COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 1. January 11, 2019
A look at the EU's General Data Protection Regulation eight months later

Although much of the business world was aware that the European Union's General Data Protection Regulation would irrevocably change the way data is managed, the GDPR implementation date in May 2018 still came as somewhat of a surprise. Many companies were not quite sure how to comply, where to place their resources, and exactly how the GDPR would affect them. As previously reported in volume 1, issue 12 of *RSCC*, a survey conducted just three months after the implementation date by Dimensional Research and TrustArc found that just 20 percent of companies surveyed considered themselves to be GDPR compliant.

No one was certain how the member nations' data protection authorities — and the newly formed European Data Protection Board — would investigate and enforce complaints and violations. There was considerable focus on the Irish Data Protection Commission, due to the high number of big tech firms with EU headquarters based in Ireland. The dreaded "four percent of global revenue" fine was bandied about, but no one could give a clear answer as to what would trigger such a massive penalty, if anything. There have been questions regarding territorial scope, how to properly obtain consent, and how to conduct internal investigations and third-party vetting under the GDPR.

In the last eight months some of these questions have received answers, but many new questions have arisen. Here are three things that have become clear in the last eight months:

- Consumers and organizations are aware of their rights and have demonstrated that they will exercise them under the law.
- Data protection authorities are serious about investigating and enforcing GDPR, and they have the resources to do it.
- Companies are still figuring out how to comply, and although authorities are cognizant of this fact and are releasing guidance on a regular basis, there is increasingly less flexibility for violators.

Areas of concern for organizations

Data subject access requests (DSARs)

Organizations have received steady influxes of DSARs since the GDPR went into effect. Many of these requests come from former or current employees or customers, and it's common for a DSAR to precede litigation. Companies are often not in the position to properly vet each request for data, nor are they able to provide all of the required data when a DSAR is approved. They must not only provide the nature, location and security requirements of any data they hold, but also the business case and legal grounds for collecting and storing that data. This requires granular knowledge and expert personnel.

The Dimensional Research and TrustArc survey found that one of the biggest problems that companies face in complying with GDPR was the lack of trained expert personnel and software solutions to help manage the troves of data. The survey also found that the sheer amount of resources required to map out data flows and understand

what the data is, where it's going and, most importantly, *why* it's in the system was a serious obstacle. Nevertheless, requests for data are not going away; in fact, they've increased dramatically since May, and companies unable to properly assess requests and provide the required information could face significant consequences, especially if a request is part of a legal action.

Cross-border data transfers

Another unresolved issue involves cross-border data transfers, both within the EU and between the EU and a non-EU party. Transfers of data from EU member states to third parties were previously governed by standard contractual clauses, which are a set of clauses prescribed and approved by the European Commission. Standard contractual clauses, however, were found to be inadequate following a lawsuit filed by privacy activist Maximilian Schrems, alleging that Facebook, Inc. violated EU data privacy laws by transferring his personal data to the U.S. To manage data transfers to the U.S., the EU established two separate protocols, Safe Harbor and Privacy Shield, but they were also challenged in court by Schrems. The Irish data protection authority referred the case and 11 questions regarding data transfers to a third country, to the European Court of Justice in April 2018. Whatever decision the court hands down will have significant implications for cross-border transfers. As of now, companies are in a holding pattern, but there will most likely be a decision in 2019, and compliance officers should be ready to adapt to the new transfer protocol.

In a related issue, the United Kingdom was once a "one stop shop" for companies looking to do business in the EU and remain compliant with the GDPR, but recent developments regarding Brexit have complicated the picture. Brexit makes the U.K. a "third country" in terms of international data transfers. In order for EU-based organizations to send data to another country, the third country must be awarded "adequacy" status, meaning their data management frameworks (both private and public) protect the personal data of EU citizens as effectively as GDPR does. It is unlikely that the U.K. will be awarded adequacy status before Brexit, presenting serious challenges for companies operating on both sides of the Channel. A possible solution to that particular issue is the transfer of operations to Ireland, where the local data protection authority maintains a well-resourced office, and local authorities are eagerly courting foreign direct investment.

Cases to watch

Dozens of cases are pending with data protection authorities across the EU. The majority of these cases will be settled quietly, without fines and outside the court. Those decisions, of which there will be hundreds in the coming year, will slowly fill comprehension gaps regarding how to comply with the GDPR. A few cases, however, feature tech titans battling it out over issues that will have a sweeping impact on how data is managed going forward. Here are three cases to watch.

Facebook data breach

The Irish Data Protection Commission announced it is investigating a data breach at Facebook discovered by the company on Sept. 25. The breach involves 50 million users and potentially 40 million more, and it is one of the cases that could feature the vaunted fine of four percent of global annual revenue. More likely, however, the case will demonstrate how enforcement of data breaches will look going forward and how Europe will handle class action lawsuits that may come in the wake of an enforcement action.

Google and "the right to be forgotten"

This case, brought against Google LLC by the French regulator, Commission nationale de l'informatique et des libertés, will answer a very important question: Where does the right to be forgotten end, if at all? Several other

parties have joined this case in support of Google, including the Wikimedia Foundation, Inc., France's Fondation pour la liberté de la presse, Microsoft Corporation, Reporters Committee for Freedom of the Press, Article 19, Internet Freedom Foundation, and Paris-based Défenseur des droits. A decision is expected in early 2019.

noyb and the issue of "forced consent"

noyb, a nongovernmental organization seeking to enforce existing EU data protection legislation, filed four complaints against Google, WhatsApp Messenger, Instagram and Facebook focusing on the concept of "freely given consent," a central tenet of the GDPR that noyb says Google and Facebook knowingly violated. Any decision will have far-reaching effects on how consent is defined in reality (as opposed to on paper) and will define the competitive landscape between big tech and smaller enterprises going forward.

Takeaways

- The grace period for GDPR compliance, if there ever truly was one, is now over. Companies should expect determinations to come down the pipeline by early spring, as the thousands of complaints and requests lodged since May 2018 begin to be fully resolved.
- The vast majority of complaints are minor, the resolution of which will help to fill in gaps of understanding in aspects of the GDPR. Other cases, such as the Facebook data breach or the case regarding the right to be forgotten, will shape the way personal data is managed for years to come.