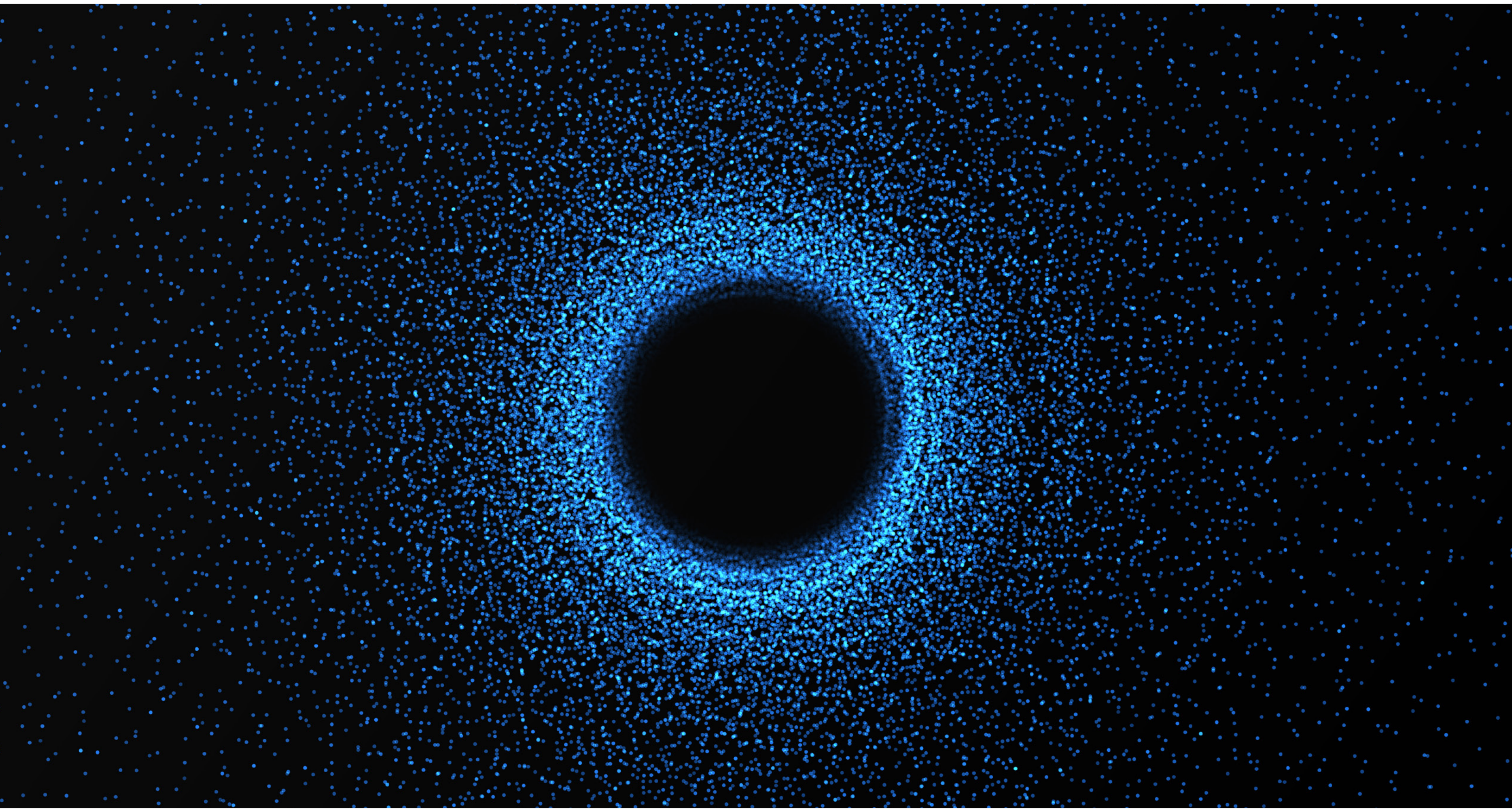
McKinsey
& Company

Risk Practice

GDPR compliance since May 2018: A continuing challenge

Companies must automate and streamline, or the challenge of GDPR compliance will overwhelm them.

by Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, and Marie Wahlers



© Rost-9D/Getty Images

July 2019

With the implementation of the European Union's General Data Protection Regulation (GDPR) on May 25, 2018, a new regulatory regime for business in Europe and beyond has begun. McKinsey research shows that few companies feel fully compliant: as many as half, feeling at least somewhat unprepared for GDPR, are using temporary controls and manual processes to ensure compliance until they can implement more permanent solutions. Broader organizational challenges persist as well—particularly honoring and protecting the rights of data subjects and ensuring that impact assessments, reporting of breaches, and audit organizations are functioning properly. With numerous stopgaps still in place, companies struggle to implement sustainable, long-term solutions.

GDPR's international reach

While the GDPR is an EU regulation, it is not solely an EU matter. It has global reach, as GDPR obligations affect international companies with customers or employees in Europe as well as those serving as data processors in Europe or for European companies. Governments outside Europe are introducing new data-protection regulations or enhancing existing rules to make them similar to the GDPR. Recognizing the need to maintain a trusted and competitive digital environment, as well as to ensure free transfer of personal data to and from the EU, states that have acted include Australia, Brazil, California in the United States, Japan, and South Korea.

IT implementation is still underway

As we have seen, businesses continue to work on IT solutions for GDPR projects, many by using manual processes and temporary controls extensively to ensure compliance. Such measures, however, do not add up to a sustainable approach, especially given the regulatory requirements for the use of state-of-the-art data-protection technology, the likely increase in requests for access to personal records over time, and the growing challenge of keeping personal data secure. Three areas need particular attention: security controls, data management, and automation.

Security controls

Data-security breaches can tarnish a company's reputation and damage its finances, as recent major incidents at global firms show. According to research by the Ponemon Institute, the average cost of a data breach in 2017 was $3.62 million—or $141 for each compromised record. Implementing security controls will probably account for the biggest share of future spending on the GDPR for most businesses.

To maintain robust data security, companies must implement IT controls in line with those of peers and adopt best practices in areas such as encryption, data anonymization or pseudonymization, and identity and access management. Companies should also base their investments on up-to-date appraisals of their security gaps in personal data. The controls themselves must reflect the content of the personal-data assets in question. A master customer-data system, for example, requires stricter controls and better protection than does a system containing security contacts for a business team.

Data management

Manual processes and temporary work-arounds are prevalent in certain aspects of data management relevant to GDPR compliance:

Responses to requests from data subjects exercising their rights under the GDPR. Customers may want, for example, to transfer their personal data to other institutions. Many companies approach such requests pragmatically by opting, for now, to use centers of excellence. Then such companies wait to see how many requests they receive from customers before deciding which technical solutions to pursue in the long term. In a few cases, such as those involving the right of data subjects to access, automation has already been deployed. The solutions in use have not, however, matured enough to capture the full complexity of the requests expected under the new regulation.

Transparency for customers, as encoded in fair-processing notices and consent statements. This is crucial to ensure the fulfillment of formal requirements: one European regulator, for example, imposed a multimillion-dollar fine on one corporation for violating the GDPR's transparency standards. To offer customers an informed opt-in option while still managing to keep opt-in ratios reasonable, companies will need to ensure that consent-management systems are auditable and that consent statements are really transparent and well positioned.

Reporting of data breaches. Only 25 percent of the companies we surveyed said that they can meet the requirement to report any data breach to regulators no later than 72 hours after management becomes aware of it. For a large, decentralized organization, reporting appropriately and quickly can be difficult. Companies will experience a sharp rise in mandatory interactions with regulators; according to estimates, the number of incidents that must be reported may increase a hundredfold or more. To cope, companies will need to ensure that they have enough staff, adequate training, an appropriate process, and a ticket system that handles related requests.

Automation

Article 30 of the GDPR requires businesses to record processing activities that use personal data. So far, most companies have treated this as a mostly manual exercise, running surveys to capture data-processing activities and their characteristics. To keep the Article 30 record updated, however, companies will have to run such surveys regularly. Although full automation is unusual, companies can introduce automated tools to ease part of the burden.

To orchestrate the update of the Article 30 record, some businesses already use tools such as collaboration platforms that provide data-storage capabilities. What's more, tools that use artificial intelligence and business rules to identify personal data are now mature enough to help update the Article 30 record. Tools to identify data-processing activities and the personal data in them are starting to emerge and could eventually be adopted for this purpose as well.

Organizational challenges remain

The challenges companies have faced since May 2018 are not confined to data and IT. Businesses must also ensure that the processes designed during the preparations for the GDPR actually work and produce the expected results. Areas of particular concern include enabling the rights of data subjects, handling breaches and crises, and managing audit processes.

Although full automation is unusual, companies can introduce automated tools to ease part of the burden.

Unfortunately, the many companies that began their implementations late have not had sufficient time to pressure-test new processes and run “war games” on them. Adding to the complexity is the continuing uncertainty about the number and types of requests and breaches that may occur under the GDPR. In any case, the GDPR—and data protection in general—can be regarded, more and more, as strategic assets promoting the sustainable growth of companies.

At a time when individuals are becoming more aware of their rights and more concerned about the use of their personal data, companies must prepare for requests from a range of stakeholders: not just clients and regulators but interest groups and the media as well. Even compliant organizations run the risk of reputational damage if customers believe that they have not been treated fairly. Regulatory-reporting requirements and rising customer expectations also pressure companies to respond quickly when adverse events occur. This pressure is also reflected in the GDPR’s wide reach outside the European Economic Area and in the fact that regulators in other countries have adopted similar regimes.

For these reasons, we expect that many companies will continue to improve their GDPR compliance as part of wider efforts to streamline organizations and processes. Ideally, new IT solutions should be introduced only after internal testing and auditing. Data breaches or surges in requests may sometimes demand quick fixes, but the results are usually better if companies implement solutions in a more controlled way.

Companies will need to increase their level of automation and streamline the organization or the challenge of sustaining GDPR compliance over the long term will overwhelm them. The important building blocks include support for tools, continued investment in cybersecurity, and improved internal processes. The lion’s share of investment in organizational and technical-security measures is still to come.

Daniel Mikkelsen is a senior partner in McKinsey’s London office; **Henning Soller** is a partner in the Frankfurt office, where **Marie Wahlers** is a specialist; and **Malin Strandell-Jansson** is an expert in the Stockholm office.