WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Privacy Shield Details Unveiled

March 3, 2016

AUTHORS

Daniel K. Alvarez | **Dr. Christian Rolf**

Following up on the announcement of the EU-U.S. Privacy Shield agreement that we detailed in our February 2, 2015 Client Memo, officials from the European Commission earlier this week released a set of documents, including a draft adequacy decision, setting forth the details of the new EU-U.S. Privacy Shield regime. While the framework still has to work its way through additional review and approval processes on both sides of the Atlantic, the released documents give companies more information about what requirements will attach to use of the Privacy Shield for EU-U.S. data transfers. Below, we provide a broad overview of the details provided in these documents, and our initial take on steps companies should take now that this information is public.

Privacy Principles for Companies Participating in Privacy Shield

The 34-page draft adequacy decision reveals a privacy regime that is significantly different from the EU-U.S. Safe Harbor regime that was invalidated by the European Court of Justice on October 6, 2015. While most of the decision is focused on access to information by U.S. public authorities, here we will focus primarily on the new requirements that will apply to companies that choose to participate in Privacy Shield.

In particular, companies that participate in Privacy Shield will have to commit to abiding by seven principles set forth in the adequacy decision (the "Privacy Principles"):

- Notice Principle. Under this principle, companies must provide consumers with information relating to the processing of personal data (e.g., type of data collected, purpose of processing, right of access and choice, potential transfer conditions, etc.). Companies must have a publicly available privacy policy that both reflects their commitment to the Privacy Principles and provides links to the Department of Commerce's website, a new "Privacy Shield List" that will be established as part of the new regime, and the website of an appropriate alternative dispute settlement provider.

- Choice Principle. Consumers must be able to opt out of any sharing of their personal data with a third party (other than an agent acting on behalf of the company) or any use of their data for a "materially different" purpose. Also, companies must obtain affirmative express consent (i.e., consumers must opt in) for sharing or materially different use of sensitive data.

- Security Principle. Companies creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures that account for the risks related to the processing and nature of the data.

- Data Integrity and Purpose Limitation Principle. Personal data collected by companies must be relevant, reliable, accurate, complete and current.

- Access Principle. Consumers have the right to obtain confirmation of whether a company is collecting personal data related to them and to see that data within a reasonable timeframe. This right may be restricted only in exceptional circumstances. Further, consumers must be able to correct, amend or delete personal information where it is inaccurate or collected in violation of the Privacy Principles.

- Accountability for Onward Transfer Principle. Any transfer of a consumer's personal data from a company to a different controller or processor can take place only where the transfer is (i) for limited and specified purposes, and (ii) on the basis of a contract (or comparable arrangement) that provides for the same level of protection as that guaranteed by the Privacy Principles.

- Recourse, Enforcement and Liability Principle. Participating companies must provide robust mechanisms to ensure compliance with the Privacy Principles and recourse – including appropriate remedies – for EU data subjects whose personal data have been processed in a non-compliant manner.

Enforcement

As reflected in the last principle above, enforcement is a critical component of the Privacy Shield regime. The EC draft adequacy decision discusses at length what companies need to do to comply with this principle.

- Under the Privacy Shield regime, EU data subjects may pursue cases of non-compliance directly with the companies that hold their information. To comply with the Privacy Shield regime, companies must implement an effective mechanism to deal with such complaints. For example, companies must include in their privacy policies clear notice informing consumers about a point of contact, either within or outside the company, that will handle complaints (including any relevant establishment in the EU that can respond to inquiries or complaints).

- Companies also must designate an independent dispute resolution body (in either the United States or the EU) to investigate and resolve individual complaints.

- As part of a company's certification (and recertification), the Department of Commerce will verify that the company's privacy policies conform to the Privacy Principles and will maintain an updated list of participating organizations. More generally, the Department of Commerce will be significantly increasing its enforcement and monitoring capabilities to perform its role under the Privacy Shield.

- The Federal Trade Commission will give priority consideration to complaints implicating the Privacy Principles received from the independent dispute resolution or self-regulatory bodies appointed by the different companies, the Department of Commerce, and EU national data protection authorities ("DPAs") to determine whether Section 5 of the FTC Act has been violated.

- Companies are obligated to cooperate in the investigation and resolution of any complaints pursued by EU national DPAs that concern processing of human resources data collected in the context of an employment relationship, or if the companies have voluntarily submitted to oversight by the DPAs.

- Finally, if no other available avenue of redress has satisfactorily resolved the EU data subject's complaint, the individual may invoke binding arbitration by a newly established "Privacy Shield Panel."

Next Steps

As mentioned above, there are a number of steps that must be taken before the Privacy Shield regime is fully in effect. For example, the Article 29 Working Group has to review the documents and issue its non-binding opinion, which likely will come in April. As a result, companies still have time to consider the potential implications for their businesses and weigh the costs and benefits of participating in Privacy Shield and other alternatives we have previously outlined for EU to U.S. data transfers. Part of that calculation likely should include Privacy Shield's chances of success when the inevitable

court challenges come; despite the robust data protection requirements and review mechanisms included in the regime, a number of critics already have focused on perceived loopholes to cast doubt on whether the agreement satisfies EU law.

Meanwhile, the EU national DPAs, including the German DPA, are currently not engaging companies that use alternatives to the invalidated Safe Harbor regime for the data transfer to the United States. However, the German DPA has made clear that continuing to rely solely on Safe Harbor is no longer an option, and has launched enforcement action against companies still relying solely on Safe Harbor.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Dr. Christian Rolf (+49-69-79302-151, crolf@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

March 3, 2016