Insight

IN-DEPTH DISCUSSION

JULY 13, 2016

The Privacy Shield: What U.S. Multinational Employers Need To Know To Enjoy The Benefits Of The Newest EU-U.S. Data Transfer Mechanism

BY PHILIP L. GORDON

Since the European Court of Justice declared invalid, on October 6, 2015,[1] the Safe Harbor agreement between the U.S. Department of Commerce and the European Commission for the transfer of personal data, hundreds of U.S. multinationals have been struggling to find an alternative while waiting hopefully for the Safe Harbor's replacement. The Privacy Shield, effective as of July 12, 2016, may provide the alternative these organizations have been seeking. For U.S. multinationals that relied on the Safe Harbor to transfer human resources data from EU subsidiaries to their U.S. parent corporation, the Privacy Shield will seem familiar notwithstanding U.S. and EU officials' public pronouncements that this new data transfer mechanism substantially enhances the now much-maligned Safe Harbor. Nonetheless, U.S. multinationals should consider several caveats before strapping on the Privacy Shield.

Basic Steps To Enjoy The Privacy Shield's Benefits

As with the Safe Harbor, the basic steps necessary to enjoy the Privacy Shield's benefits are straightforward. An eligible[2] U.S. organization must self-certify on the Commerce Department's recently launched Privacy Shield website and publish a Privacy Shield Privacy Policy that embodies the Privacy Shield Privacy Principles. U.S. organizations will be able to self-certify beginning August 1, 2016.

Self-certifying for transfers of human resources data in the context of the employment relationship is substantially the same as self-certifying for transfers of other types of personal data. The organization will be required to provide basic information, including, for example, the organization's

1 Philip Gordon and Tahl Tyson, *What Does The European Court of Justice's Invalidation Of the U.S. – EU Safe Harbor Framework Mean for U.S.-Based Multinational Employers?*, Littler Insight (Oct. 6, 2015).

2 The certifying entity must be subject to the jurisdiction in the U.S. of either the Federal Trade Commission or the Department of Transportation.

contact information, information about the data transfer, and information about the organization's privacy policy. A corporate officer must sign the self-certification form.

Self-certification for transfers of HR data entails one critical distinction from other types of data transfers. The organization is required to choose EU data protection authorities ("DPAs") from among the several available independent dispute resolution mechanisms. The implications of this mandatory selection are discussed below. In addition, organizations must pay a fee that will not exceed $500 USD, and will be less for smaller companies, to subsidize this dispute resolution mechanism.

The "human resources privacy policy" submitted with the self-certification must contain the same mandatory elements as other Privacy Shield privacy policies. The policy must address the organization's commitment to all seven of the "Privacy Shield Privacy Principles" (the "Principles"). These Principles include Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse/ Enforcement and Liability. To satisfy the Commerce Department that the HR privacy policy fully addresses the Principles, the policy submitted by the certifying organization must contain a long list of required elements including, among others, the following:

1. An identification of all U.S. affiliates that will access transferred personal data and their commitment to adhere to the Principles;
2. The categories of personal data collected;
3. The purposes for the collection;
4. The third parties to which data may be transferred;
5. A description of data subjects' access rights; and
6. A contact for requests to exercise individual rights and submit complaints.

There is one significant distinction between an HR privacy policy and privacy policies addressing other types of personal data under the Privacy Shield. The HR privacy policy does not have to be posted on a publicly available website. Instead, the policy must be posted where it will be available to all EU-based employees whose personal data will be transferred to the U.S. subject to the Privacy Shield. This typically means that the policy will be posted on the corporate intranet. Organizations that choose not to publicly post their HR privacy policy will be required to submit the policy with the self-certification form rather than just providing a link.

Once the certifying organization completes these basic steps, the Commerce Department will review the self-certification form, to confirm that required information has been provided, and the HR privacy policy, to confirm that it addresses all required elements. If so, the Commerce Department will list the U.S. parent corporation and any certifying affiliates on its Privacy Shield List. Immediately after the listing, the EU subsidiaries can begin transferring their employees' personal data to the U.S. Because the European Commission has determined that the Privacy Shield "ensures an adequate level of protection for personal data," the EU subsidiaries will not need to obtain additional approvals from local DPAs, albeit in some countries, such as France, the DPA must be notified of the data transfer.

The Privacy Shield can be used to transfer personal data of both current and former EU employees. The U.S. parent corporation must apply the Principles to all transferred data for as long as that information is retained, even if the parent corporation subsequently decides to withdraw from the Privacy Shield. An organization that withdraws from the Privacy Shield will be required to satisfy the annual verification and recertification requirements (discussed below) for as long as the organization retains personal data transferred pursuant to the Privacy Shield.

Not So Simple: Implementing A Privacy Shield Compliance Program For Transfers Of HR Data

Satisfying the formal requirements for self-certification generally will be straightforward, but achieving meaningful compliance that mitigates enforcement risk will be far more complicated, and enforcement risk, particularly for transfers of HR data, has increased materially. To begin with and as discussed in detail below, virtually all enforcement will take place in the EU, *not* the U.S. Second, EU DPAs, particularly in countries like France, Germany and Spain, appear to be primed to flex their enforcement muscle. Third, while EU employees may not grasp all the nuances of the debate over the Safe Harbor, they and their works council or trade union have become generally leery of large-scale transfers of HR data to the U.S. As a result, they are readier than ever to complain, especially if they sense that the U.S. parent corporation is not taking data protection seriously.

To demonstrate its commitment to compliance to its EU employees (and their representatives) and, if needed, to regulators, the U.S. parent corporation should consider taking the following steps:

1. Confirm That EU Subsidiaries Comply With Local Requirements For Cross-Border Data Transfers To The U.S.

The Privacy Shield framework document emphasizes that the "Privacy Shield Principles are relevant only when [HR data is] transferred or accessed" and that collection and processing of HR data "prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected." Supplemental Principles §III.9.a.i. As a practical matter, this requirement to comply with local laws means that EU subsidiaries must take the following steps before transferring their employees' personal data to the U.S. pursuant to the Privacy Shield: (a) provide their employees with notice of data processing, including transfer to the U.S. pursuant to the Privacy Shield; (b) consider local law restrictions on cross-border data transfers, particularly on transfers of sensitive personal data, such as employees' health information; (c) confer with works councils or trade unions, if any and if legally required, concerning data transfers to the U.S.; and (d) depending on the country, register with or notify the local DPA of data processing, including cross-border data transfers.

In a world where technology permits a small or medium-sized U.S. business to be a multinational employer, many EU subsidiaries of organizations that will certify to the Privacy Shield are only small sales offices or factories with no locally assigned human resources professional or legal counsel. As a result, these subsidiaries likely will address compliance with local data protection laws for the first time when the U.S. parent corporation decides to transfer EU employees' personal data to the U.S.

2. Establish Policies And Procedures To Implement The Privacy Shield Privacy Principles

While the HR privacy policy submitted to the Commerce Department will contain the high-level principles that should guide the handling of EU employees' personal data transferred to the U.S., that policy typically will not instruct U.S.-based HR professionals, payroll personnel, managers and others on exactly what it is they need to be doing to achieve compliance. For example, the Privacy Shield framework document requires certifying organizations to satisfy the Security Principle by "tak[ing] reasonable and appropriate measures to protect [transferred personal data] from loss, misuse and unauthorized access, disclosure, alteration and destruction." Principles, §II.4.a. However, that document identifies no specific measures to be taken.

Because there is a similar lack of detail for most of the other Principles, certifying organizations will need to develop detailed policies and procedures to implement the Principles. Some of those policies and procedures are described below.

a. *Notice And Choice Principles*

U.S. multinational employers typically will transfer EU employees' personal data to the U.S. to store it in a centralized human resources information system ("HRIS") that facilitates global workforce management.

Given this purpose, the HR privacy policy likely will inform the EU workforce only about the use and disclosure of their personal data for HR administration purposes.

If the U.S. parent subsequently were to use transferred personal data for other purposes, such as to market the company's products to the EU workforce or to support a global charitable campaign, it would be required to give EU employees the opportunity to opt out from the previously undisclosed use. According to the Privacy Shield framework document, such "choices must not be used to restrict employment opportunities or take any punitive action against such employee." Supplemental Principles §III.9.b.i. In other words, EU employees cannot be confronted with a choice between consenting to the new use or losing their job.

As a benefit to employers, the Privacy Shield specifically excludes from the Notice and Choice Principles processing EU employees' personal data for "promotions, appointments or other similar employment decisions." This exclusion applies only "[t]o the extent and for the period necessary to avoid prejudicing" the decision-making process. Supplemental Principles §III.9.b.iv. This exclusion should help to avoid a situation where notice disrupts the employment decision-making process.

To handle transferred data in compliance with the Notice and Choice Principles, the certifying organization should consider implementing several policies and practices. By way of illustration, it should specifically identify the categories of employees authorized to access EU employees' personal data; the categories of data that can be accessed; the permissible purposes for access, use and disclosure; and the steps to be taken before using such data for a purpose not previously disclosed in the HR privacy policy or otherwise.

b. *Accountability For Onward Transfer Principle*

Under the Accountability For Onward Transfer Principle, certifying organizations must require, by written agreement, that third parties who receive transferred personal data provide the same level of protection for that data as required by the Privacy Shield. The U.S. parent corporation must enter into these "onward transfer agreements" with both agents, such as HR service providers, and non-agents that will use transferred personal data for their own purposes. Organization that certify to the Privacy Shield within sixty days of its effective date (*i.e.*, September 10, 2016) will have nine months from the date listed on the Privacy Shield List to bring contracts with third parties into conformance with this Principle.

The Privacy Shield establishes an important exception from the requirements described above for cross-border data transfers within a corporate group. The U.S. parent corporation can make such transfers without an "onward transfer agreement" provided that "other instruments, such as EU Binding Corporate Rules [BCRs] *or other intra-group instruments (e.g., compliance and control programs),* ensuring the continuity of protection of personal information under the Privacy Shield Principles" have been implemented. Supplemental Principles §III.10.b.i (emphasis supplied). The italicized phrase gives U.S. parent corporations greater flexibility because it allows them to forego not only onward transfer agreements but also the potentially onerous process of implementing BCRs when those organizations need to share EU employees' personal data with non-U.S. and non-EU affiliates, for example, when an HR director for Europe, the Middle East, and Africa ("EMEA") resides in the United Arab Emirates.

c. *Security Principle*

To satisfy this Principle, the U.S. organization will need to implement specific measures, such as access controls, restrictions on storage of EU personal data on portable storage media, safeguards for paper records containing EU personal data, and secure methods of document disposal. The organization may be able to leverage for this purpose policies and practices used to safeguard other types of sensitive employee data, such as Social Security numbers and protected health information subject to the Health Insurance Portability and Accountability Act ("HIPAA").

d. *Access Principle*

Under the Access Principle, individuals have the right to access their personal data, to correct personal data that is inaccurate, and to delete personal data that the U.S. organization processes in violation of the Principles. However, the detailed procedures established by the Privacy Shield framework for implementing these rights have limited applicability to HR data transferred in the context of the employment relationship.

The Privacy Shield dictates that "employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, *regardless of the location of data processing and storage."* Supplemental Principles §III.9.c.i (emphasis supplied). The Privacy Shield also mandates, in light of EU employees' rights under local law, that the U.S. parent corporation "cooperate in providing such access either directly or through the EU employer." *Id.* Consequently, certifying organizations will need to implement policies and procedures to facilitate a coordinated response to requests by EU employees to exercise their rights to access, amend and delete their personal data.

3. Establish An Annual Verification Process

The Privacy Shield requires that certifying organizations recertify annually, and that before recertification, they verify on-going compliance with the Principles. The verification can be conducted as a self-assessment or by an outside entity. In either case, the certifying organization must verify that the attestations in its self-certification and assertions in its HR privacy policy are true and that "privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles." Supplemental Principles §III.7.a.

To meet those standards, organizations that choose to conduct a self-assessment must verify that:

a. The HR privacy policy is "accurate, comprehensive, prominently displayed, completely implemented and accessible";

b. The HR "privacy policy conforms to the Privacy Shield Principles";

c. Individuals are informed how to submit complaints, both internally and to the relevant EU data protection authority;

d. Employees with access to transferred personal data have received training and will be disciplined for policy violations; and

e. The organization conducts periodic compliance reviews.

Supplemental Principles §III.7.c. The verification must be signed by an authorized corporate representative and must be produced upon request to employees, or in the context of an investigation or complaint proceeding.

4. Be Prepared To Resolve Complaints In The EU

As noted above, U.S. organizations that certify to the Privacy Shield to transfer HR data are required to agree to cooperate with investigations by, and abide by the advice of, EU data protection authorities. Notwithstanding this certification by the U.S. parent corporation, the Privacy Shield framework document emphasizes that even after HR data is transferred, "primary responsibility for that data vis-à-vis the employee remains with the organization in the EU." Supplemental Principles §III.9.d.i. Consequently, the framework document provides that EU employees who are not satisfied with the internal resolution of their data protection complaints "should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work" even if the U.S. partent corporation is responsible for the alleged violation. Supplemental Principles §III.9.d.i.

To fulfill its representation in the self-certification form, the U.S. parent corporation would be required to participate in the complaint proceeding in the EU with its EU subsidiary. Significantly, this proceeding will be governed by the relevant EU Member State's law and not by the Principles or U.S. law. In addition, the U.S. parent corporation will be required to abide by the advice of the DPA, which could include an order to implement remedial measures and/or to compensate the employee.

Should U.S. Multinational Employers Certify To The Privacy Shield?

Since the Privacy Shield was initially announced in early February 2016,[3] many U.S. multinational employers have confronted the question whether to rely on the Privacy Shield as a data transfer mechanism once it will have been finalized. While waiting for the finalization, some of these organizations implemented as a data transfer mechanism the Standard Contractual Clauses (the "Clauses"), which are form agreements approved by the European Commission as ensuring an adequate level of protection for personal data transferred outside the EU. Others have taken a wait-and-see approach. With the Privacy Shield now finalized, these organizations will need to decide whether to certify. In doing so, they should take three principal considerations into account.

First, the Privacy Shield's validity remains subject to substantial uncertainty. To begin with, Max Schrems, who filed the original challenge to the Safe Harbor, already has indicated his intent to initiate proceedings with the aim of forcing a review of the Privacy Shield by the European Court of Justice ("ECJ").[4] The lengthy critiques of the official draft of the Privacy Shield by the Article 29 Working Party in April 2016 and the European Data Protection Supervisor in June 2016 provide a playbook for such a legal challenge and would give it immediate credibility, particularly because the European Commission did not revise the draft to address many of the criticisms.

Second, the Privacy Shield could soon be materially revised. The Privacy Shield is designed to ensure compliance with the EU's current data protection framework document, the Data Protection Directive (the "Directive"). In May 2018, the General Data Protection Regulation ("GDPR") will replace the Directive.[5] It is unclear whether the European Commission is planning to address this change in the applicable legal regime by revising the Privacy Shield. In its critique, the Article 29 Working Party raised concerns that the Privacy Shield does not provide an adequate level of protection as required by the GDPR.

Finally, certifying to the Privacy Shield may materially increase enforcement risk for the U.S. parent corporation. Both EU employees and data protection authorities are more closely scrutinizing U.S. multinationals' data handling processes. Certifying to the Privacy Shield would facilitate the local DPA's extension of its enforcement authority to the U.S. parent corporation.

In sum, the Privacy Shield's finalization may make U.S. multinationals' handling of cross-border transfers of EU employees' personal data more, not less, complicated than ever. Consequently, these organizations should undertake a thorough (and privileged) review of their current data protection practices for EU employees' personal data, evaluate the available options for transfers of EU employee data to the U.S., and implement the data transfer mechanism that suits the corporate group best. As demonstrated by recent enforcement actions in Germany against U.S. multinationals for continued reliance on the invalidated Safe Harbor, the time for a wait-and-see approach to implement an alternative to the Safe Harbor has passed.

This article was first published in the International Association of Privacy Professionals' Privacy Tracker blog.

3 Philip Gordon, *EU and US Beat The Clock With Their Announcement Of The "Privacy Shield" a/k/a Safe Harbor 2.0*, Littler ASAP (Feb. 3, 2016).

4 Notably, Max Schrems recently submitted a complaint with the Irish Data Protection Commissioner alleging that the Standard Contractual Clauses do not ensure an adequate level of protection for personal data transferred to the U.S.

5 Philip Gordon, *Ten Steps For U.S. Multinational Employers Towards Compliance With Europe's New Data Protection Framework – The General Data Protection Regulation*, Littler Insight (Jan. 21, 2016).