to the Privacy Principles.

The Privacy Shield List will be administered by the U.S. Department of Commerce and will be available to the public. The Department of Commerce will also maintain a public list of organizations that have been removed from the Privacy Shield List, and provide a link to Privacy Shield-related FTC cases maintained on the FTC website.

Compliance Review and Complaint Handling

The Privacy Shield will provide several mechanisms to ensure compliance by U.S. self-certified companies with the Privacy Principles. These would include oversight and enforcement through the Department of Commerce and the FTC. In addition, EU data subjects would have the possibility to lodge complaints and have these complaints resolved. The details include:

- Upon receipt of a complaint by an EU data subject, the company must, within a period of 45 days, provide a response.

- Companies must designate an independent dispute resolution body to investigate and resolve individual complaints, and to provide appropriate recourse.

- The Department of Commerce will verify that the company's privacy policies conform to the Principles.

- The FTC will give priority consideration to certain instances of noncompliance with the Privacy Principle to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive practices has been violated.

- Where a National Data Protection Authority investigates a complaint regarding noncompliance with the Privacy Principles, companies are obliged to cooperate if the complaint concerns the processing of HR

employment data.

- As a recourse mechanism of "last resort," the EU data subject may invoke binding arbitration by a Privacy Shield Panel.

Access of Personal Data by U.S. Public Authorities and Redress Mechanisms

Access by public authorities for **law enforcement, national security, and other public interest purposes** shall be subject to **limitations, safeguards, and oversight mechanisms**. In addition, a redress mechanism shall be established for EU data subjects in the area of national security through an **Ombudsperson** who will be independent from the national security authorities. The Ombudsperson will follow up on complaints and inquiries made by EU individuals regarding national security access to their data.

Next steps

The Privacy Shield can only enter into effect if the EU College of Commissioners adopts a so-called **Adequacy Decision** by which they confirm that personal data that is transferred to the U.S. under the Privacy Shield will have an "adequate level of protection."

A first draft of the **Decision** was already published on Feb. 29, 2016, and is now to be reviewed by the Article 29 Working Party – an umbrella organization that encompasses the Data Protection Commissioners of the 31 EEA Member States. A Committee composed of representatives of the EU Member States will also be consulted. However, neither the Article 29 Working Party, nor the EU Member States Committee, nor the EU Parliament need to consent to the Decision, so it appears to be more a question of *when* than of *if* the Privacy Shield will enter into effect.

Companies should therefore not lose any time and consult with their counsel in order to start taking the necessary steps to be in a position to join the new framework as soon as it is in place.

This *GT Alert* was prepared by **Dr. Viola Bensinger** and **Françoise Gilbert**. Questions about this information can be directed to:

- Dr. Viola Bensinger | Berlin | +49 (0) 30 700 171 150 | viola.bensinger@gtlaw.com
- Françoise Gilbert | Silicon Valley | +1 650.804.1235 | gilbertf@gtlaw.com
- Ian C. Ballon | Silicon Valley/Los Angeles | +1 650.289.7881 | ballon@gtlaw.com
- Luke Dixon | London | +44 (0) 203 349 8756 | dixonl@gtmlaw.com
- Lori S. Nugent | Dallas | +1 214.665.3630 | nugentl@gtlaw.com
- Radboud Ribbert | Amsterdam | +31 (0) 20 301 7333 | ribbertr@eu.gtlaw.com
- Elizabeth C. Rogers | Austin | +1 512.320.7256 | rogersel@gtlaw.com
- Alan N. Sutin | New York | +1 212.801.9286 | sutina@gtlaw.com
- Or your Greenberg Traurig attorney

Albany
+1 518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+1 82-2-369-1000

Shanghai
+86 21 6391 6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+972 (0) 3.636.6000

Tokyo¤
+81 (0)3 4510 2200

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900