Gesmer Updegrove LLP

ClientUpdate

April 2018

Europe's General Data Protection Regulation Landing Soon

Europe has always taken a different view of data privacy than the United States. In general, the US has adopted a somewhat laissez faire approach, focusing regulation on specific industries (e.g., the health industry with HIPAA) or specific classes of individuals (e.g., children with COPPA). Ever since the passage of the EU's 1995 Data Protection Directive ("Data Protection Directive"), though, Europe has taken the position that data privacy should be treated as more of a fundamental human right, applicable to all.

While Americans and US-based companies have tended to look at the EU Directive from afar, the EU has adopted a much more rigorous and far-reaching law – the General Data Protection Regulation ("GDPR") – that is demanding more attention from people on this side of the Atlantic. It goes into effect on May 25, 2018.

What Does the GDPR Do?

Like the Data Protection Directive before it, the GDPR establishes a framework in the EU (and, actually, in Iceland, Liechtenstein and Norway as well) for the treatment of "Personal Data" that is held or processed there. In general, "Personal Data" includes any information "relating to an identified or identifiable natural person," or "Data Subject." This exceedingly broad definition means that even something as innocuous as collecting email addresses from prospective clients will trigger its protections.

This matters in the United States because the GDPR purports to have significant extra-territorial reach. A US-based company that collects or processes Personal Data from Europeans may find itself subject to the new law, even if it has no substantial presence in Europe.

For companies that are subject to the GDPR, the price of ignoring its requirements could be significant. The GDPR provides for fines and penalties that, in some circumstances, can run as high as the greater of €20 million or 4% of the worldwide revenues of the offending organization.

So What Does The GDPR Require?

The GDPR demands quite a bit, given the expansive nature of what it is trying to accomplish. With some exceptions, it requires that Personal Data only be collected when a Data Subject is clearly told what information is being collected; how it will be used; the legal basis for the collection; who will have access to it; how long it will be retained; and, if it is the subject of automated processing (such as social media profiling), what protections are in place to safeguard the data.

Further, the Data Subject is afforded a bundle of rights that come into existence *after* the data is collected, including:

- the right to access the data;
- the right to object to the processing of the data (for example, direct marketing);
- the right to demand the data in a machine-readable form;
- the right to complain that the data is being processed in a manner inconsistent with the GDPR;

- the right to have the personal data updated or corrected; and
- the right to have the data deleted – the so-called "right to be forgotten."

Transfers of Data

The GDPR would be a toothless tiger if it could be circumvented simply by moving the data to a less regulated locale. Consequently, the GDPR includes significant protections to permit the transiting of data only to places and organizations where it will receive "adequate" protection.

Laws in the United States plainly do not provide protection comparable to that afforded by the GDPR, so even during the reign of the Data Protection Directive, much time was spent and ink spilled deciding how Personal Data be collected in Europe could be used in the United States.

Some years ago, the EU and the United States established a framework called the "Safe Harbor," which permitted organizations to self-certify compliance with the major aspects of the law. In light of disclosures about widespread data monitoring by the US government, the Safe Harbor was deemed inadquate and replaced by a similar framework called the Privacy Shield, which also involved self-certification.

The GDPR does not do away with the Privacy Shield, but does contemplate a wider range of options for parties wishing to establish that the data will be adequately protected in its new home. These include the use of approved standard contractual clauses, binding corporate rules, and enforceable codes of conduct and certification mechanisms.

So Now What?

The GDPR may well require enterprise-wide changes for collectors of Personal Data. For some organizations, the May 25 deadline represents not just a daunting challenge, but an impossible goal.

However, whether your organization is ahead of the curve or behind it, now is the time to dedicate resources to reaching substantial compliance as soon as possible. Next steps may include the following:

- **Data mapping**. Auditing the kinds of Personal Data your organization collects and processes, and how it is protected.
- **Notice and Consent**. Updating privacy policies and other documents associated with the collection and use of Personal Data. Additionally, consider the future treatment of preexisting data.
- **Third-parties**. Vetting third parties (such as, say, hosting or co-location services) with whom the data will be shared, and updating written agreement with them.
- **Processes**. Establishing processes by which Data Subjects can exercise their rights with respect to their Protected Data.
- **DPO**. Designating a Data Protection Officer.

This is certainly not an exhaustive list, but is a great place to start.

This advisory is for information purposes only, and does not constitute legal advice. If you would like to discuss the General Data Protection Regulation, please contact Joe Laferrera at (617) 350-6800 or email him at joe.laferrera@gesmer.com.

Joe Laferrera