Kilpatrick

Insights: Alerts

Privacy Shield or Model Clauses: Which is Better for You?

March 1, 2016

Written by **Jon Neiditz** and **Meghan K. Farmer**

Yesterday the European Commission released a draft "adequacy decision" on the protection provided by the EU-U.S. Privacy Shield together with the texts that will constitute the EU-U.S. Privacy Shield framework. Once adopted (and if not successfully challenged), the Commission's adequacy finding will establish that the safeguards provided when data are transferred under the new EU-U.S. Privacy Shield are equivalent to data protection standards in the EU. In light of today's announcement, and even though the Privacy Shield may not be available until the summer, many U.S. companies are already beginning to consider whether to self-certify to the Privacy Shield framework or maintain the standard contractual clauses that they have adopted either before the demise of the Safe Harbor Framework or in response to that demise.

The Privacy Shield is designed to impose stronger obligations on U.S. companies for protecting the personal data of Europeans than were afforded by the previous Safe Harbor Framework. As a result, the Privacy Shield also imposes stricter obligations on companies than do the model contractual clauses in certain respects. Privacy Shield requirements and processes related to enforcement, compliance review and complaint handling are more onerous for companies than the requirements imposed by the model clauses. Although self-certification to the Privacy Shield may provide a more streamlined mechanism for legalizing transfers of personal data from the EU to the U.S. for companies (such as cloud providers) for which entering into numerous agreements containing model contractual clauses is cumbersome, or for companies that frequently engage subcontractors who cannot or will not agree to comply with the model clauses, there are also important tradeoffs to consider.

Monitoring and Enforcement

A key component of the Privacy Shield is that it provides for stronger monitoring and enforcement of compliance. Companies that self-certify to the Privacy Shield will be subject to greater scrutiny by regulators under the Framework than under the model clauses. The model clauses provide for enforcement and oversight by independent arbitrators and, in the case of Human Resources data, national/local Data Protection Authorities (DPAs). Oversight and enforcement of the Privacy Shield, by contrast, may be conducted by a number of bodies including the U.S. Department of Commerce, the Federal Trade Commission (FTC), the Department of Transportation, other U.S. "statutory bodies that will effectively ensure compliance with the Principles," independent dispute resolution bodies, the Privacy Shield Panel and, in certain cases, DPAs.

Companies can expect that the new agreement will be subject to a great deal of scrutiny on both sides of the Atlantic, and as a result, the FTC will likely play a more active role in enforcement of the Privacy Shield than it did under the Safe Harbor framework. The FTC has committed to reviewing referrals alleging non-compliance with the principles that it received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU member states; and (iii) the Department of Commerce. Participation in the Privacy Shield framework will subject organizations to the FTC's jurisdiction, where they might not have been under the model clauses.

The Department of Commerce will also be taking on an expanded enforcement role under the new framework. The Department's responsibilities will include conducting *ex officio* compliance reviews of self-certified organizations, receiving, reviewing and undertaking to resolve complaints of non-compliance, verifying companies' registration with an independent recourse mechanism, and removing non-compliant organizations from the Privacy Shield List. The Department of Commerce will maintain and publish the list of U.S. organizations that have self-certified to the Privacy Shield. The Department of Commerce will also maintain an updated list of organizations that are no longer part of the framework setting out the reason for their removal from the list. The Department of Commerce will publish a list of organizations that had previously self-certified to the Department but that have been removed from the list, either for non-compliance or other reasons, and provide a warning that the organizations on the list are no longer participants in the Privacy Shield. This process may subject companies to speculation or negative public perception related to their removal from the list.

In addition, the Privacy Shield expressly provides for sanctions for non-compliance not provided for under the model clauses. Sanctions may include publicity for findings of non-compliance, requirement to delete data, removal of a seal, injunctive awards and compensation for individuals for losses incurred as a result of non-compliance.

Complaint Handling and Redress

In addition to increased monitoring and oversight, the Privacy Shield places more obligations on companies with respect to complaint handling and redress than the model clauses. Self-certifying organizations to the Privacy Shield will be required to:

- Respond to complaints within 45 days;
- Provide a response to the data subject that includes an assessment of the merits, and if the complaint has merit, information as to how the organization will rectify the problem;
- Designate an independent dispute resolution body in the EU or the U.S. to investigate and resolve individual complaints and provide recourse, free of charge to the individual;
- Respond promptly to requests for information from the Department of Commerce relating to their adherence to the principles;
- Retain records on the implementation of its privacy practices and make such records available upon request to the FTC or an independent recourse mechanism in the context of an investigation or complaint;
- Cooperate with DPAs in the investigation and resolution of complaints concerning the processing of human resources data, or where they have voluntarily submitted to the DPA's oversight.

Compliance Review

Companies' adherence to the Privacy Principles will be subject to ongoing compliance review. The Department of Commerce will systematically verify, during certification and re-certification, that an organization's policies conform to the principles. It will also conduct, on an ongoing basis *ex officio* compliance reviews of self-certified organizations. Companies self-certifying to the framework will be required to respond promptly to requests from the U.S. Department of Commerce relating to their adherence to the Privacy Principles and may be required to complete detailed questionnaires. Although it is not yet clear whether these requirements will be more or less burdensome in practice than the audit rights provided to data exporters and supervisory authorities under the model clauses, it is likely that the measures will be invoked more frequently under the Privacy Shield.

Advantages of the Privacy Shield

The Privacy Shield does offer certain advantages over the model clauses. For companies that have found the process of entering into numerous agreements containing the model clauses to be administratively burdensome, the Privacy Shield may provide a more streamlined mechanism for ensuring transfers of personal data from the EU to the U.S. are lawful. For companies, like cloud providers, that transfer personal data to the U.S. from numerous EU data controllers, the Privacy Shield may be an attractive solution.

The Privacy Shield framework may also streamline the process of entering into agreements with subcontractors. The model clauses require that subcontractors adopt the model clauses exactly as written. The Privacy Shield may be advantageous in this regard because, although it requires that subcontractors be contractually required to provide the same level of privacy protection as the Privacy Shield Principles, it does not require that the subcontractor adopt any language verbatim. Under the Accountability for Onward Transfer Principle, any onward transfer of personal data from an organization to controllers or processors can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Privacy Principles.

The Privacy Shield may also come to signify the commitment of your organization to the protection of personal information, a very important message to many organizations. Any such benefit, however, seems likely to be outweighed for such organizations by the mere prospect that if something went wrong they could be listed — with no right to be forgotten — on the Department of Commerce's new "wall of shame."

Companies that have been successful at implementing model clauses should carefully consider whether self-certification to the Privacy Shield is advantageous given the additional requirements. Although it may offer be a good solution for companies that face certain challenges with respect to implementing the model clauses, those that have had success with the model clauses may not want to subscribe to the additional requirements, oversight and possible enforcement that the Privacy Shield entails.

Finally, we expect the costs and benefits associated with these and other derogations to change substantially over the next few years and will be there to help you adjust to all such changes. The next shoe to drop, for example, could well be efforts to make model clauses substantially more onerous, given the incentive structure that is now being created.

To view a printer-friendly version of this alert, click here.

Related People

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com

Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com