Lowenstein Sandler

Client Alert / July 13, 2016

PRIVACY AND INFORMATION SECURITY

US-EU PRIVACY SHIELD ADOPTED

US organizations welcomed (finally) a replacement for Safe Harbor, but remained wary as judicial challenges to the Privacy Shield may lie ahead

By: Mary J. Hildebrand, CIPP/US/E

In a joint press conference in Brussels on Tuesday, July 12, European Union (EU) Commissioner Vera Jourova and US Secretary of Commerce Penny Pritzker announced final approval of the Privacy Shield. While negotiators expressed confidence in the new framework, prominent voices warned that shortcomings remained — particularly with respect to surveillance by US intelligence services. The Privacy Shield provides US organizations with another option for EU data transfer which, if it survives legal challenges, will contribute to the stability of cross-border commercial activity.

In the nine months since Safe Harbor was invalidated by the European Court of Justice (ECJ) in the *Schrems* decision, the Privacy Shield has been the subject of intense scrutiny by EU regulators and scores of industry groups. The Article 29 Working Party (WP29) issued an opinion on the Privacy Shield in mid-April, raising questions regarding, among other points, the onward transfer of personal data, the complexity of available redress mechanisms, the absence of key EU data protection principles (such as data minimization), and the failure of the Privacy Shield to exclude the massive and indiscriminate collection of personal data originating from the EU by US intelligence agencies. In the wake of this opinion, negotiators returned to the bargaining table, announcing on June 24 that all points raised by WP29 had been addressed and the Privacy Shield now conformed to the requirements of *Schrems.*

On July 8, the Article 31 Committee reviewed and approved the revised Privacy Shield, followed quickly by final approval from the European Commission on July 12. The Privacy Shield is effective immediately upon notification to the member countries, but the US Department of Commerce (DOC) is not expected to be in a position to accept registrants until early August 2016. Thus far, there is no indication that US organizations previously covered by Safe Harbor will receive any special consideration from the DOC if they elect to self-certify under the Privacy Shield.

As the Privacy Shield wound its way through the EU approval process, US organizations were left with few options for legally transferring personal data from the EU to the US. EU regulators expressed a preference for binding corporate rules (BCRs), but US organizations largely stayed away due to their associated complexity and expense. Although viewed by some as unsuitable for business models that emphasize direct online interaction with data subjects, Standard Contractual Clauses (SCCs) became the primary alternative to Safe Harbor. US companies that execute SCCs are required to consent to governing law and jurisdiction in the EU. Privacy Shield, by contrast, may be appropriate for a range of business organizations and, with the exception of HR data transfers, final enforcement powers and jurisdiction remains in the US.

In its current iteration, the Privacy Shield clarifies several areas identified as problematic by WP29, including:

Onward Transfer of Personal Data: Third parties who receive personal data from Privacy Shield companies are required to guarantee the same level of protection provided under the Privacy Shield in a written contract. The Privacy Shield company retains downstream liability for the failure by such third parties to meet this contractual obligation.

Redress Mechanisms: The processes for redress available to data subjects for data misuse under the Privacy Shield are explained in greater detail in the revised Privacy Shield, with an emphasis on accessibility and affordability. If a claim is not resolved directly by the Privacy Shield company, free alternative dispute resolution is available. Individuals may also seek assistance from their own data protection authorities, who will work with the Federal Trade Commission on a solution. If none of these mechanisms successfully resolve a claim, the parties will pursue binding arbitration.

Data Retention: The revised Privacy Shield provides that a certified organization may retain personal data "only for as long as it serves [the original or compatible] purpose of processing." However, personal data may be retained indefinitely if it is not "in a form identifying or making identifiable the individual." In making this determination regarding form, the Privacy Shield adopts a

"risk-based approach," which takes into account the practical ability of the Shield-certified organization to identify an individual from its database.

US Government Access: In this critical area, the Privacy Shield includes a comprehensive review of the assurances provided by the US. According to the EC, the US has "ruled out indiscriminate mass surveillance on personal data transferred to the US," under the Privacy Shield. The Office of the Director of National Intelligence provided additional documentation to further clarify that bulk collection of data could only be used under specific conditions, and detailed the safeguards that must be in place for the use of data under such circumstances.

Ombudsmen: The Ombudsmen, who will reside within the US Department of State, will be authorized to investigate claims by EU citizens alleging that the national security aspects of the Privacy Shield have been violated. The revised Privacy Shield emphasizes that the Ombudsman is independent of the US intelligence community.

Notwithstanding these and other revisions, observers expect that legal challenges to the Privacy Shield will reach the ECJ, perhaps within a matter of months. At issue will be whether the Privacy Shield meets the "essential equivalence" requirement for protection of data transfers to non-EU countries established by the ECJ in *Schrems*. Not surprisingly, there is no shortage of conflicting opinions on this issue.

According to Max Schrems, even with the limitations set forth in the Privacy Shield, the "mere possibility of mass surveillance is contrary," to *Schrems*. Joe McNamee, Executive Director of European Digital Rights, stated "Sadly, for both privacy and for business, this agreement helps nobody at all. We now have to wait until the Court again rules that the deal is illegal and then, maybe, the EU and the US can negotiate a credible arrangement that actually respects the law, engenders trust and protects our fundamental rights." The Computer and Communications Industry Association, the Business Software Alliance, and BusinessEurope expressed support for the Privacy Shield and hopes for a quick resolution of any court proceedings. With Brexit creating substantial uncertainty, some insist that the ECJ will not risk compounding an already difficult situation by invalidating the Privacy Shield. There are also further opportunities to fine-tune the Privacy Shield at the mandatory annual reviews, and adjustments will also be necessary to conform to the General Data Protection Regulation (GDPR).

What's Next for Privacy Shield?

With potential legal challenges on the horizon, all eyes will be on the WP29 as it meets later this month to evaluate the revamped Privacy Shield. The WP29 Opinion provides a blueprint for future litigation if the regulators determine that its key concerns have not been adequately addressed. It remains to be seen whether regulators and other stakeholders are prepared to commit to legal recourse, or conclude that mandatory annual reviews and the requirements of GDPR will be sufficient to ensure that appropriate adjustments are incorporated into the Privacy Shield. EU authorities have already signaled that automated processing (e.g., profiling) of EU personal data by certified US organizations will be addressed via these avenues. US organizations confronting the decision of whether to self-certify under the Privacy Shield must take these factors into account, as well as the case against Facebook for its reliance on the SCCs, which has been referred to the ECJ. As recently as last month, German data protection authorities pursued enforcement actions (and assessed fines) against companies that adopted a "wait and see" approach on data transfer by continuing to rely on Safe Harbor. Although further change appears inevitable, decisions now have to be made.

We will continue to provide guidance and updates as the situation evolves.

contacts

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

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