EU-US PRIVACY SHIELD RELEASED

Date: 1 March 2016

Public Policy & Law Alert

By: Bruce J. Heiman, Ignasi Guardans, Etienne Drouard, Michael J. O'Neil

PRIVACY SHIELD RELEASED.

On February 29, following an earlier February 2 announcement, but with few details, the U.S. Secretary of Commerce released letters to the European Commission setting forth the EU-U.S. Privacy Shield Principles along with undertakings of different U.S. government agencies — the Departments of Commerce, Transportation (DOT), State, and Justice; the Federal Trade Commission (FTC); and the Office of the Director of National Intelligence — to enforce and implement them. The Privacy Shield is a new transatlantic framework for data sharing intended to replace the EU-U.S. Safe Harbor Agreement struck down by the European Court of Justice on October 6, 2015, in the *Schrems* case. U.S. companies adhering to the EU-U.S. Privacy Shield will be able to receive, store, and use personal data from Europe according to its terms.

KEY ELEMENTS.

First, the EU-U.S. Privacy Shield Principles set out the key requirements a company must meet in terms of assuring that U.S. protections of European personal data will be essentially equivalent to that provided in Europe. The Privacy Shield maintains the self-certification regime previously established for the Safe Harbor, but with clearer obligations on companies, annual recertification, and enhanced complaint resolution (enforcement). The key requirements are:

- Notice – disclosure of the types of data the company collects and the purpose for that collection, the third parties to which it may disclose that data, and how individuals can file complaints in the European Union or United States;
- Choice – a requirement to afford clear, conspicuous, and readily available means to opt out or opt in, depending on the nature of the data involved;
- Accountability for onward transfer – i.e., the use of third-party processors;
- Security – the obligation to use reasonable and appropriate measures to protect data;
- Data integrity and purpose – the obligation to limit data collection to specified purposes;
- Access – an individual's right to access and correct, amend, or delete that data;
- Recourse – complaints must be investigated and expeditiously resolved at no cost to the individual;

- Enforcement – government follow-up must occur to assure companies adhere to their assertions; and
- Liability – sufficiently rigorous sanctions must be administered to ensure compliance.

Second, letters from the federal agencies that will enforce Privacy Shield obligations on companies set out the means by which those agencies will administer the protections set forth in the Privacy Shield Principles. They include:

- Requirements that companies certifying under the Privacy Shield publish their privacy policies, establish independent recourse mechanisms, and respond promptly to individual complaints, at no cost to the individual;
- Regular channels of communication between EU Data Protection Agencies and U.S. agencies to communicate individual complaints from the European Union;
- Requirements that U.S. agencies, e.g., FTC and DOT, assert their enforcement jurisdiction and promptly resolve complaints that are not satisfied under the company process;
- Requirements for binding arbitration in the event that U.S. agency enforcement is not effective;
- Requirements for annual recertification by companies participating in the Privacy Shield;
- Requirements that U.S. agencies provide sufficient resources to promptly follow up on individual complaints, maintain accurate Privacy Shield lists, and ensure the certifying companies are, in fact, compliant; and
- Annual reviews by the EU and U.S. authorities to ensure effective enforcement of the Privacy Shield Principles.

Third, the Privacy Shield Principles also establish greater restraints on U.S. government access to information of EU individuals — directly addressing the complaint of the European Court of Justice in the *Schrems* case about widespread and indiscriminate surveillance:

- Appointment of a Privacy Shield Ombudsman at the State Department to address requests from EU individuals relating to U.S. signals intelligence;
- A description of how the U.S. intelligence signals collection process works, including an explanation of why no non-U.S. person should be subjected to indiscriminate mass surveillance; and
- Detailed explanations and descriptions of additional legal remedies that EU individuals may exercise under U.S. law.

What Comes Next? The European Commission has formally posted the Privacy Shield proposal. To implement it, however, the European Commission must issue a so-called adequacy decision with respect to the Privacy Shield, i.e., that it provides an adequate level of protection of personal data by reason of U.S. law or commitments. This determination would replace that originally issued with respect to the EU-U.S. Safe Harbor.

Before the European Commission can act, however, three bodies will opine on the merits of such an adequacy determination. The group of national Data Protection Authorities, the Article 29 Working Party, will issue an opinion. So too will the Article 31 Committee, made up of representatives of each EU member state. Finally, the

European Parliament will be heard, although a vote taken by the European Parliament is not necessarily binding or required. Once each of these organizations has spoken, the European Commission can issue the adequacy determination, which must be approved by the College of Commissioners, i.e., all EU Commissioners. Estimates are that this process will take several months. Fortunately, the head of the Article 29 Working Party has suggested that enforcement will essentially be suspended during this time (i.e., through April).

Here in the United States, given the recent enactment of the Judicial Redress Act, implementation will require adoption of monitoring mechanisms, enforcement procedures, an arbitration process, and the organization of the office of an ombudsman appointed within the State Department.

Will The Privacy Shield Stand? We expect that the adequacy determination will be made by the European Commission. At that point, U.S. companies will need to make any necessary adjustments in order to accede to the new EU-U.S. Privacy Shield.

A number of privacy advocates have already been discussing potential challenges to the Privacy Shield before the European Court of Justice. Perfecting a legal strategy and getting to the European Court of Justice could take several years. Also, the Privacy Shield must undergo annual EU-U.S. reviews during that time and could be modified or even cancelled if the European Commission is unhappy with its implementation and enforcement. It could also be challenged by EU Data Protection Authorities, which retain the power to investigate EU data controllers sharing data with U.S. companies that accede to the EU-U.S. Privacy Shield.

We can help ensure your successful compliance with the new regime. Please contact any of the attorneys listed for further information or assistance.

KEY CONTACTS

BRUCE J. HEIMAN
PARTNER

WASHINGTON DC
+1.202.661.3935
BRUCE.HEIMAN@KLGATES.COM

