PUBLICATION

What U.S. Businesses Should Be Thinking About Now that European Commission Has Adopted Privacy Shield

July 12, 2016

On July 12, 2016, the European Commission formally adopted the EU-U.S. Privacy Shield, a new framework governing the transatlantic flow of data. The Privacy Shield replaces the former Safe Harbor Privacy Principles, which the Court of Justice of the European Union declared invalid in October 2015.

As the Privacy Shield will apply to all transatlantic transfers of personal data, it will affect nearly every U.S. business with European customers or employees. Here, we offer the big picture of the new regime and what U.S. businesses need to be thinking about.

Out with Safe Harbor …

Unlike the United States, which operates under a patchwork of privacy laws governing different industry sectors, the EU has adopted the comprehensive Data Protection Directive as a privacy framework for protection of all personal data among member states. Under the Data Protection Directive, personal information may flow to a non-member nation (i.e., the United States) only if that nation's privacy protections are deemed "adequate." As the U.S. laws were deemed to provide "inadequate" privacy protections, the EU and U.S. crafted a political agreement for the establishment of the EU-U.S. Safe Harbor Program.

The Safe Harbor Program provided a self-certification scheme that allowed U.S. organizations that self-certified their commitment to EU privacy principles to transfer personal data of EU citizens to the United States. Safe Harbor was self-regulated through the private sector with oversight by the U.S. Department of Commerce and the Federal Trade Commission.

The high court of the EU, however, invalidated the Safe Harbor framework in 2015 after the Edward Snowden disclosures of U.S. Intelligence activities led to EU fears that U.S. governmental agencies could access personal information in ways that undermined the adequacy of the protections under the Safe Harbor framework.

… And In with Privacy Shield

While reflecting similar principles of data privacy as Safe Harbor – *notice, choice, forward transfer accountability, security, data integrity, access, and recourse and enforcement* – Privacy Shield expands each of the principles and places more stringent requirements on the transferring U.S. organization.

For example, the U.S. organization will need to clearly and conspicuously notify EU users that it is participating in Privacy Shield and that their data can be transferred to the U.S. When dealing with vendors, a certified organization must make sure those vendors will abide by Privacy Shield's principles. From a data security standpoint, participants must take appropriate measures to protect data, but what is deemed "reasonable" will take into account the nature and sensitivity of the data. Privacy Shield also includes assurances that limit U.S. law enforcement and intelligence from engaging in mass surveillance of EU citizens' data.

The most far-reaching change, however, is Privacy Shield's enforcement mechanisms. While self-certification of compliance is still an option, it now must be accompanied by an affirmative self-assessment, signed annually by a corporate officer. Certifying organizations also will be required to use third-party dispute

resolution bodies to investigate and resolve user complaints, and unresolved complaints can be escalated to the U.S. Department of Commerce and binding arbitration. The Federal Trade Commission also has committed to vigorous enforcement of Privacy Shield, including the review and investigation of complaints from EU authorities.

Next Steps

If your organization anticipates that it will engage in any transatlantic data transfers, you will want to take immediate steps to certify for Privacy Shield; acting within the next 90 days provides the advantage of a nine-month grace period in which to bring third-party agreements into conformity. Accordingly, now is the time to review your organization's privacy practices and if necessary update them to meet Privacy Shield's principles, as well as to review vendor and other third-party agreements for future compliance.

Baker Donelson's Privacy and Information Security Group is available to assist with any questions or legal advice in connection with Privacy Shield or other privacy and security issues.