JENNER&BLOCK

Data Privacy and Cybersecurity

Update on the EU General Data Protection Regulation: Countdown to Implementation

By: Emily A. Bruemmer and Jennifer J. Yun

Nearly two years ago, on May 24, 2016, the European Union (EU) adopted a new law—the General Data Protection Regulation (GDPR or Regulation)—to replace the Data Protection Directive, which has governed data protection in the EU since 1995. While the GDPR resembles the Data Protection Directive, it has some important differences. These include new rights for data subjects, such as the right to data portability and the right to erasure ("right to be forgotten") in certain circumstances; new data breach notification requirements, including a requirement to notify the relevant Data Protection Authority within 72 hours of discovery of the breach (unless exceptions apply); and much stricter penalties and fines for non-compliance.

The Clock is Ticking

EU Data Protection Authorities can begin enforcing the GDPR against companies beginning on May 25, 2018, with no further action required by the EU Member States to bring the GDPR into effect. For companies that have operations in the European Union or that offer goods and services to (or monitor) EU residents, the time to get into compliance with the GDPR is running short.

What Next?

During this countdown, companies can benefit from guidance on the GDPR issued both by the EU and by Member State data protection authorities. At the EU level, the main source is the Data Protection Working Party established by Article 29 of the Data Protection Directive—or, as it is commonly known, the "Article 29 Working Party." This is an independent body tasked with advising the European Commission on data protection issues, and over the past year, it has released guidance interpreting many provisions of the GDPR, including the right to data portability; data protection impact assessments (DPIAs); data protection officers (DPOs); how to determine the relevant lead supervisory authority; and administrative fines. It also has issued draft guidance on data breach notification; automated individual decision-making; consent; and transparency, all of which are pending finalization following the close of the comment period.

Member State data protection authorities also have published their own guidance. The United Kingdom Information Commissioner's Office has created a *Guide to the GDPR,* along with draft guidance on controller-processors and children. Meanwhile, both the Data Protection Commissioner in Ireland and the Data Protection Authority in Spain have issued guidance on qualifications for DPOs and on the right to access personal data. Belgium and France also have issued guidance. And this is likely just the start, as Member States continue to interpret the Regulation.

Steps Organizations Should Take

As US companies sift through this guidance, they should keep several high-level considerations in mind. First, companies should determine whether the GDPR applies to them. The GDPR has a wide reach, applying to companies that are established in the European Union, offer goods and services to EU residents, or track EU residents online.

Second, if the GDPR applies, companies must determine, for each data processing activity, the legal basis for processing personal data. Unlike the United States, where processing personal information is generally permitted unless prohibited or circumscribed by federal or state laws and regulations, the EU requires companies to have a legal basis for processing personal data in the first instance. The GDPR provides six possible bases for processing, and if a company cannot justify processing personal data based on one of these bases, then the processing will not be deemed lawful. Because data subject rights will vary depending on which legal basis for processing a company relies upon, companies' selection of legal bases will impact the applicable rights of data subjects.

Third, an important and related step of GDPR compliance is determining which of these data subject rights apply. Additionally, companies should check whether they are processing any "special categories" of personal data or data related to criminal convictions or offenses, and, if so, what additional requirements apply to the collection and use of such data. Companies will need to update their internal processes and procedures to ensure that they can comply with data subjects' requests to exercise their rights.

Fourth, companies should determine whether they need to appoint a DPO or conduct a DPIA.

Fifth, companies must develop breach notification procedures to make sure that they will comply with the new requirements to notify the relevant supervisory authority and data subjects, as required under the GDPR.

Sixth, companies must review existing contracts with vendors and other third parties to ensure that they appropriately allocate responsibilities and impose obligations required under the GDPR.

Last, but certainly not least, companies must notify data subjects how they process personal data and ensure that they provide data subjects with the extensive information required by the GDPR's new notice provision.

Potential Complications

The European Commission has expressed concerns regarding Member State readiness for the new regime. Although the GDPR will take effect in Member States automatically, Member States nonetheless need to implement national legislation to address important administrative issues, such as that data protection authorities are appropriately funded. According to statements by Věra Jourová, the European Commissioner for Justice, Consumers and Gender Equality, only two Member States (Germany and Austria) have passed the necessary national legislation.

Additionally, despite its ICO issuing detailed guidance on compliance with the GDPR, the United Kingdom is in the midst of negotiating its departure from the EU. The effects of "Brexit" on the applicability of the EU's data privacy regime in the United Kingdom remain to be seen.

Finally, organizational awareness of European data protection and privacy law should not stop at the GDPR. In 2009, the EU adopted Directive 2009/136/EC on the processing of personal data and the

protection of privacy in the electronic communications sector (the ePrivacy Directive). This directive addresses topics such as network security, confidentiality of electronic communications, electronic tags such as “cookies,” and unsolicited e-mail marketing. The European Commission proposed updates to this directive in January 2017 in the form of a proposed ePrivacy Regulation. Companies should be aware of this proposed legislation, and alert to its progress as it makes its way through the EU political system, as—like the GDPR—the ePrivacy Regulation promises to significantly impact multinational companies’ business operations.

The authors would like to thank Partner Nancy Libin, chair of the Data Privacy and Cybersecurity Practice, for her guidance and contribution to this article.

Contact Us

Emily A. Bruemmer

ebruemmer@jenner.com | Download V-Card

Jennifer J. Yun

jyun@jenner.com | Download V-Card

Meet Jenner & Block's Data Privacy and Cybersecurity Team