Lowenstein Sandler

Client Alert / December 16, 2016

PRIVACY AND INFORMATION SECURITY

EUROPEAN UNION – ARTICLE 29 WORKING PARTY RELEASES GUIDANCE ON KEY ELEMENTS OF GDPR

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

Today – Friday, December 16 – the European Union's Article 29 Working Party (WP29) released guidance on the implementation of certain key provisions of the General Data Protection Regulation (GDPR) for public commentary. In this eagerly anticipated communication, WP29 focused on "one-stop shop," data portability, mandatory data protection officers (DPOs), and enforcement mechanisms, specifically with reference to the Privacy Shield. GDPR has jurisdiction over any organization that collects, receives or processes the personal data of EU citizens without regard to the organization's geographic location. Consequently, U.S. companies of every size and industry may have a significant stake in the nature and scope of WP29's guidance.

WP29's guidance documents are lengthy and will require time to absorb and translate into informed recommendations. In the interim, here are some key takeaways:

One-Stop Shop

WP29's guidance on the one-stop shop principle reflects the inherent complexity of multinational corporate structures, with detailed descriptions of relevant concepts and myriad examples. The basic principle is that the data protection authority (DPA) located in the member country of an organization's "main establishment" will take the lead role. The main establishment is where decisions about processing personal data are made. These concepts are deceptively simple. Data processing decisions are frequently decentralized for credible business reasons, leading WP29 to admit that there may be lead authorities for different types of functions within the same organization. The worst-case scenario, it would seem, would be the lot of organizations that do not have a main establishment within the EU; for these companies, the one-stop shop rule will not apply and **any** DPA may commence an investigation into data protection practices and violations.

Data Portability

GDPR creates the right to "data portability," which means individual data subjects may receive their personal data back from controllers/processors on request, or direct that their personal data be transferred to a different organization. While the concept appears straightforward, WP29's guidance indicates that practical implementation of the principle may be anything but. Among other things, "personal data" means not only the personal data provided by the data subject but any personal data generated by the data subject's activity (e.g., search history, traffic data or location data). Data portability rights are triggered by processing based on the data subject's consent or in the context of a contract with the data subject. However, data portability does not apply to personal data processed for "legitimate interests," such as combatting fraud.

In comments sure to be closely scrutinized by the technology and advertising industries, WP29 did not bar data subjects from requesting, receiving, and/or transferring data that an organization regards as its own trade secrets or other intellectual property. This conflict may arise, for example, with respect to personal data "generated by" the data subject's activity. WP29 states that data subjects may not misuse such information in a way that constitutes an unfair business practice or intellectual property infringement, but goes on to say a "potential business risk" is not, in and of itself, a reason to refuse data portability.

Appointment of DPOs

DPOs must function independently within their organizations and be involved at the earliest possible stage in every development related to data protection. As envisioned by WP29, the DPO will attend management meetings, product development forums, and other venues where data protection is implicated, and will be involved in any data breach incident from the outset. WP29 also indicates that the role and responsibilities of DPOs may not be suitable for execution by chief privacy officers or other C-level executives because of the inherently independent nature of the DPOs' function. DPOs, the WP29

makes clear, owe their first responsibility to data protection and not necessarily to the organization that employs them.

Enforcement; Privacy Shield

WP29 will be replaced by the European Data Protection Board (EDPB) when the GDPR comes into force in May 2018. WP29 affirmed its authority over various functions until then, including coordinating enforcement of cross-border cases. In what might be regarded as a sort of trial run, WP29 issued position papers on mutual assistance, cooperation and the one-stop shop rule, and announced that some of these mechanisms will be implemented on a test basis during 2017.

WP29 also took steps to support the Privacy Shield framework, which recently became the subject of a judicial challenge by Digital Rights Ireland based on allegations that the framework fails to adequately protect the personal data of EU citizens. WP29 made available communications documents that will be posted for use by individuals and organizations with complaints arising under the Privacy Shield. In addition, WP29 confirmed that it will serve as the "EU centralized" body to process complaints by EU citizens that their personal data was improperly accessed by U.S. government agencies. From the standpoint of U.S. companies, these steps by the highly regarded WP29 to ensure that EU data subjects have viable means of redress for misuse of personal data transferred to the U.S. bode well for the future of the Privacy Shield.

Conclusion

As an independent advisory body, WP29's opinions do not reflect the views of the European Commission. Nonetheless, WP29 is highly influential, and the guidance issued today is an important piece of the puzzle for U.S. companies striving to implement GDPR a mere 16 months from now. Stay tuned.

contact

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

Mary J. Hildebrand, CIPP/US/E

973 597 6308
mhildebrand@lowenstein.com