Lowenstein Sandler

Client Alert / March 2016

PRIVACY AND INFORMATION SECURITY

PROPOSED PRIVACY SHIELD IMPOSES SIGNIFICANT NEW OBLIGATIONS ON US COMPANIES

By: Mary J. Hildebrand, CIPP/US/EU, Esq.

Article 29 Working Party Opinion Expected in Mid-April

The European Commission (EC) offered the US private sector its first glimmer of commercial certainty regarding data transfer from the EU since Safe Harbor was invalidated on October 15, with its release of the draft Privacy Shield on Monday, February 29. US companies would still be required to self-certify to the US Department of Commerce (DOC) on an annual basis and the US retains ultimate jurisdiction, but that's where the similarity to the Safe Harbor begins and ends.

As proposed, the Privacy Shield requires compliance with the Privacy Shield Principles and Supplementary Principles (Principles), which impose significant new obligations on US companies that import personal data from the EU, including a pledge not to collect any more data than is minimally necessary to conduct the processing required, and tighter restrictions and potential liability associated with the onward transfer of personal data. US companies are required to include these assurances and many others in their privacy policies, which will be regularly monitored by the DOC and enforced by the Federal Trade Commission (FTC) in close cooperation with EU data protection authorities (DPAs). Potential sanctions for violations by US companies may include exclusion from future data transfers.

Some key elements of the proposed Privacy Shield include:

The Principles: The Privacy Shield not only requires that the Principles be reflected in published privacy policies, but implementation must be verified at the time of self-certification and regularly thereafter. Failure to comply with the Principles may lead to removal from the list of qualified organizations published by the DOC, and a requirement that all applicable personal data be deleted or returned.

Notice: "Clear and conspicuous" notice must be provided when "individuals are first asked to provide personal information to the organization," regarding, among other things, the types of personal data collected, the purpose of such use and collection, and the type or identity of third parties to whom it may be disclosed.

Choice: Organizations must provide individuals with clear, conspicuous and readily available mechanisms to exercise choice regarding the disclosure of personal information to third parties, and for the use of personal information for a purpose that is "materially different" from the authorized purpose. Individual choice regarding "sensitive information" requires an express opt-in for such disclosure or use.

Accountability for Onward Transfer: Any onward transfer of personal data to a third party requires a written contract. If personal data is transferred to a controller, the US company must comply with Notice and Choice Principles prior to such transfer, and the transfer must be for a clearly delineated purpose. When the US company engages an agent, it must ensure that the agent will process the personal data in a manner that is consistent with the Principles; this is particularly important because the US company is responsible for the agent's compliance. There is a grace period of up to nine months to comply with the contractual requirements.

Security: There are no hard and fast rules regarding security protocols; however, security must be commensurate with the risk involved in the processing and the nature of the personal data.

Data Integrity and Purpose Limitation: Personal data collected must be "limited to the information that is relevant to the purpose of processing." Organizations may not process personal data in a way that is incompatible with the purpose for which it was collected or subsequently authorized by the individual. Reasonable steps must be undertaken to ensure that personal data is reliable for its intended use, accurate, complete and current.

Access: Individuals must have access to their personal data except where the burden or expense of providing access is "disproportionate to the risk to the individual's privacy." Notably, access does not have to be justified, but it's very clear that any refusal to provide prompt access must be supported by credible reasons consistent with the Principles.

Recourse, Enforcement and Liability: Individuals have recourse to several no-cost options if an organization fails to comply with the Principles, including a direct complaint against the organization (requiring resolution within 45 days); alternative dispute resolution using an independent third party; or registering complaints with their local DPA, who will coordinate with the FTC regarding the complaint. The final resort is binding arbitration.

Special Requirements for HR Data: Organizations that handle HR data transferred from the EU must agree at the time of self-certification to comply with recommendations rendered by a panel of DPAs specifically created to advise on individual complaints in the context of human resources and employment data. The DPA panel permits the parties a reasonable opportunity to comment and provide evidence. Any failure to abide by such advice within 25 days of its release may result in a referral to the FTC or another US agency with enforcement authority. For organizations that import any other category of personal data from the EU, agreement to comply with the advice rendered by DPA panels is voluntary.

Mergers: Organizations subject to the Privacy Shield must notify the DOC in advance of any planned merger, and if the surviving entity is not compliant with the Privacy Shield (or prepared to agree in writing to such compliance), then "any personal data…acquired under the Privacy Shield must be promptly deleted."

Monitoring and Enforcement: The DOC will actively monitor compliance by US organizations, including at each annual renewal of the Privacy Shield. The FTC has enforcement authority, including the right to pursue a noncompliant organization for violation of Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."

Limits on US Government Access: For the first time, the US Office of the Director of National Intelligence has provided written assurance that any access by public authorities for national security purposes will be subject to clear limits, safeguards and oversight mechanisms to prevent generalized access. An independent ombudsman in the US Department of State will be charged with determining whether any relevant laws have been violated.

Annual Joint Review: The EC and the DOC will conduct an annual joint review regarding all aspects of the Privacy Shield. Reviewers are empowered to draw on all sources of available information, including compliance by individual organizations. The EC will also hold an annual privacy summit in the EU, inviting all stakeholders to comment on developments in US privacy law and their impact on European citizens.

From the perspective of US organizations seeking firm parameters around data transfer from the EU to the US for business purposes, announcement of the Privacy Shield brings that goal a step closer. However, EU approval of the Privacy Shield, including an evaluation of the draft "adequacy decision" explaining why the Privacy Shield satisfies the standards for data privacy and security established by the *Schrems* decision, remains uncertain. Criticism of the European Commission's reasoning was immediate and quite pointed; in particular, commentators claim that the Privacy Shield fails to provide "essential equivalence" to EU standards, and the Judicial Redress Act signed into law by President Obama on February 24 fails to adequately provide EU citizens with an effective private remedy should the US government violate their rights. In fact, certain commentators have already announced that if the Privacy Shield is adopted "as is," they will challenge it in front of the European Court of Justice.

The Privacy Shield and the adequacy decision are now slated for review by a committee composed of representatives of EU member states and by the Article 29 Working Party, with an opinion expected in mid-April. In the interim, we should expect heightened scrutiny, commentary and criticism from all stakeholders, including the DPAs. Stay tuned.

contacts

Please contact the attorney named below for more information on this matter.

Mary J. Hildebrand, CIPP/US/EU, Esq.
973 597 6308
mhildebrand@lowenstein.com