EU and US agree to Privacy Shield to replace the Safe Harbor

Dominic A. Paluzzi, James J. Giszczak | Monday, March 14, 2016

EU and U.S. officials recently reached an agreement to implement the EU-U.S. Privacy Shield program, which, if passed, would succeed the now-invalidated U.S.-EU Safe Harbor program. We've put together the following FAQs to help you understand the nuts and bolts of the program and get a better idea of what action your organization may need to take.

What does the Privacy Shield look like?

The purpose of the Privacy Shield is to strengthen protections for individuals whose personal data is transferred from the EU to the U.S. The Privacy Shield program is outlined in the 128-page Privacy Shield Documents, which also contain a draft adequacy decision (the importance of which is discussed in more detail below).

How can an organization qualify for the Privacy Shield?

For an organization to be able to rely on the Privacy Shield to affect transfers of personal data from the EU to the U.S., it must "self-certify its adherence to the principles" to the Department of Commerce or its designee. To be eligible, the organization must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), the Department of Transportation (DOT) or other statutory authority that will "effectively ensure compliance" with the principles. While initial certification is voluntary, once an organization chooses to certify "effective compliance is compulsory," and self-certification must be done annually.

What are the privacy principles and what do they mean?

As under the Safe Harbor program, organizations that have self-certified must comply with seven privacy principles when transferring and processing data originating out of the EU:

1. Notice requirements
2. Choice i.e., individual "opt-out" mandate
3. Data security, integrity and purpose limitations
4. Individual access
5. Accountability for Onward Transfer
6. Individual recourse

7. Enforcement and Liability

WHAT IS THE INDIVIDUAL OPT-OUT MANDATE?

Privacy Shield organizations must give individuals the choice to opt out of having their personal information disclosed to a third party (except the Privacy Shield organization's agent) or used for a purpose materially different from the purpose or purposes for which it was originally collected and subsequently allowed.

WHAT IS THE OPT-IN MANDATE?

With limited exceptions, when it comes to an individual's sensitive information, the individual must expressly opt in before the Privacy Shield organization can disclose or use the information.

WHAT IS THE ONWARD TRANSFER PRINCIPLE?

The onward transfer principal means that any data transfer to a third party must be in accordance with a contract that provides that, among other things, the recipient of the data will provide the same level of protection as the principles listed above. This also requires that for Privacy Shield organizations with contracts with agents, the Privacy Shield organization must, upon request, provide a summary or copy of the relevant privacy provisions to the Department of Commerce.

WHAT ARE THE REQUIREMENTS TO ENSURE INDIVIDUAL RECOURSE?

Privacy Shield organizations must have effective internal mechanisms to allow them to handle complaints concerning the organization's noncompliance with the seven principles. In addition, the Privacy Shield organizations must commit to respond to those complaints within 45 days. An independent alternative dispute resolution (ADR) mechanism must also be put in place so individuals can pursue their non-compliance issues. The ADR mechanism must be freely available and, the key word there, free, meaning no requirement that the complainant pay their costs as is the case in many ADR provisions. Individuals must also be able to bring their claims to their national Data Protection Authorities (DPAs), which would then work with the Department of Commerce to ensure the Privacy Shield organization handles the complaint.

WHAT LIABILITY DO PRIVACY SHIELD ORGANIZATIONS HAVE?

Privacy Shield organizations are liable if an agent transfers data to processes that transferred data information in violation of the seven principles. However, the Privacy Shield organization would be able to escape liability if it can demonstrate it was not responsible for the event(s) giving rise to the damage.

WHAT ARE THE SPECIAL REQUIREMENTS COVERING HR DATA?

A Privacy Shield organization that wants to cover HR data must commit to cooperate with the European DPAs during the investigation and resolution processes. This includes agreeing to an agreement to comply with any advice from the DPAs that the organization needs to take specific action to comply with the principles.

Are there other principles to be aware of?

The Privacy Shield program includes a number of other principles worth noting. These include:

1. Sensitive data
2. Journalistic exceptions
3. Secondary liability
4. Performing due diligence and conducting audits
5. The role of the DPAs
6. Verifying an organizations privacy practices
7. Information concerning an individual's right of access
8. Application of HR data
9. Requirements for contracting when data is transferring just for processing purposes, i.e., onward transfers
10. Dispute resolutions and enforcement, which includes more detail on recourse, remedies, sanctions, FTC actions, and others
11. The handling of travel information
12. Timing of the "opt-out" option requirement
13. Data for pharmaceutical research, medical products and other related purposes
14. Public authority access request handling
15. Public records and the use of publicly-available information

What is next and is there anything left in the air?

The first next step is for the EU to review and make a determination of "adequacy." While there is no specific deadline for this determination, the EU Article 29 Working Party, which is made up of the national data protection authorities in the EU states, issued opinions that will be key to the EU's determination as to whether the Privacy Shield would adequately protect its citizens' individual data that is transferred to the U.S.

If the EU determines that the Privacy Shield is adequate, the EU Commission's draft decision would then have to be adopted by the EU Commission and approved by the 31 31 Working Group, which represents the EU Member states, before it can actually become law. If there are any materials changes, further negotiations with the U.S. would be required.

There is still the chance that the Privacy Shield program may not happen. In the event the EU Commission adopts a decision finding that the U.S. provides an adequate level of protection under the Privacy Shield program, the decision could still be challenged before national data privacy authorities, which is what caused the downfall of its predecessor Safe Harbor framework.

What can organizations do in the meantime with no Safe Harbor and no Privacy Shield law?

Until the Privacy Shield becomes actual law, there are model contract clauses, consent and binding corporate rules and other mechanisms organizations can continue to use during transfers from the EU. While none of these mechanisms can offer the types of protections afforded by the Safe Harbor or the Privacy Shield, they do provide a structure for dealing with data transfers.

Takeaways

The Privacy Shield program is in its infancy stages. It is not formalized yet, and it has a long way to go before it is.

Organizations that deal with transferring data originating from the EU, however, will want to take a close look at what the Privacy Shield program will require because, in the event it is formalized into law, it will help keep organizations out of trouble. Specifically, organizations will want to look into how they can affect the reporting and compliance mechanisms, and how to resolve complaints within the proposed 45-day timeframe.

For more information, please contact one of the attorneys listed below.

Dominic A. Paluzzi

James J. Giszczak