PRIVACY AND DATA SECURITY ALERT

JULY 12, 2016

SHOOK
HARDY & BACON

EUROPEAN COMMISSION ADOPTS EU-U.S. PRIVACY SHIELD FOR TRANSATLANTIC DATA FLOWS

U.S. companies are nearer to having another lawful basis for transferring personal data across the Atlantic that is administratively easier to implement and manage. After the October 6, 2015, European Court of Justice ruling invalidating the Safe Harbor framework for personal data transfers from the European Union to the United States, businesses could no longer rely on a uniform mechanism for legally carrying out such transfers. Instead, U.S. companies had to look to other alternatives, such as obtaining consent from individuals or implementing Standard Contractual Clauses for each set of transfers, in order to comply with laws in the EU. Today, the EU Commission formally adopted its adequacy[1] decision on Privacy Shield, which is set to become operational on August 1, 2016.

Like Safe Harbor, Privacy Shield relies on seven principles for data protection. But unlike Safe Harbor, Privacy Shield includes stronger obligations on companies under several of these principles, as described below:

- *Notice*—Companies must notify individuals about data handling practices and international transfers. Under Safe Harbor, companies had to notify individuals of the purposes for data collection and use, how to contact the company, the types of third parties to which personal information was disclosed, and the individual's choices and means for exercising those choices. Privacy Shield imposes additional notification requirements, including disclosure of the type of data collected, the entities or subsidiaries of the company adhering to the Principles, the right of individuals to access their information, the designated independent dispute resolution body, being subject to enforcement by the Federal Trade Commission, U.S. Department of Transportation, or other authorized agency, the

1 Under the 1995 EU Data Protection Directive (95/46/EC), personal data (defined as data about an identified or identifiable individual) can be transferred to another country where that country ensures "adequate" protection of the data. The EU Commission's decision sets forth its determination that the Privacy Shield framework provides "adequate" protection of data transferred from the European Union to the United States.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Camila Tobón
dd 303.285.5318
mtobón@shb.com

Al Saikali
dd 305.960.6923
asaikali@shb.com

possibility for individuals to invoke binding arbitration under certain conditions, the requirement to disclose data in response to lawful requests by public authorities, and conditions for onward transfer to third parties. Companies are also specifically required to make their policies public and provide a link to, or the web address for, the Privacy Shield list.

- *Choice*—Individuals have the ability to opt out of disclosure of their information to third parties or processing for a purpose other than the one for which the information was provided. This principle remains largely unchanged with Privacy Shield.
- *Security*—Companies must take reasonable and appropriate measures to protect personal information. This principle remains largely unchanged with Privacy Shield.
- *Data integrity and purpose limitation*—Personal data must be limited to that which is relevant for the purpose of processing and reliable for its intended use. Privacy Shield changes the prior framework by requiring companies to continue to apply the Privacy Shield Principles to the data transferred under the program when they cease to self-certify, otherwise they will have to delete the data. Privacy Shield now also includes specific data retention requirements. Personal data can be retained in a form that identifies the individual (or makes the individual identifiable) only for as long as it serves a purpose that is compatible with that for which the information was collected or subsequently authorized by the individual.
- *Access*—Individuals have the right to know whether companies are processing their personal information and this right can be restricted only where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would be violated. In addition, individuals must be able to correct, amend, or delete personal information where it is inaccurate or where it has been processed in violation of the Principles. This principle remains largely unchanged with Privacy Shield.
- *Accountability for onward transfer*—As with Safe Harbor, companies must apply the notice and choice principles to the onward transfer and must ensure that third parties to which they

transfer personal information provide adequate protections for the data. Under Privacy Shield, companies are specifically required to enter into agreements with those third parties in order to pass on the obligations under the Principles. Furthermore, those third parties must notify the company if they determine that they can no longer provide the same level of protection as the Principles and the contract must specify that when this determination is made, the third party will cease processing or take steps to remediate.

- *Recourse, enforcement, and liability*—There must be a readily available independent recourse mechanism to ensure compliance with the privacy principles. Privacy Shield expands the options available to individuals to enforce their rights. Companies must timely respond to individual complaints, or cooperate in the investigation of complaints made by individuals in the EU to their home data protection authority. There is still an alternative dispute resolution mechanism, but there is now also a Privacy Shield arbitration panel. Finally, under the Judicial Redress Act (which was signed into law in February of this year), citizens from designated countries will be allowed to enforce their data protection rights in U.S. courts.

Privacy Shield also includes assurances from the U.S. government about limitations on access to personal information by government agencies and creates an Ombudsperson role to oversee investigations of EU citizen complaints about U.S. government surveillance. Finally, Privacy Shield will be reviewed annually by a joint coalition including the U.S. Department of Commerce, Federal Trade Commission, EU Commission, and interested data protection authorities in the EU and other stakeholders.

Companies looking to rely on Privacy Shield will have to review their privacy and data handling policies and procedures and determine whether modifications need to be made to become compliant with the program's requirements. The next step is to begin the self-certification process, which will be available to U.S. companies beginning August 1, 2016.

For more information on the EU – U.S. Privacy Shield, please contact Camila Tobón, Director of Shook's International Data Privacy Task Force, at mtóbon@shb.com or (303) 285-5318.

DISCLAIMER

This information is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

The choice of a lawyer is an important decision and should not be soley upon advertisements.

For more information about privacy and data security law, please visit Al Saikali's blog.