PAUL HASTINGS

STAY CURRENT

July 2016

Follow @Paul_Hastings

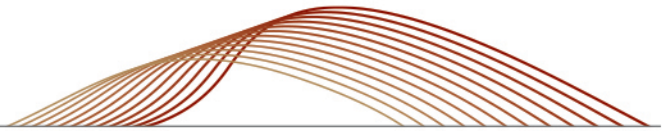
Five Ways that Privacy Shield is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification

By Paul Hastings Global Privacy and Cybersecurity Practice

On July 8, 2016, the EU Member States approved the EU-U.S. Privacy Shield, and the European Commission subsequently adopted it on July 12, 2016. With the U.S. Department of Commerce accepting certifications starting August 1, 2016, Privacy Shield will replace Safe Harbor as a compliance mechanism for personal data transfers from Europe to the United States (or a key component of a global data transfer strategy). Whether your company is Safe Harbor certified or considering Privacy Shield certification for the first time, the decision to proceed to Privacy Shield will depend on a number of factors, including:

- the extent and maturity of other data transfer compliance mechanisms in place (*e.g.*, Model Contracts, Binding Corporate Rules, and individual Data Protection Authority Approval),
- business needs,
- scope of global footprint,
- exposure to EU citizens, workforce, outsourcing, and cloud utilization,
- maturity of the company's privacy program, including its redress program,
- sophistication of vendor management and current state of contracts,
- types and sensitivity of data and data elements,
- whether the company is in an industry that is a particular target of regulators, and
- whether the transfers relate to B2B or B2C relationships.

For companies that elect to proceed under Privacy Shield, two key components will help drive an informed strategy for certification: (1) understanding how Privacy Shield differs from Safe Harbor, and (2) having an action plan to prepare for certification.



Five Ways that Privacy Shield Differs from Safe Harbor

1. **New Privacy Shield Policy Requirements**. The Privacy Shield principles are largely the same as Safe Harbor and include Notice, Choice, Access, Security, Onward Transfer, Data Integrity/Purpose Limitation, and Redress. However, Privacy Shield policies must include statements regarding the enforcement body, a new arbitration right, disclosures to public authorities, and the company's liability for onward transfers.

2. **Heightened Onward Transfer Requirements**. Companies participating in Privacy Shield will face tightened conditions for onward transfers to their third-party business partners. For example, a company may only transfer personal data to a partner for a limited purpose and pursuant to a contract that provides at least the same level of protection as the Privacy Shield principles. The good news is that companies certifying within the first two (2) months of the effective date of Privacy Shield will have nine (9) months from their date of certification to bring contracts into compliance.

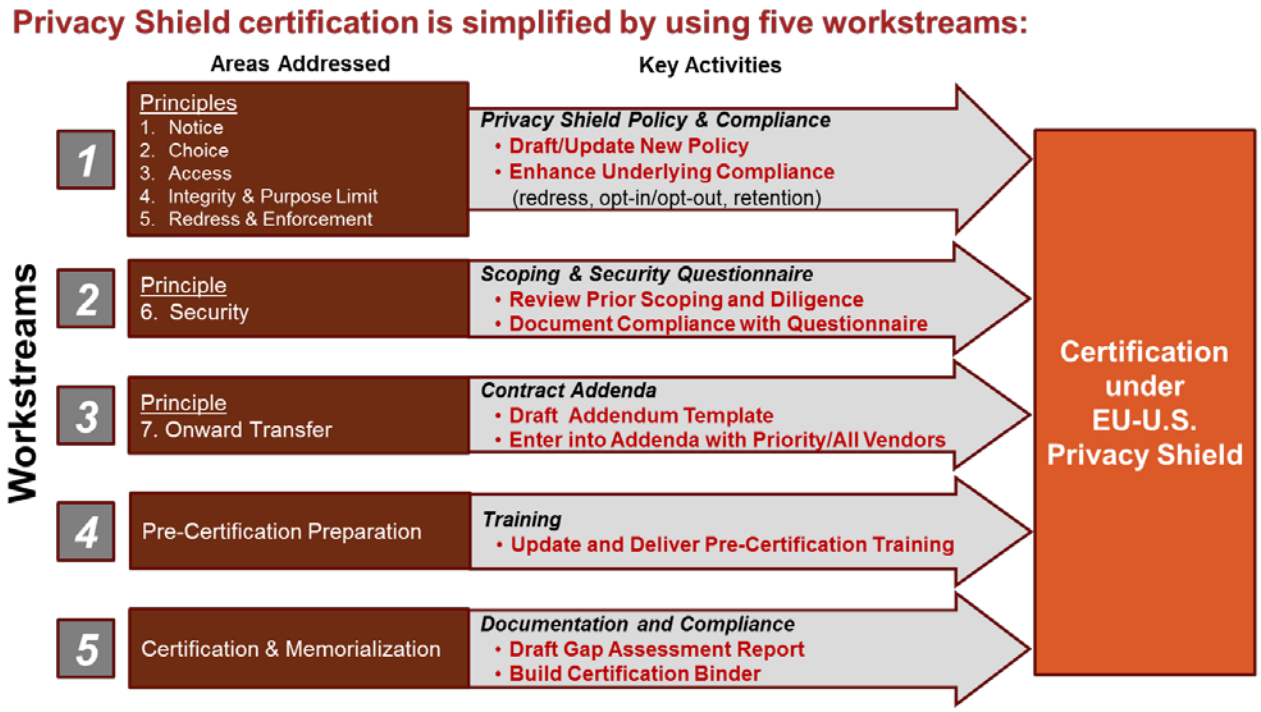
3. **Stronger Supervision and Enforcement Activities by the Department of Commerce and FTC**. The intent of Privacy Shield is to transform the oversight system from self-regulating to one that is more responsive and proactive. The certification and annual recertification process will remain unchanged, but the Department of Commerce will actively monitor compliance through detailed questionnaires, among other things. Additionally, the FTC will maintain a "wall of shame" for companies that are subject to FTC or court orders in Privacy Shield cases.

4. **New Redress Timelines and Process for Misuse of Data by Commercial Companies**. Any EU citizen who believes that his or her data has been misused will have several redress possibilities under Privacy Shield. Among them, EU citizens will be able to report complaints directly to their local Data Protection Authorities. Redress mechanisms include established timelines for responses by a subject company. Privacy Shield also creates a new arbitration right for unresolved complaints.

5. **Redress Process for U.S. Government Indiscriminate Access or Mass Surveillance**. There will be clear limitations, safeguards, and oversight mechanisms for access by public authorities for law enforcement and national security purposes. A new redress mechanism will inform a complainant whether an access or surveillance matter has been properly investigated and that either U.S. law has been followed or has been remedied in the case of non-compliance.

Five Simple Steps to Certify under Privacy Shield

While there has been considerable concern about whether to certify under Privacy Shield in light of other available compliance mechanisms (Binding Corporate Rules, Model Contracts, etc.), Paul Hastings' Privacy and Cyber Implementation Solutions group has developed a simple five-step approach to quickly and cost-effectively achieve certification. The following graphic depicts our five-step approach to satisfying the seven Privacy Shield Principles:



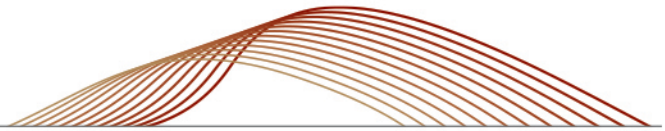
Step 1 – Develop and Maintain a Privacy or Privacy Shield Policy. The policy will be based on the seven (7) Principles for certification under the EU-U.S. Privacy Shield. If you are currently or were a Safe Harbor company, your Safe Harbor policy can be easily leveraged and supplemented to meet Privacy Shield requirements. Some examples of the subject matter that is covered in the policy include:

- **Notice**. Privacy Shield Companies must update or prepare a global or EU applicable privacy policy or EU notice statements for the data subject of the certification to ensure such policy or notice is accurate, comprehensive, and visible to data subjects. Also, companies often simultaneously aim to improve awareness so that both data subjects and management have comfort that employees are aware of the appropriate operating practices.

- **Choice**. The policy will also cover areas where consent, permission, data use limitations or opt-out strategies, and special treatment for "Sensitive Personal Data" are applicable.

- **Access, Data Integrity, and Redress**. The policy also addresses other areas related to existing processes or controls, if applicable, to meet Access, Data Integrity, and Redress requirements needed to cover a Privacy Shield election.

Step 2 – Validate Security Safeguards with Customized Questionnaire. A Privacy Shield company must maintain adequate and reasonable administrative, technical, and physical safeguards and controls designed to address appropriate security requirements for U.S. and EU applications that capture or process data within the scope of the certification. To validate a company's security safeguards, we deploy a quick and simple security questionnaire to system, application, and interface owners who handle data subject to the certification.



Step 3 – Address Onward Transfers. Following a review of existing contracts, a contract addendum template is prepared that addresses the specific Privacy Shield wording requirements for third-party vendors and other onward transferees. While this step can require some effort, depending on your industry and jurisdiction, companies can leverage expertise and experience from analogous compliance activities relating to contractual safeguard enhancements under the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996, Safe Harbor, Model Contracts and other similar regimes.

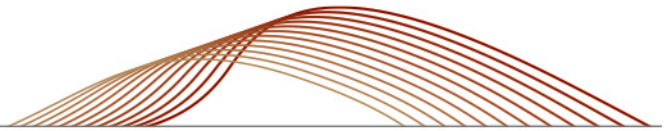
Step 4 – Update Training. Similar to Safe Harbor, Privacy Shield has a training requirement for employees and workers who have access to EU citizen data. For Safe Harbor companies, training can be quickly updated. For companies new to the process, certifying under Privacy Shield is an opportunity to create or update/enhance existing training to both satisfy Privacy Shield and develop a consistent baseline privacy and data protection/security training module for global use.

Step 5 – Prepare for Certification. Documentation supporting the company's Privacy Shield certification (*e.g.*, policies and procedures, gap assessment report, and contract addendum) is prepared/compiled and included in a compliance binder. The compliance binder will also facilitate the company's annual recertification efforts and help respond to any regulatory inquiries, if they arise.

Additional Considerations

Benefits and Risks of Privacy Shield. Of all the existing compliance mechanisms, Privacy Shield is the least expensive to maintain and the most flexible (*i.e.*, Privacy Shield is a blanket approval for transfers and does not require data transfer and use specificity like Model Contracts and BCRs). Although Privacy Shield authorizes only data flows between Europe and the U.S., enterprising companies can leverage Privacy Shield EU to U.S. transfers with a second-step, subsequent transfers onward as a key mechanism to facilitate global data flows. On the other hand, there is some debate whether there will be increased regulatory compliance pressure spurred on by the new U.S. Department of Commerce compliance questionnaires and increased cooperation with EU data protection authorities or whether the Privacy Shield will have a lower risk of enforcement scrutiny consistent with that under Safe Harbor. In any event, Privacy Shield could still be challenged in the European courts or complicated by Brexit in the event that the U.K. adopts its own approach to privacy and data transfers.

Pursing Privacy Shield as Part of Global, Integrated, Cost-Effective Compliance Approach. The forthcoming European General Data Protection Regulation ("GDPR") and other laws (including privacy laws in non-EU jurisdictions) will require additional investment and internal partnership in the underlying good data hygiene, data management and data use, and sharing practices. While some companies have already supplanted Safe Harbor by putting a series of Model Contracts in place, many companies are planning to incorporate Privacy Shield as a key strategic component of a larger, global compliance program that takes advantage of one global framework and audit approach that can be cost-effectively used to satisfy many key global requirements and multiple data transfer compliance solutions (*i.e.*, U.S. laws, GDPR, Model Contracts, Privacy Shield, and potentially BCRs and APEC's Cross Border Privacy Rules Certifications).



To learn more about Privacy Shield and the approaches being taken by others, please contact Jim Koenig, Behnam Dayanim, Sherrese Smith, Ashley Winton, or any member of our **Privacy and Cybersecurity Implementation Solutions Group** or larger **Global Privacy and Cybersecurity practice**.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

London

Ashley P. Winton
44.020.3023.5121
ashleywinton@paulhastings.com

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

Brent Hoard
1.212.318.6524
brenthoard@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com