THE
NATIONAL LAW REVIEW

The Status of the GDPR As the One-Year Mark Gets Closer

jackson lewis.
Article By
Joseph J. Lazzarotti
Maya Atrakchi
Mary T. Costigan
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Administrative & Regulatory

- All Federal
- European Union

Tuesday, February 19, 2019

In honor of Data Privacy Day (Data Protection Day in Europe), the European Commission ("the Commission") released a statement on the status of the EU's General Data Protection Regulation ("GDPR") which took effect on May 25, 2018. The joint statement by the Commission's First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel stressed the importance of the GDPR in light of recent large-scale data breaches, and the positive effect the law has had in raising awareness on data protection and rights available to citizens.

The Commission noted that national Data Protection Authorities (DPAs) across the EU have received more than 95,000 complaints from citizens since May. Moreover, the DPAs have been active in guiding organizations, in particular small and mid-sized businesses, on their obligations under the GDPR. This will be bolstered by a "raising awareness" campaign soon-to-be launched by the Commission, to help organizations and individuals better understand their GDPR rights and requirements.

Although the GDPR is a regulation, not a directive, which makes it directly binding and applicable, there are still areas within the regulation that require EU member states to supplement the GDPR with local legislation. The Commission's statement called on five EU member states that have not passed such legislation "to adapt their legal frameworks to the new EU-wide rules as soon as possible". EU member

states yet to enact GDPR implementation laws include, Bulgaria, Czech Republic, Greece, Portugal and Slovenia.

Together with the joint statement, the EU Commission released an info-graph, tracking GDPR developments over the past eight months. Key statistics include:

- Most common types of complaints reported to the DPAs: telemarketing, • promotional emails and • video surveillance/CCTV.
- 40,000 data breach notifications reported to DPAs across the EU.
- 255 ongoing investigations by DPAs of cross-border GDPR violations.
- Three fines issued by DPAs for GDPR violations– the largest fine issued was in the sum of €50,000,000 for lack of consent to processing personal data.

Investigations into potential infringements of the GDPR can be initiated by a Supervisory Authority or triggered by a data subject complaint. Sanctions for violations range from reprimands to fines. However, depending on the sensitivity of the data, the nature of the violation, the risk of harm to the data subjects, and the egregiousness of the violation, the fines can be significant. Fines, which are calculated based on the company's global annual turnover of preceding financial year, can reach up to 4% or €20 million (whichever is greater) for non-compliance with the GDPR, and 2% or €10 million (whichever is greater) for less important infringements. In addition, the GDPR permits data subjects certain legal recourse for processing violations that affect their rights. These include the right to bring a private cause of action for material or non-material damages resulting from a violation or the right to pursue "collective actions," which are similar to US class actions.

In other recent GDPR developments, in late 2018, the European Data Protection Board published draft Guidelines on the territorial scope of the GDPR (Article 3) for public consultation. Once finalized, this guidance will be particularly relevant for U.S.-based companies when assessing whether employee or customer data they process falls under the scope of the GDPR (*See also Does the GDPR Apply to Your US-Based Company?)*. Most notably for non-EU data controllers and data processors, the guidelines address the processing of personal data in the context of offering goods or services to an individual in the EU, or the monitoring of their behavior in the EU, under Article 3(2). The Guidelines provide that individuals "targeted" in the EU includes "natural persons, whatever their nationality or place of residence." In other words, the targeting criteria will apply regardless of the "citizenship, residence, or other type of legal status of the data subject" as long as the data subject is in the EU at the time of processing. With respect to the monitoring of a data subjects behavior in the EU, the Guidelines note the European Data Protection Board (EDPB) "considers that tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioral monitoring, for example, through wearable and other smart devices." The public consultation period for the Guidelines ended January 18, 2019 and the final version should be instructive, particularly for non-EU organizations.

The GDPR has brought new and enhanced privacy and security obligations for organizations around the globe, including U.S.-based companies. Compliance with GDPR is not optional and as of December 2018, more than 50% of regulated

organizations are still not fully GDPR compliant.