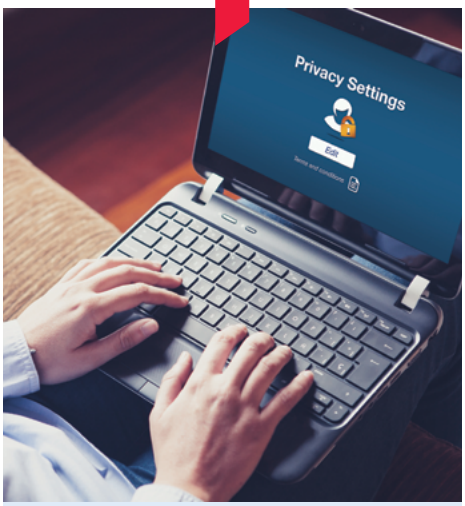
AN ALERT FROM THE BDO TECHNOLOGY PRACTICE

BDO KNOWS: TECHNOLOGY



U.S. TECH FIRMS BREATHE A SIGH OF RELIEF: THE PRIVACY SHIELD IS HERE

SUMMARY

Last October, the Court of Justice of the European Union (CJEU) abruptly invalidated the 15-year-old U.S.-EU Safe Harbor Framework for transatlantic transfers of personal data following a complaint against Facebook's data privacy practices. The ruling left thousands of companies—and $260 billion of transatlantic commerce—in legal limbo. A number of companies were able to rely on alternative legal mechanisms, such as binding corporate rules (BCRs) or standard contractual clauses (SCCs), for data transfers, but those measures require time and weren't helpful to companies caught by surprise. Without an alternative mechanism, companies in the EU were prohibited from moving personally identifiable information belonging to European citizens outside the EU.

After missing the initial deadline, the EU and the U.S. agreed on a new framework on Feb. 2, 2016: the EU-U.S. Privacy Shield. Adoption of the Privacy Shield depended upon the European Commission (EC)'s decision on whether the Privacy Shield provided an adequate level of protection under EU data protection law.

On July 12, the EC determined that, under the Privacy Shield framework, United States companies meet the standard of adequacy for personal data transferred under the EU-U.S. Privacy Shield. In effect, this formally approved the agreement, which will go through annual joint reviews.

Following the adequacy decision, the U.S. Department of Commerce (DOC) 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. Almost 300 companies—the majority of them in technology—have been certified under the new framework as of Sept. 28, including Microsoft, Salesforce, Google, GoPro, Akamai Technologies and Oracle America.

DETAILS

Like the Safe Harbor Framework it replaced, the EU-U.S. Privacy Shield aims to facilitate the lawful transfer of personal data for European citizens to the United States. 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

HOW DO I GET MORE INFORMATION?

For more information about how technology organizations can prepare to certify under the Privacy Shield or comply with evolving EU data privacy requirements, please contact:

TIM CLACKETT
310-557-8201 / tclackett@bdo.com

DEENA COFFMAN
212-798-4037 / dcoffman@bdo.com

SLADE FESTER
408-352-1951 / sfester@bdo.com

HANK GALLIGAN
617-422-7521 / hgalligan@bdo.com

STEPHANIE GIAMMARCO
212-885-7439 / sgiammarco@bdo.com

PAUL HEISELMANN
312-233-1876 / pheiselmann@bdo.com

AFTAB JAMIL
408-352-1999 / ajamil@bdo.com

GLENN POMERANTZ
212-885-8379 / gpomerantz@bdo.com

ANTHONY REH
404-979-7148 / areh@bdo.com

GEORGE RUDOY
212-817-1746 / grudoy@bdo.com

DAVID YASUKOCHI
714-913-2597 / dyasukochi@bdo.com

Read more ▶

cooperation. These provisions were important criteria used in making the adequacy determination.

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 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. Going a step further, when dealing with sensitive data, organizations have to obtain data subjects' affirmative, express consent, often termed "opt-in" rather than a passive "opt-out" consent that is permissible for non-sensitive information. This must occur, generally speaking, both at the point of collection and prior to any changes in how the information is used and shared.

- 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. This is a continuation of the trend of lawmakers and regulators expecting companies in possession of sensitive, personal information to protect it adequately.

- The *Data Integrity and Purpose Limitation Principle* requires that personal data collected 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 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 use DPAs or contract with another third-party dispute resolution provider like the Better Business Bureau. The DOC has committed to receiving, reviewing and facilitating resolution of complaints submitted to DPAs within 90 days.

To self-certify under the Privacy Shield, organizations must complete seven steps:

- Confirm eligibility to participate in the framework—U.S. organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) can certify.

- Develop a Privacy Shield-compliant privacy policy and publish a public privacy policy that includes language and links to specific Privacy Shield resources.

- Identify an independent recourse mechanism to investigate unresolved complaints at no cost to individuals.

- Ensure a compliance verification mechanism is in place—either a developed self-assessment or a third-party assessment program.

- Designate an internal contact to handle questions, complaints, access requests and other issues that may arise related to the Privacy Shield.

- Review the required information for self-certification.

- Submit the self-certification information and fee, which is determined by annual revenue.

BDO INSIGHTS

After nearly a year of organizations operating in data limbo, the news of a data-sharing agreement between the EU 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.

Nonetheless, organizations should understand 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 do not self-certify will need to rely on alternative legal mechanisms for data transfers, such as implementing BCRs, which only allow for

Read more ▶

intracompany data transfers, or entering into multiple SCCs. These options are typically more cumbersome and may not always be suitable depending on the circumstances.

The Privacy Shield further reconciles differences in data privacy protections across EU 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.

While the EC determined the Privacy Shield provides adequate protection, some in the EU feel an "enforceable" self-certification framework does not go far enough to effect compliance with the data privacy principles stipulated in the framework. It's also important to note 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 GDPR 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 GDPR comes into force, data transfers between the EU and the United States will be subject to these more stringent measures, including significantly more severe and frequent sanctions for violations.

The U.S. legal community also has expressed some concern about the Privacy Shield exacerbating the conflict between the recently amended Federal Rules of Civil Procedure—the rules governing e-discovery—and EU privacy regulations. Currently, discovery teams work to balance EU data protection requirements against discovery obligations using a mixture of data minimization, deduplication, redaction, and more sophisticated artificial intelligence-driven data analysis to limit data collection to only the most critical evidence. These case-by-case balancing acts can be nerve-wracking, and many are counting on an earnest, thorough attempt to filter out all noncritical sensitive information in as much as possible to provide favor with U.S. and EU judges and regulators.

Another development that organizations should closely monitor is the effect of "Brexit"—the U.K.'s popular vote to leave the EU—on the Privacy Shield. Depending on the terms of the "divorce," the U.K. may no longer be party to the EU's treaties with the United States, including the Privacy Shield agreement and the protection it affords. In addition, the U.K. Information Commissioner's Office (ICO) stated following the Brexit vote that "upcoming EU 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, technology 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 EU.

BDO TECHNOLOGY PRACTICE

BDO works with a wide variety of technology clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

People who know Technology, know BDO.