Lowenstein Sandler

Client Alert / April 29, 2016

PRIVACY AND INFORMATION SECURITY

EU DATA PROTECTION UPDATE: LANDMARK GENERAL DATA PROTECTION REGULATION PASSES FINAL HURDLE AND REGULATORS WEIGH IN ON PRIVACY SHIELD

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

For the US private sector, the impact of these events is significant and necessitates prompt action.

In a flurry of activity over the last two weeks, the European Union approved the General Data Protection Regulation (GDPR), ensuring that the new regime becomes effective in 2018, and the Article 29 Working Party (WP29) issued its closely watched opinion regarding the Privacy Shield. Organizations that process any personal data of EU citizens fall within the newly expanded jurisdiction of the GDPR, so preparation of an implementation strategy is essential. Additionally, any US entity in a holding pattern regarding selection of a data transfer mechanism for EU citizens' personal data pending approval of the Privacy Shield may wish to revisit its strategy in light of the nature and scope of the WP29 opinion.

General Data Protection Regulation: What's In Store

On April 14, 2016, after four-plus years of negotiation, the European Parliament officially adopted a final version of the GDPR. This comprehensive legislation will become effective and replace the current Privacy Directive (95/46/EC) in 2018, exactly two years and 20 days after publication in the *Official Journal of the European Union* this spring. The GDPR will impact a myriad of operational and strategic programs for businesses that fall within its jurisdiction, including a host of US organizations. In addition to its extraterritorial reach, the GDPR expands the concept of personal data to specifically include data that *indirectly identifies* a natural person (such as IP address), provides for "joint and several liability" for data misuse among controllers and processors, and requires appointment of a data protection officer by any organization that processes data as a "core activity" or that processes sensitive data on a "large scale." And, as has been widely reported, violations of the GDPR are punishable by fines of up to 4 percent of the global annual turnover (revenue) of the offending organization. The just-released final version of the GDPR cites consent, data transfer (including breach of standard contract clauses and binding corporate rules), data portability, and profiling violations as among those eligible for the maximum 4 percent penalty, with breach notification, data protection impact assessments, and failure to cooperate with data protection authorities identified as violations subject to a maximum fine of 2 percent. Additional highlights may be found here.

Initially, the two-year implementation period may have appeared generous; in reality, compliance with the GDPR will clearly require commitment, resources, and budget. And, as with any new legislation especially of this magnitude, questions abound. In particular, the GDPR's new requirements, such as mandatory data protection impact assessments for high-risk processing, have no precedent in the Privacy Directive. The WP29 has acknowledged that appropriate guidance is necessary to meet the implementation deadline.

In anticipation of the final enactment of the GDPR, the WP29 released a "GDPR Action Plan" in February 2016. As outlined in the plan, top priorities for the next year include establishing an infrastructure for the European Data Protection Board (EDPB), preparation for implementing the "one-stop shop" principle, and taking steps to ensure consistency of implementation across the EU. Of particular interest to US organizations, WP29 has promised guidance during 2016 for controllers and processors, specifically with respect to data portability, and data protection impact assessments for high-risk processing (defined to include profiling and any systemic monitoring of a "publicly accessible area"). WP29 has assumed responsibility to provide appropriate and practical guidance for stakeholders during the GDPR implementation, a heavy burden for an organization already tasked with analysis and monitoring of the Privacy Directive, harmonizing the GDPR with the e-Privacy Directive, and other important initiatives. As observers have noted, only time will tell if WP29 has the bandwidth to fulfill all its commitments in a timely manner.

WP29 Opinion on Privacy Directive: The Concerns

On April 13, 2016, WP29 issued its much-anticipated opinion on the Privacy Shield. While praising

the dedicated effort of negotiators and citing significant improvements compared with Safe Harbor, WP29 ultimately concluded that, taken as a whole, the Privacy Shield failed to provide "essentially equivalent" protection for the personal data of EU citizens transferred to the US. On the plus side, commentators were relieved that WP29 left intact other data transfer mechanisms (i.e., model contracts, binding corporate rules and consent).

Among the key concerns expressed by WP29:

Key EU data protection principles are absent or require clarification: Examples include data retention, data minimization, and protection against automated individual decisions based solely on automated processing, such as profiling.

Onward transfer of personal data: WP29 insisted that onward transfers from a Privacy Shield entity to a third country must provide the same level of protection as the Shield, including national security, with the entity having responsibility for conducting an assessment prior to the transfer.

Redress mechanism too complex: According to WP29, the additional avenues of recourse available to individuals are welcome, but in practice the structure is too complex and difficult to use and is, therefore, ineffective.

National security: WP29 notes that the Privacy Shield does not exclude massive and indiscriminate collection of personal data originating from the EU. WP29 reiterated its strongly held position that such collection can "never be considered as proportionate and strictly necessary in a democratic society," as required under the protection offered EU citizens by the Charter of Fundamental Rights of the European Union. WP29 further maintains that the newly created position of ombudsman is not sufficiently independent or vested with adequate authority to guarantee a satisfactory remedy for EU citizens.

Joint review: WP29 requests clarification of the annual joint review process including participants, authority, and public communications.

There's one more opinion to come — the Article 31 Committee is scheduled to provide input on the Privacy Shield in the next few weeks. While the European Commission is not bound by either opinion, the influence of these powerful regulators is undeniable. If the European Commission proceeds with approval of the Privacy Shield in June as planned, then the WP29 opinion strongly suggests that judicial challenges will be forthcoming. Moreover, the specific objections cited by the WP29 may forecast the nature of cases raised by various stakeholders, with the European Court of Justice (ECJ) the only body having authority to invalidate a decision of the European Commission.

For US companies weary of the prolonged effort to replace Safe Harbor, the WP29 Opinion raises the specter of continued uncertainty. Indeed, there is a very real possibility that any US organization that implements the Privacy Shield after approval by the European Commission may be compelled to dismantle the structure if the Privacy Shield is invalidated by the ECJ. Therefore, US organizations with other viable data transfer options may want to reevaluate whether it's preferable to implement those options before the Privacy Shield (with or without modification) becomes a reliable approach to data transfer. Certain US organizations, such as enterprises that routinely transfer personal data from thousands or even millions of individual users each day, may decide that currently available transfer mechanisms are not suitable and may prefer to continue waiting for the Privacy Shield. However, with WP29 publicly reiterating that any company transferring data without an approved mechanism in place is violating applicable law, these organizations face a dilemma — continue waiting for the Privacy Shield because it's the best fit for their business, or risk a potential enforcement action. As yet, despite the WP29 statement, the data protection authorities have not taken action with respect to companies waiting on approval of the Privacy Shield.

What's Next?

The clock is ticking — US organizations have two years to implement the GDPR. In the US, passage of a federal law is closely followed by detailed rule-making at the agency level. In the EU, however, the WP29 is charged with initial responsibility for issuing "guidance" on the GDPR according to its own schedule. Once established, the EDPB will assume a critical role, as will the data protection authorities. In parallel, the Privacy Directive will continue to wind its way through the approval process with the prospect of judicial challenges ahead.

US companies need to develop an implementation plan for the GDPR, while keeping a close eye on guidance emanating from various stakeholders in the EU. As a starting point:

Map Your Data Flows. Understand and map the type and sources of your data, including when, how, and where such data is collected, processed, and stored, and document a legitimate basis for such processing.

Notice and Consent. Identify and document the nature and scope of notices provided to data subjects, and their consent, to your collection and processing of personal data.

Evaluate Data Usage. Track your data collection, usage, and disclosure practices, and assess whether they are aligned with the permitted purpose consented to by the data subject. Among other risks, authorities could potentially flag the collection of data that is not necessary to fulfill the stated purpose.

Assess Commercial Relationships. Begin an assessment of what changes, if any, may be required to your business relationships in order to comply with the GDPR including, for example, your contracts with customers, service providers, controllers, processors and subprocessors.

Since the Privacy Directive was first adopted in 1995, the evolution of EU data protection law has been anything but smooth. There is cautious optimism that the finalized GDPR — even including the substantial penalties for noncompliance — will provide a reliable level of conformity across the EU. US companies subject to the jurisdiction of the GDPR will have to lock down their data collection, transfer and processing practices and ensure they are in sync with the new regulations by the implementation date. We will keep you updated and continue to provide helpful counsel as new developments occur.

contacts

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

Mary J. Hildebrand, CIPP/US/E

973 597 6308

mhildebrand@lowenstein.com