MARSH

INSIGHTS | MAY 2019

One-Year Anniversary of the GDPR: A Look Back and Ahead

When the European Union's General Data Protection Regulation (GDPR) took effect in May 2018, proponents of the new law promised a profound change in data privacy protection. The sweeping regulation has not disappointed. Here's a quick look at where we are one year later.

Open for Business

The European Data Protection Board (EDPB), which coordinates the EU's data protection authorities, recently reported that regulators brought more than 200,000 cases in 31 countries and issued nearly €56 million in fines in the first nine months the GDPR was in effect. That tally includes a €50 million fine levied against one company that regulators claim inadequately advised customers about how it collected personal data from new customer accounts and subsequently used that data. (Given the company's size, the fine did not approach the maximum possible 4% of its annual revenue.)

Perhaps more striking than the monetary value of fines imposed is the diversity of enforcement actions. Some cases involve traditional privacy concerns, such as the failure to encrypt or control access to personal data. Others demonstrate the GDPR's broad scope.

In Poland, for example, regulators penalized a company that scraped data — mostly mailing and email addresses — from public sources because the company only provided notice passively by posting a statement on its website. In Austria, regulators fined a local business for performing excessive surveillance when its security cameras recorded people walking on the sidewalk outside the business. More recently, the European Data Protection Supervisor announced that it would audit contracts between EU agencies and a major cloud vendor to make sure data transferred abroad by the vendor would be protected by GDPR standards.

These initial actions confirm that the GDPR carries many obligations well beyond data breach notification, and that regulators are holding companies accountable. No penalties have come close to the much-discussed maximum fine of €20 million or 4% of annual revenue, whichever is greater. But companies can expect data protection authorities to be aggressive with their sanction powers, which are entirely new for some EU members, and expansive in their interpretation of data privacy rights.

Global Regulatory Momentum

Regulators intended for the reach of the GDPR to extend far beyond the EU's borders, with the rights granted under it following wherever an individual's data may sprawl. However, the GDPR has also prompted many nations to introduce comprehensive data privacy rules of their own. Brazil, India, Japan, Thailand, the US, and others have adopted laws with protections similar to those in the GDPR.

In the US, the California Consumer Privacy Act (CCPA) mimics the GDPR in many ways. It includes a broad definition of personal data; creates new rights for individuals to challenge how companies collect, protect, or store that data; and applies to a broad range of companies. The CCPA also features the GDPR concept of the individual's right to have personal data expunged (the "right to be forgotten"), an emphasis on providing clear consent notices, and the right to opt out of commercial sales of personal data. While changes to the CCPA are still being considered before it takes effect in 2020, other US states have followed with similar proposals.

A consequence of this regulatory wave is the drive toward greater data localization — the practice of keeping personal data stored on devices or servers that are physically present in the territory where the data was generated. As many large technology companies have already discovered, transferring large amounts of data outside of the EU can quickly run afoul of GDPR requirements, and prompt EU regulators to scrutinize the receiving jurisdiction's data protection standards. Outside of the EU, some nations' laws overtly require data localization.

These laws assert greater control over privacy, but they also present challenges for cloud solutions and data sharing practices intended to create greater flexibility and efficiencies. We can expect these challenges to provoke discussion about efforts to harmonize data protection standards globally. Ultimately, however, companies may incur substantial costs in order to bring their data use practices into compliance.

Implications for Technology

While the GDPR made a bold statement about the need to protect the individual's right to privacy, businesses are quickly discovering that no policy exists in a vacuum.

Since its implementation, the GDPR has butted up against some law enforcement practices. German regulators, for example, have raised objections to the German Federal Police's choice of body cameras because they store data in a cloud environment outside of the EU.

A more far-reaching situation has provoked debate about access to data of website registrants. That information, which is made available by the Internet Corporation for Assigned Names and Numbers (ICANN), is commonly known as WHOIS data. ICANN's mission is to ensure that when a domain name is typed in, the associated webpage loads. As part of its mission, ICANN collects basic information on domain name registrants, such as names, mailing addresses, email addresses, and phone numbers for administrative and technical contacts.

For decades, law enforcement, cybersecurity researchers, and intellectual property owners used the WHOIS database to shut down illicit websites, stop spam, and enforce copyrights. Since the GDPR took effect, however, public access to the WHOIS data has been blocked. Many in the cybersecurity field and in law enforcement have criticized the loss of this capability, and recently the US Department of Commerce urged ICANN to find a solution that would allow third-party access for legitimate purposes.

The GDPR, and similar privacy laws, will also face challenges in relation to evolving technology. The growth and development of 5G networks, the Internet of Things, and artificial intelligence (AI) all depend on greater connectivity and increased data sharing. The European Parliament recently issued ethics guidelines that identify AI as "a growing threat to the right of human beings to form their own opinions and take autonomous decisions." The guidelines call for greater scrutiny of AI's ability to "use personal and non-personal data to sort and micro-target people, to identify individual vulnerabilities and exploit accurate predictive knowledge."

As AI evolves, however, it should help companies comply with privacy regulation by tracking the use and transfer of personal data. But there will be growing pains as the technology develops. Businesses should expect the EU to take an active approach to AI's consumption and processing of personal data, especially when that processing distinguishes individuals based on race, gender, political beliefs, or any other sensitive category, even where the consequences are unintentional.

More Work Lies Ahead

The enactment of the GDPR marked a titanic shift for data privacy, signaling the start of more aggressive privacy oversight and enforcement in an era of rapidly advancing technology.

Thousands of GDPR actions are currently pending, and organizations should expect EU regulators to continue to aggressively pursue instances of non-compliance.

The GDPR has brought regulatory momentum to other regions, including the US. The standards being enacted are not uniform and companies may struggle to comply where privacy regimes conflict. In addition, the evolution of technology will have privacy impacts that will challenge many organizations.

The combination of these factors creates the potential for a hydra-like cyber risk for businesses. Risk professionals should prepare for the potential pitfalls that lie ahead by consulting with their advisors and insurance brokers about evolving regulatory standards and changing technology, and adopting insurance policy terms and conditions to address their organizations' widening exposures.

.

For further information, please contact your local Marsh office or visit our website at marsh.com.

MATTHEW MCCABE
Senior Vice President and
Assistant General Counsel for Cyber Policy
+1 212 345 9642
matthew.p.mccabe@marsh.com