Published on *The National Law Review* https://natlawreview.com

EU-US Privacy Shield to Launch August 1, Replacing Safe Harbor

Article By:

Cynthia J. Larose

Susan L. Foster, Ph.D.

I. Introduction: Privacy Shield to Go Live August 1 (at Last)

The replacement for ***Safe Harbor*** is finally in effect, over nine months after Safe Harbor was struck down by the Court of Justice of the EU in the ***Schrems*** case. As most readers will be aware, ***Privacy Shield*** provides an important legal mechanism for transferring personal information from the EU to the US. The Department of Commerce (Commerce) has promised to launch a Privacy Shield website on August 1, 2016 that will allow companies to certify compliance with Privacy Shield.

The Privacy Shield documents are comprised of a 44-page "Adequacy Decision" and 104 pages of "Annexes" that contain key information concerning Privacy Shield's standards and enforcement mechanisms. Companies that are considering certifying under Privacy Shield should review the entire Adequacy Decision and its Annexes, as well as the promised FAQs and other documents that the Department of Commerce will provide on the new Privacy Shield website. A good starting point for companies is Annex II, which contains the essential Privacy Shield "Principles" and a set of "Supplemental Principles" that clarify certain points and provide useful examples for putting Privacy Shield into practice.

Our summary aims to highlight key points and provide a basic roadmap as companies start to get to grips with the new Privacy Shield requirements.

II. Privacy Shield Principles

The Principles set out in Privacy Shield will be largely familiar to companies that had certified under Safe Harbor, but Privacy Shield contains a lot more detail and occasionally demands more stringent standards and actions than Safe Harbor.

1. Notice. Notice must be provided as soon as possible to the individual – preferably at the time the individual is asked to provide personal information. Notice must be given in "clear and conspicuous language." The company must tell the individual that it participates in Privacy Shield, and must link to the Privacy Shield list that will be published on the Web by Commerce. The company must tell

individuals what types of personal information are being collected, for what purposes, and with whom it may be shared. Individuals must be told how to make complaints to the company and its options for resolving disputes (which the company must select from a menu of limited alternatives, as discussed further below). The company must inform the individual of the company's obligation to disclose personal information in response to lawful requests by public authorities, including for national security or law enforcement. A new requirement calls for the company to describe its liability with regard to transfers of the personal information to third parties (also discussed further below).

2. Choice. Choice comes into play primarily when the data controller wants to disclose personal information to a third party (other than agents under a contract) or use it for a purpose that is materially different than the purpose for which it was collected (which would have been communicated to the individual under the Notice principle). In many instances, consent can be obtained on an opt-out basis, provided that the new use or transfer has been disclosed clearly and conspicuously, and the individual is given a "readily available" means to exercise her choice. Critically, however, the transfer and processing of "sensitive" information requires the ***affirmative express consent*** of the individual, subject to a short list of exceptions described in the Supplemental Principles. An opt-out is not sufficient for sensitive information, which includes medical/health, race/ethnicity, political opinions, religious or philosophical beliefs, trade union membership, and information about sexuality. (As before, financial information is not considered sensitive, but companies should recall that risk-based security measures still need to be taken even if opt-out consent is used.)

3. Accountability for Onward Transfer. This Principle contains some key differences from Safe Harbor and should be carefully reviewed by companies looking at Privacy Shield. Privacy Shield has tightened up the requirements for transferring personal information to a third party who acts as a data controller. It is not possible simply to rely on the transferee being Privacy Shield-certified. The transferor company must enter into a contract with the transferee company that specifies that the information will only be processed for "limited and specified purposes consistent with the consent provided by the individual" and that the transferee will comply with the Principles across the board. If the transferee is acting as the transferor's agent (i.e., as a "data processor" in EU terminology) then the transferor must also take "reasonable and appropriate steps" to ensure that the transferee is processing the personal information consistently with the Principles. In all cases, the transferee must agree to notify the transferor if the transferee can no longer meet its privacy obligations. Commerce can request a summary or copy of the privacy provisions of a company's contracts with its agents.

4. Security. The standard for data security is "reasonable and appropriate measures" to protect personal data from being compromised, taking into account the nature of the personal information that is being stored. It's strongly implied that companies need to perform a risk assessment in order to determine precisely what measures would be reasonable and appropriate. The risk assessment and security measures should be documented in the event of an investigation or audit, and for purposes of the required annual internal review.

5. Data Integrity and Purpose Limitation. Indiscriminate collection of personal information is not permitted under Privacy Shield. Instead, personal information should be gathered for particular purposes, and only information that is relevant to those purposes can be collected. It's not always possible to anticipate every purpose for which certain personal information might be used, so Privacy Shield allows use for additional purposes that are "not incompatible with the purpose for which it has been collected or subsequently authorized by the individual." The benchmark for compatible processing is "the expectations of a reasonable person given the context of the collection." Generally speaking, processing personal information for common business risk-mitigation reasons, such as anti-

fraud and security purposes, will be compatible with the original purpose. Personal information cannot be retained for longer than it is needed to perform the processing that is permitted under this Principle. Additionally, companies have an affirmative obligation to take “reasonable steps” to ensure that the personal information they collect and store is “reliable for its intended use, accurate, complete, and current.” These requirements imply that periodic data cleaning may be necessary for uses that extend over a significant period of time.

6. Access. Individuals have the right to know what personal information a company holds concerning them, and to have the information corrected if it is inaccurate, or deleted if it has been processed in violation of the Privacy Shield Principles. There are a couple of exceptions: If the expense providing access is disproportionate to the risks to the individual’s privacy, or if another person’s rights would be violated by giving access, then a company can decline. Companies should use this option sparingly and document its reasons for refusing any access requests.

7. Recourse, Enforcement & Liability. One of the EU Commission’s main objectives in negotiating Privacy Shield was to ensure that the program had sharper teeth than Safe Harbor. Privacy Shield features more proactive enforcement by Commerce and the FTC, and aggrieved individuals who feel their complaints haven’t been satisfactorily resolved can bring the weight of their local DPA and Commerce to bear on the offending company. We describe the recourse, enforcement and liability requirements below in a separate section.

III. Privacy Shield Supplemental Principles

The Supplemental Principles in Annex 2 elaborate on some of the basic Principles (summarized above) and, in some cases, qualify companies’ obligations. The summary below highlights some significant points – but again, companies should read the Supplemental Principles in full to appreciate some of the nuances of the Privacy Shield requirements.

1. Sensitive Personal Data. This section sets out some exceptions to the affirmative opt-in consent requirement that mirror the exceptions in the EU Data Protection Directive.

2. Journalistic Exceptions. Privacy Shield acknowledges the significance of the First Amendment in US law. Personal information that is gathered for journalistic purposes, including from published media sources, is not subject to Privacy Shield’s requirements.

3. Secondary Liability (of ISPs, etc.) Companies acting as mere conduits of personal information, such as ISPs and telecoms providers, are not required to comply with Privacy Shield with regard to the data that travels over their networks.

4. Due Diligence and Audits. Companies performing due diligence and audits are not required to notify individuals whose personal information is processed incidental to the diligence exercise or audit. Security requirements and purpose limitations would still apply.

5. Role of the Data Protection Authorities. The Supplemental Principles describe the role of the DPA panels and the DPAs generally in greater detail. As discussed above, companies processing their own human resources information will be required to cooperate directly with the DPAs, and the Supplemental Principles seem to imply that cooperation includes designating the DPA Panels as those companies’ independent recourse mechanism. In addition to the fees attendant on this choice (capped at $500/year), companies will have to pay translation costs relating to any complaints against them.

6. Self-certification. This section outlines what the self-certification process should look like when the Privacy Shield enrollment website launches. It also contains information about what will happen when a Privacy Shield participant decides to leave the program.

7. Verification. Privacy Shield-certified companies must back up their claims with documentation. We discuss this further in the section below on enforcement.

8. Access. This section describes access requirements in more detail and also gives some guidance as to when access requests can be refused.

9. Human Resources Data. Companies planning to use Privacy Shield for the transfer of EU human resources data will want to review this section carefully. Privacy Shield does not replace or relieve companies from EU employment law obligations. Looking beyond the overseas transfer element, it's critical to ensure that employee personal information has been collected and is processed in full compliance with applicable EU laws concerning employees.

10. Contracts for Onward Transfers. US companies are sometimes unaware that all EU data controllers are required to have data processing contracts in place with any data processor, regardless of the processor's location. Participation in Privacy Shield, by itself, is not enough. If a Privacy Shield-certified data controller wants to transfer the EU-origin personal information to another data controller, it can do so under a contract that requires the transferee to provide the same level of protection as Privacy Shield, except that the transferee can designate an independent recourse mechanism that is not one of the Privacy Shield-specific mechanisms. **Companies will need to review their existing and new contracts carefully.**

11. Dispute Resolution and Enforcement. We discuss this separately below.

12. Choice – Timing of Opt Out (Direct Marketing). This section focuses on opt-out consent for direct marketing. Companies should provide opt-out choices on all direct marketing communications. The guidance states that "an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes." However, companies should keep in mind that the European standard for impracticability here may be tougher than we would expect in the US. In particular, US companies should consider EU requirements for direct marketing via e-mail or text, which typically requires advance consent unless the marketing is to an existing customer and is for goods or services that are similar to the ones previously purchased by the customer.

13. Travel Information. Common sense prevails with regard to travel data – when travel arrangements are being made for an EU employee or customer, the data transfer can take place outside of the Privacy Shield requirements if the customer has given "unambiguous consent" or if the transfer is necessary to fulfill contractual obligations to the customer (including the terms of frequent flyer programs).

14. Pharmaceutical and Medical Products. Pharma companies will want to review the fairly lengthy discussion of how Privacy Shield applies to clinical studies, regulatory compliance, adverse event monitoring and reporting, and other issues specific to the pharma industry. Privacy Shield is broadly helpful – and in some respects clearer than the pending GDPR.

15. Public Record and Publicly Available Information. Some, but not all, of the Principles apply to information obtained from public records or other public sources, subject to various caveats that make this section important to read in full.

16. Access Requests by Public Authorities. Privacy Shield companies have the option of publishing statistics concerning requests by US public authorities for access to EU personal information. However, publishing such statistics is not mandatory.

III. Recourse, Enforcement and Liability

A significant change in Privacy Shield from Safe Harbor is the addition of specific mechanisms for recourse and dispute resolution. One of the major perceived failings of Safe Harbor was that EEA citizens had no reasonable means to obtain relief or even to lodge a complaint. In order to satisfactorily self-certify, US companies will need to put processes in place to handle complaints.

Under Privacy Shield, at a minimum, such recourse mechanisms must include:

1. Independent Investigation and Resolution of Complaints: Readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual ... and damages awarded where the applicable law or private-sector initiatives provide;

2. Verification that You Do What You Say: Follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented, and in particular, with regard to cases of non-compliance; and

3. You Must Fix the Problems: Obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Prompt response to complaints is required and if a company uses an EU Data Protection Authority as a third party recourse mechanism and fails to comply with its advice within 25 days, the DPA may refer the matter to the FTC and the FTC has agreed to give priority consideration to all referrals of non-compliance from EU DPAs.

The verification requirement is more robust than under Safe Harbor. Companies may choose to either self-assess such verification or engage outside compliance reviews. Self-assessment includes certifying that its policies comply with the Principles and that it has procedures in place for training, disciplining misconduct and responding to complaints. Both outside compliance reviews and self-assessment must be conducted once a year.

Privacy Shield certifying organizations have responsibility for onward transfers and retains liability under the Principles if its third party processor violates the Principles, with some exceptions. Third party vendor management and contractual requirements for compliance with the Principles will be important components to manage the risk.

Dispute Resolution

There is ample ground for operational confusion under Privacy Shield, but none more so than with respect to dispute resolution. There are multiple methods available to data subjects (individuals) to

lodge complaints, and companies subscribing to Privacy Shield must be prepared to respond through any of those. When companies certify under Privacy Shield, they need to choose an independent enforcement and dispute resolution mechanism. The choices are either:

- Data Protection Authority Panels
- Independent Recourse Mechanism

a. *Individuals* – Individual data subjects may raise any concerns or complaints to the company itself, which is obligated to respond within 45 days. Individuals also have the option of working through their local DPA, which may in turn contact the company and/or the Department of Commerce to resolve the dispute.

b. *Independent Recourse* – As discussed above, the Privacy Shield requires that entities provide an independent recourse mechanism, either a private sector alternative dispute resolution provider (such as the American Arbitration Association, BBB, or TRUSTe) or a panel of European DPAs. NOTE THAT THE DPA PANEL IS MANDATORY IF YOU ARE APPLYING TO PRIVACY SHIELD TO PROCESS/TRANSFER HR DATA. For disputes involving HR data that are not resolved internally by the company (or any applicable trade union grievance procedures) to the satisfaction of the employee, the company must direct the employee to the DPA in the jurisdiction where the employee works.

c. *Binding Arbitration* – A Privacy Shield Panel will be composed of one or three independent arbitrators admitted to practice law in the US, with expertise in US and EU privacy law. Appeal to the Panel is open to individuals who have raised complaints with the organization, used the independent recourse mechanism, and/or sought relief through their DPA, but whose complaint is still fully or partially unresolved. The Panel can only impose equitable relief, such as access or correction. Arbitrations should be concluded within 90 days. Further, both parties may seek judicial review of the arbitral decision under the US Federal Arbitration Act.

Enforcement

In addition to the above discussion on the multiple avenues available to data subjects for complaints, there are other expanded types of enforcement under Privacy Shield. A certifying organization's compliance may be directly or indirectly monitored by the US Department of Commerce, the FTC (or Department of Transportation), EU DPAs, and private sector independent recourse mechanisms or other privacy self-regulatory bodies.

Privacy Shield brings an expanded role to the Department of Commerce for monitoring and supervising compliance. If you have following Safe Harbor, one of the EU grounds for disapproval was the apparent lack of actual enforcement by US regulatory authorities against self-certifying organizations. The Department of Commerce has committed to a larger role and has greatly increased the size of the program staff.

Some of the new responsibilities of the Department of Commerce under Privacy Shield include:

- Serving as a liaison between organizations and DPAs for Privacy Shield compliance issues;
- Conducting searches for false claims by organizations that have never participated in the program and taking the aforementioned corrective action when such false claims are found.
- Conducting *ex officio* investigations of those who withdraw from the program or fail to recertify to verify that such organizations are not making any false claims regarding their

participation. In the event that it finds any false claims, it will first issue a warning, and then, if the matter is not resolved, refer the matter to the appropriate regulator for enforcement action; and

- Conducting periodic *ex officio* compliance reviews which will include sending questionnaires to participating organizations to identify issues that may warrant further follow up action. In particular, such reviews will take place when the Department has received complaints about the organization's compliance, the organization does not respond satisfactorily to its inquiries and information requests, or there is "credible" evidence that the organization does not comply with its commitments. Organizations will be required to provide a copy of the privacy provisions in their service provider contracts upon request. The Department of Commerce will consult with the appropriate DPAs when necessary;
- Verifying self-certification requirements by evaluating, among other things, the organization's privacy policy for the required elements and verifying the organization's registration with a dispute resolution provider;

Private sector independent recourse mechanisms will have a duty to actively report organizations' failures to comply with their rulings to the Department of Commerce. Upon receipt of such notification, the Department will remove the organization from the Privacy Shield List.

The above overview illustrates the complexity of Privacy Shield vs. Safe Harbor and the multiplication of authorities in charge of oversight, all of which is likely to result in greater regulatory scrutiny of and compliance costs for participating organizations. By way of contrast, when an organization relies on alternative transfer mechanisms such as the Standard Clauses, the regulatory oversight is performed by EU regulators against the EU company (as data exporter). Therefore, before settling on a transfer mechanism, organizations will want to consider the regulatory involvement and compliance costs associated with each option.

IV. Choosing Your Next Steps

Privacy Shield may not appeal to all US companies. Privacy Shield allows for a degree of flexibility in handling new data flows. However, that comes at the costs of fees, rigorous internal reviews and arguably much more onerous audits and enforcement than the two main alternatives, Binding Corporate Rules for intra-group transfers, and Standard Clauses for controller-to-controller or controller-to-processor transfers (regardless of corporate affiliation). Data transfers within corporate groups may be better addressed by Binding Corporate Rules that speak specifically to the groups' global privacy practices – or even by the Standard Clauses, particularly for smaller corporations with only a few affiliates. Even outside corporate groups, the Standard Clauses may be adequate if the data flows are straightforward and unlikely to change much over time. An important point to note is that, in comparison to Safe Harbor, Privacy Shield requires more detailed company-to-company contracts when personal information is to be transferred – it's no longer enough that both companies participate in the program. US companies should consider the potential operational benefits of Privacy Shield against its increased burdens.

It is important to consider timing. The Commerce Department Privacy Shield website will be "open for business" as of August 1. Lest you despair about the possibility of analyzing and updating those contracts that implicate the Accountability for Onward Transfer Principle in order to certify to Privacy Shield, Annex II has provided a bit of a "grace period" for what have been called early joiners.

> *The Privacy Principles apply immediately upon certification. Recognizing that the Principles will impact commercial relationships with third parties, organizations that certify to the Privacy*

Shield Framework in the first two months following the Framework's effective date shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which they certify to the Privacy Shield. During that interim period, where organizations transfer data to a third party, they shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.

If your company determines that Privacy Shield is the right choice, and you are diligent about the ground work required to accurately certify before that two-month window closes, you will be able to take advantage of the nine-month grace period to get those third party relationships into line.

Finally, US companies should stay alert to the legal challenges that the Standard Clauses are currently facing (again driven by concerns about mass surveillance), the possibility that EU regulators may start exacting further commitments when approving BCRs, and the very high likelihood that new legal challenges will be mounted against Privacy Shield shortly after it is implemented. Even if a company adopts Privacy Shield, or instead elects to stick with the Standard Clauses, it may want to get ready to switch if one or the other is struck down by the Court of Justice of the EU. Of course, if the Court of Justice strikes down both Privacy Shield and the Standard Clauses, it will be back to the drawing board for EU and US government negotiators.

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume VI, Number 208

Source URL:https://natlawreview.com/article/eu-us-privacy-shield-to-launch-august-1-replacing-safe-harbor