BDO KNOWS:
DATA PRIVACY

SUBJECT
NEW RULES GOVERNING DATA FLOW BETWEEN THE U.S. AND THE EUROPEAN UNION

SUMMARY

Last October, a European Court of Justice (CJEU) ruling abruptly invalidated the 15-year-old U.S.-E.U. Safe Harbor Framework for transatlantic transfers of personal data. The invalidation of Safe Harbor left thousands of companies in legal limbo. After missing the initial deadline, the E.U. and the U.S. came to an agreement on a new framework on Feb. 2, 2016, announcing the E.U.-U.S. Privacy Shield. Adoption of the Privacy Shield was contingent upon the outcome of the European Commission (EC)'s decision on whether the Privacy Shield provided an adequate level of protection under E.U. data protection law.

On July 12, the EC determined that the United States does indeed ensure an adequate level of protection for personal data transferred under the E.U.-U.S. Privacy Shield, in effect formally approving the agreement, which will go through annual joint reviews. Following the adequacy decision, the U.S. Department of Commerce launched a new website to provide organizations with information to guide the process of self-certifying under the Privacy Shield. The website began accepting certifications on Aug. 1.

DETAILS

Like the Safe Harbor Framework it replaced, the E.U.-U.S. Privacy Shield aims to facilitate the lawful transfer of personal data for European citizens to the U.S. as part of the $250 billion in annual trade between the United States and the E.U. It provides a framework for data controllers and processors to implement the seven core and 16 supplemental data privacy principles (the Principles). The Privacy Shield expands the obligation to both controllers and processors, and incorporates a more formal agreement with U.S. authorities for enforcement and cooperation. These provisions were important criteria used in making the adequacy determination.

CONTACT:

DEENA COFFMAN
BDO Consulting Managing Director
dcoffman@bdo.com

GLENN POMERANTZ
Partner and BDO Global Forensics Practice Leader
gpommerantz@bdo.com

The seven foundational privacy principles set forth the following obligations:

- The Notice Principle obliges organizations to provide specific information to data subjects relating to the processing of their personal data (i.e., the type of data collected, purpose of the collection and how the information will be used, and how to make an inquiry or complaint). An organization must include in its privacy policy a declaration to comply with Privacy Shield Principles so that the commitment becomes enforceable. It must also inform individuals of the rights afforded under the Privacy Shield, the requirement to disclose personal information in response to a lawful request by public authorities and its liability when transferring data to third parties, among other requirements.
- The Choice Principle provides data subjects the choice to decide at any time whether their personal information may be disclosed to a third party or used for a purpose that is materially different from the purpose(s) for which consent was originally obtained. When dealing with sensitive data, organizations have to obtain data subjects' express consent.
- The Security Principle requires organizations creating, maintaining, using or disseminating personal data to take "reasonable and appropriate" security measures that take into account risks involved in the processing and nature of the data.
- The Data Integrity and Purpose Limitation Principle requires that personal data is limited to what is relevant for processing purposes and restricts an organization from processing personal data in a way that is incompatible with the purpose for which it was originally collected or authorized. It also requires data processors and controllers to take reasonable steps to ensure that personal data is accurate, complete and current.
- The Access Principle ensures that data subjects have the right to access their own personal information and are able to correct, amend or delete that information where it is inaccurate or has been processed in violation of the Principles.
- The Accountability for Onward Transfer Principle requires that any transfer of data collected under the Privacy Shield to third parties is limited to only what is necessary. The data is still subject to the same protections as provided by the organization certifying under the Privacy Shield. An organization doing business under the Privacy Shield certification remains liable if the agent processes the protected personal information in a manner inconsistent with the Principles.
- The Recourse, Enforcement and Liability Principle requires organizations to provide mechanisms for assuring compliance with the Principles, recourse for individuals who are impacted by non-compliance and consequences for the organization not following the Principles. Individuals who believe their data has been misused by a company claiming certification under Privacy Shield can submit complaints via a free, readily available dispute mechanism provided by the company. That company is required to respond to the complaint within 45 days. Though ideally the company will resolve the complaint itself, the new framework also requires participants to provide an independent redress mechanism through which individuals' complaints are investigated and resolved. Some companies are required to use the European Data Protection Authorities (DPAs) for this, while others have the option to choose to use DPAs or contract with another entity like the Better Business Bureau. The U.S. Department of Commerce has committed to receiving, reviewing and facilitating resolution of complaints submitted to DPAs within 90 days.

BDO INSIGHTS

After nearly a year of organizations operating in data limbo, the news of a data sharing agreement between the E.U. and United States to replace the Safe Harbor Framework is a welcome development, as it offers organizations on both sides of the Atlantic a single data transfer authorization mechanism with clear guidelines. Organizations should understand, however, that certification will require a detailed analysis of their data flow, access, use and security controls, as well as policies and procedures. Aligning these key areas with a lengthy list of new requirements (only summarized and excerpted here) will be no small feat. Organizations that choose to operate outside the framework may instead consider requesting DPA authorization, instituting binding corporate rules or making use of standard contractual clauses. These options may not always be suitable depending on the circumstances, so the Privacy Shield offers an important alternative beneficial to most U.S. organizations with operations in Europe.

The Privacy Shield further reconciles differences in data privacy protections across E.U. member states, but it does not remove all individual member state requirements, particularly in relation to employee personal information. Companies

should understand that local data protection requirements may still exist, depending on location. As the agreement begins to take hold, entities will see what enforcement of the new framework looks like. Perhaps most importantly, while certifying under Privacy Shield is voluntary, once an organization does so, its commitment to follow its framework is enforceable under U.S. law. So, organizations should review the requirements carefully and address any potential compliance gaps before moving forward.

It's also important to note that the EC based its adequacy decision on the current framework of the 1995 Data Protection Directive and not the recently adopted General Data Protection Regulation (GDPR). Entering into full effect on May 25, 2018, the GPDR is intended to further strengthen data protection for individual European citizens—including the "right to be forgotten"—and to "future proof" the rules in line with digital and technological developments. When the GPDR comes into force, data transfers between the E.U. and the United States will be subject to these more stringent measures, including significantly more severe and frequent sanctions for violations.

Another development organizations should closely monitor is the effect of "Brexit" —the U.K.'s popular vote to leave the E.U. —on the Privacy Shield. If the divorce is finalized and depending on its terms, the U.K. may no longer be party to the E.U.'s treaties with the United States, including the Privacy Shield agreement. In addition, the U.K. Information Commissioner's Office (ICO) stated following the Brexit vote that "upcoming E.U. reforms to data protection law would not directly apply to the U.K." If the U.K. adopts its own data privacy regime, it would likely need to be reviewed by the EC for adequacy. Depending on how Brexit unfolds, companies with operations in the U.K. may need to make separate arrangements for data transfers, not just between the U.K. and the United States, but also between the U.K. and the E.U.