UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

29th Annual Technology Law Conference

May 26-27, 2016
Austin, Texas

Inside the New and Improved EU-U.S. Data Transfer Framework

Lisa E. Zolidis

*Printed with permission from Harriet Pearson

March 7, 2016

Inside the New and Improved EU-U.S. Data Transfer Framework

This article previously was published on Law360 on March 4, 2016.

On February 29, 2016, and after more than two years of negotiations with the U.S. Department of Commerce, the European Commission released its much-awaited draft Decision on the adequacy of the new EU –U.S. Privacy Shield framework, accompanied by information on how the framework will work in practice.

The Privacy Shield documentation is significantly more detailed than that associated with its predecessor, the EU-U.S. Safe Harbor, imposing more specific and exacting measures on U.S. organizations wishing to join the framework. It also includes additional checks and balances designed to make sure that the privacy rights of EU individuals can be exercised when their data is being processed in the United States. That said, the seven Privacy Shield Principles are largely aligned with the privacy practices followed by Safe Harbor participants and found in other global privacy compliance programs, and should not be an insurmountable burden for companies looking to shift from Safe Harbor compliance to Privacy Shield compliance.

As compared to the Safe Harbor, the changes in the Privacy Shield fall generally into one of three categories: (1) changes to the substantive Privacy Principles with which certifying organizations must comply; (2) changes to the administration and supervision of the framework; and (3) explication of limitations on U.S. government access to data transferred under the Privacy Shield. We summarize these changes, as well as the practical implications for companies seeking to certify to the Privacy Shield.

Changes to the Privacy Principles

As was the case under Safe Harbor, organizations that wish to use the Privacy Shield must self-certify compliance with a set of Privacy Principles via a filing to the U.S. Department of Commerce, signed by a corporate officer. Annual re-certification is required, as are follow-up procedures to verify compliance.

Conceptually, the seven high-level Privacy Principles generally remain unchanged from Safe Harbor. However, there are significant new obligations under some of the Principles.

Contacts

Harriet Pearson
Partner, Washington, D.C.
harriet.pearson@hoganlovells.com
+1 202 637 5477

Eduardo Ustaran
Partner, Washington, D.C.
eduardo.ustaran@hoganlovells.com
+44 20 7296 5249

Bret Cohen
Sr. Associate, Washington, D.C.
bret.cohen@hoganlovells.com
+1 202 637 8867

For the latest privacy and cybersecurity developments, please visit us at *Chronicle of Data Protection*

www.hoganlovells.com

Notice

The Notice principle under Safe Harbor merely stated that a participating organization was required to "inform individuals about the purposes for which it collects and uses information about them, how to contact the information with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure." For the most part, certifying organizations complied with this requirement by describing these categories of information at a high level in their published Safe Harbor privacy policies.

The Notice principle under Privacy Shield is much more specific and in line with the requirements under the forthcoming EU General Data Protection Regulation (GDPR). In particular, this principle lists thirteen different details that participants must include in their published privacy policies, including (i) any relevant establishment in the EU that can respond to inquiries or complaints, (ii) the independent dispute resolution body designated to address complaints, a hyperlink to the complaint submission form of that dispute resolution body, and the possibility, under certain circumstances, for EU individuals to invoke additional binding arbitration; and (iii) the possibility that the organization may be held liable for unlawful transfer of personal data to third parties.

Organizations wishing to convert their Safe Harbor certifications will as a priority need to update their privacy policies to contain these specific data elements.

Choice

The Choice principle under Privacy Shield remains largely unchanged from Safe Harbor. It requires certified organizations to provide a mechanism for individuals to opt out of having personal information disclosed to a third party or used for a materially different purpose than that for which it was provided, although Privacy Shield clarifies that this option need not be provided when the disclosure is made to a third-party service provider that will use the information solely under the instructions of the organization (i.e. data processors, in European terms). As with Safe Harbor, Privacy Shield also requires covered organizations to obtain affirmative express consent from individuals prior to sharing sensitive information with a third party or using it for a purpose other than for which it was initially collected.

Accountability for Onward Transfer

Previously known as the "Onward Transfer" principle under Safe Harbor, the new "Accountability for Onward Transfer" principle adds more requirements for transfers to third parties than explicitly required under Safe Harbor, distinguishing between when the recipient is acting as a "controller"—that is, using the information for its own purposes—or a service provider.

The Onward Transfer principle under Safe Harbor only explicitly stated that organizations transferring Safe Harbor data to a third-party controller were required to comply with the Notice and Choice principles with respect to the data. Under Privacy Shield, the transferring organization is now explicitly required to enter into a contract with the third-party controller providing that the data may only be processed for limited and specified purposes consistent with individual consent, and that the recipient will provide the same level of protection as the Privacy Shield Principles, with two exceptions:

- A contract is not required for transfers of personal data involving a small number of employees "for occasional employment-related operational needs," such as the booking of a flight, hotel room, or