The New Framework for Personal Data Transfer from the EU to the US: The Privacy Shield

The Safe Harbor agreement, the framework companies in the United States and the European Union had been using to exchange citizens’ personal data, was declared invalid by the European Court of Justice on Oct. 6, 2015.

Over the last few years, concern has increased over the protection of EU individuals’ personal data in light of the lawfulness, security and transparency of data processing. Highlighting this attention are cases such as the one in which an Austrian citizen, Maximillian Schrems, brought to the court’s attention his concern about privacy violations from mass-surveillance programs conducted by the U.S. National Security Agency (NSA). Whistle-blower Edward Snowden, a former U.S. government computer analyst, revealed that this program allowed the NSA indiscriminate access to personal information from European individuals that was stored on Facebook, a U.S. company.

On the basis of this case, the court declared that the Safe Harbor agreement was invalid because the level of data protection in the U.S. cannot be considered adequate to protect the privacy of EU citizens. Because of the powers available to the NSA, including surveillance, even organizations compliant with the Safe Harbor agreement did not have sufficient protection.

After the decision, companies transferring personal data from EU individuals to the U.S. had to urgently review their existing data-transfer methods. The U.S. and the EU immediately started working together to define a new agreement, the so-called Privacy Shield, to allow the legitimate transfer of personal data from the EU to the U.S., and the EU Commission officially approved the agreement on July 12, 2016.

Providing clarity on data sharing between the EU and U.S. will come as a relief for many companies that were stuck somewhat in limbo while the Privacy Shield framework was being negotiated. It clears a path that allows U.S. companies to process EU citizen data once again under a clear framework and establishes a mandate that provides greater transparency of data sharing and aligns closer to the privacy rights of EU citizens.
The EU-U.S. Privacy Shield imposes stronger obligations on U.S. companies to protect EU individuals’ personal data and reflects the requirements set out by the European Court of Justice:

- **Strong obligations on commercial-sector companies and robust enforcement:** The U.S. Department of Commerce will be in charge of conducting regular updates and reviews of participating companies to ensure that they abide by the new framework to which they are adhering. Those that do not comply will face sanctions.

- **U.S. government access under clear safeguards and transparency obligations:** Access by public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. EU citizens will also benefit from a redress possibility in this area through an ombudsperson mechanism within the U.S. Department of State.

- **Effective protection of individual rights with several redress possibilities:** Under the Privacy Shield framework, any EU citizen who believes that his or her data has been misused will have recourse to several accessible and affordable dispute-resolution mechanisms, including direct resolution by the company itself within 45 days, free alternative dispute resolution (ADR) and involvement of national data-protection authorities within the EU.

- **Monitoring:** The European Commission and the U.S. Department of Commerce will establish an annual joint-review mechanism, involving national intelligence experts from U.S. and European data-protection authorities, regarding the Privacy Shield.

In a nutshell, the new EU-U.S. framework should enforce the lawfulness of EU individuals’ personal data on U.S. territory as well as require U.S. companies to self-certify annually to renew compliance with the requirements. U.S. companies will also have to display their privacy policy on their website, reply promptly to any complaints, and cooperate and comply with European data-protection authorities when handling EU citizens’ personal data.

U.S. companies now have the following key elements to consider:

- A company that runs a business at a global level and has a subsidiary located in the U.S. acting as a data importer for EU personal data should definitely consider the new Privacy Shield framework as one feasible and accessible option among the other potentially applicable methods, such as Binding Corporate Rules or the EU’s standard contractual clauses for personal data transfer.

- Adoption of the Privacy Shield principles requires obligations similar to those under the General Data Protection Regulation (GDPR), such as notice, data integrity, purpose limitation, access, security and accountability for the onward transfer, with the exception of the accountability measures (e.g., appointment of a data-protection officer and execution of data protection impact assessments). Moreover, any third parties processing personal data on behalf of a company complying with the Privacy Shield are required to provide the same level of protection set by the Privacy Shield principles. In practice, this means that these companies must verify and update any contracts with their third parties. Prior to signing any contracts, the company must assess the level of compliance of all third parties involved.

- For U.S. companies, achieving full compliance with the Privacy Shield agreement will be a challenge. U.S. companies will need to apply all the principles required by the Privacy Shield (e.g., notice, choice, accountability for onward transfers, security, data integrity, purpose limitation, access and recourse, enforcement and liability — see [www.privacyshield.gov](http://www.privacyshield.gov) for further details on these principles) in relation to personal data processing and will need to keep in mind that
monitoring activities will be carried out in order to verify compliance with these principles. (This monitoring will be carried out by the Department of Commerce.) According to this scenario, companies should:

- Evaluate which methods of personal data transfer to use to ensure that they meet the requirements set out by the Privacy Shield.
- Consider when, in order to avoid restrictions, to export personal data and when to process data locally.

Companies that choose the Privacy Shield option will have to review their privacy framework and update their compliance with the revised privacy principles established within the Privacy Shield framework. After this, they will be able to self-certify with the Department of Commerce.

Companies adopting the Privacy Shield will have to be immediately compliant with its principles. For those companies that self-certified by Sept. 30, 2016, those with pre-existing commercial relationships with third parties will be excluded from this requirement. Instead, they will have a maximum of nine months to bring these commercial relationships to conformance.

A final additional element to consider is the Brexit, the UK’s decision to leave the European Union. As many U.S. organizations have their European data centers in the UK, the UK acts as the data exporter for many EU-U.S. personal data flows.

Considering this scenario, the impact of Brexit on personal data transfer depends on how, from a regulatory point of view, the UK will manage its exit from the European Union:

- If the UK remains within the European Economic Area (EEA), it will keep the existing European regulations in place (similar to how non–EU members Iceland, Liechtenstein and Norway adhere to EU regulations).
- If the UK completely leaves the EU/EEA, the company will have to adopt one of the methods defined by the Information Commissioner’s Office (ICO), the UK’s data-protection authority.

Whatever direction is chosen, the UK government has been clear that the GDPR will be on the agenda.

Main Steps to Join the Privacy Shield

Any company that wants to join the Privacy Shield via the self-certification process should follow the steps outlined below:

1. **Confirm the organization’s eligibility to participate in the Privacy Shield:** Before embarking on this journey, organizations should check whether they are required to comply with the EU laws. Only U.S. organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) may participate in the Privacy Shield. Moreover, EU laws become applicable where the U.S. company is deemed to have a physical presence in the EU (e.g., it has physical assets in the EU, or places a cookie on an EU workstation when a visitor visits the company’s website) or it collects personal information about EU citizens.

   **Companies adopting the Privacy Shield will have to be immediately compliant with its principles.**

2. **Develop a privacy policy statement compliant with the Privacy Shield:** In order to join the Privacy Shield framework, organizations must develop a privacy policy compliant with the Privacy Shield before submitting their self-certification to the Department of Commerce. A compliant privacy policy must:
   - Declare company conformity with and adherence to the Privacy Shield principles as well as contain information on company handling practices and the choices offered to individuals with respect to the use and disclosure of their personal information.
   - Contain a hyperlink to the Privacy Shield website (www.privacyshield.gov).
   - Be written so that it is clear, concise and easy to understand.
   - Provide accurate details about the location of the organization’s privacy policy and ensure that it is publicly available (i.e., if the company has a public website, it should include the policy).
3. **Understand readiness for Privacy Shield compliance:** Put in place remediation to close gaps required to align with compliance requirements.

4. **Identify the organization’s independent recourse mechanism:** An independent recourse mechanism must be in place and available to prompt investigation of unresolved complaints at no cost to the individual.

5. **Ensure that a verification mechanism is in place:** Adequate procedures must be in place for verifying compliance with the Privacy Shield. These procedures may consist of a self-assessment or an external/third-party assessment program.

6. **Designate a contact within the organization regarding the Privacy Shield:** A contact must be provided to handle questions, complaints and access requests and any other issues that may arise. This contact would typically be someone in charge of managing privacy compliance (including Privacy Shield) within the company according to the organizational model defined (e.g., the chief privacy officer or the data-protection officer).

7. **Submit the organization self-certification to the Department of Commerce:** The company must register on the Privacy Shield website and fill out the required information before it can submit its self-certification.

## Contacts

**FRANCE**

Bernard Drui  
+33.14.296.4111  
bernard.drui@protiviti.fr

**GERMANY**

Michael Klinger  
+49.69.963.768.100  
michael.klinger@protiviti.de

Kai-Uwe Ruhse  
+49.69.963.768.100  
kaiuwe.ruhse@protiviti.de

**ITALY**

Alberto Carnevale  
+39.02.6550.6302  
alberto.carnevale@protiviti.it

Hernan Gabrieli  
+39.02.6550.6301  
hernan.gabrieli@protiviti.it

Giacomo Galli  
+39.02.6550.6303  
giacomo.galli@protiviti.it

**THE NETHERLANDS**

Anneke Wieling  
+31.20.346.0405  
anneke.wieling@protiviti.nl

**UNITED KINGDOM**

Andrew Clinton  
+44.207.024.7570  
andrew.clinton@protiviti.co.uk

Ryan Rubin  
+44.207.389.0436  
ryan.rubin@protiviti.co.uk

Jonathan Wyatt  
+44.207.024.7522  
jonathan.wyatt@protiviti.co.uk

**UNITED STATES**

Scott Laliberte  
+1.267.256.8825  
scott.laliberte@protiviti.com

Chris Louden  
+1.703.350.4397  
chris.louden@protiviti.com

Jeff Sanchez  
+1.213.327.1433  
jeffrey.sanchez@protiviti.com

Cal Slemp  
+1.203.905.2926  
cal.slemp@protiviti.com

---

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 Index.

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0217-107151

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.