McKinsey&Company

GDPR compliance after May 2018: A continuing challenge

Risk Practice April 2018

Authored by:
Daniel Mikkelsen
Henning Soller
Malin Strandell-Jansson
Marie Wahlers

GDPR compliance after May 2018: A continuing challenge

With the EU's General Data Protection Regulation (GDPR) coming into effect on May 25, 2018, businesses are scrambling to put compliance measures in place. However, recent McKinsey research showed that few companies feel fully prepared. As many as half of them expect gaps to remain after the cut-off date, especially in some areas of IT (Exhibit 1). These companies are resorting to temporary controls and manual processes to ensure compliance until they implement more permanent IT solutions in years to come.

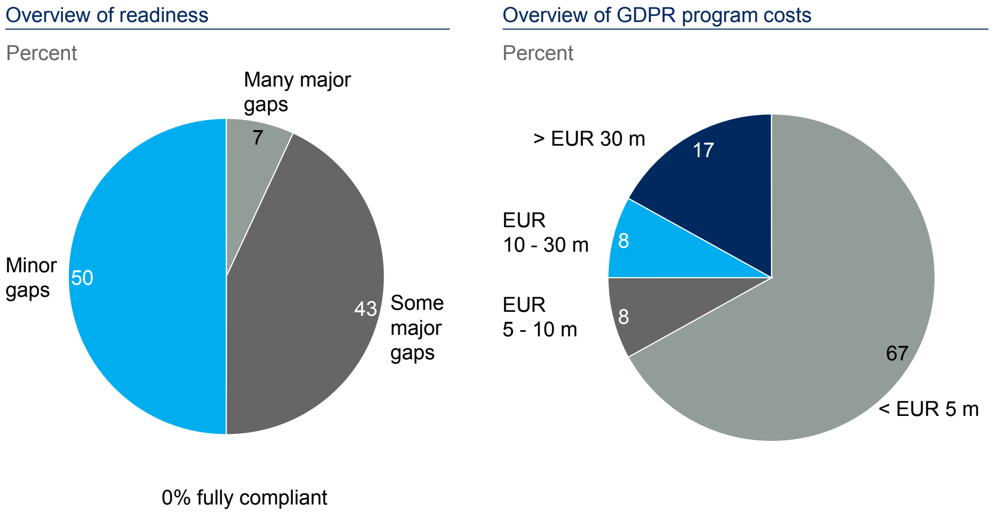

EXHIBIT 1

No one feels fully prepared for the GDPR, whatever their investment in compliance programs is

Survey of 35 senior managers conducted in January 2018

Broader organizational challenges persist too, such as ensuring that data subjects' rights are protected and respected and that impact assessments, the reporting of breaches, and audit organizations are functioning properly. To meet the imminent deadline, companies are adopting stopgap solutions, often without sufficient time to pressure-test them to see how they perform. Much work remains to be done after the May deadline if businesses are to overcome challenges like these and develop solutions that are sustainable in the long term.

IT implementation is still under way

As businesses continue to work on IT solutions for GDPR projects, many are making extensive use of manual processes and temporary controls to ensure compliance when the new regulation takes effect. However, such measures do not add up to a sustainable approach, especially given regulatory requirements for the use of state-of-the-art data protection technology, the likely increase in requests for access to personal records, and the growing challenge of keeping personal data secure. Three areas need particular attention: security controls, data management, and automation.

Security controls

Breaches in data security can tarnish a company's reputation and damage its finances, as seen in major incidents recently hitting the headlines. According to research by the Ponemon Institute, the average cost of a data breach globally was USD 3.62 million—or

USD 141 per compromised record—in 2017. Accordingly, implementing security controls is likely to account for the biggest share of future spending on GDPR for most businesses.

To maintain robust data security, companies will need to 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. The investments companies make must be aligned with up-to-date assessments of security gaps with respect to personal data. The controls themselves must fit with the content of the personal data assets in question: for instance, the master customer data system requires stricter controls and better protection than a system containing security contacts for a business team.

Data management

The use of manual processes and temporary workarounds is prevalent in certain aspects of data management relevant to GDPR compliance:

Responses to requests from data subjects exercising their rights under the GDPR, such as customers asking to transfer their personal data to other institutions. Many companies are taking a pragmatic approach to this topic by opting to use a center of excellence for the time being and waiting to see how many requests they receive from customers before deciding which technical solutions to pursue in the long term. Automation has already been deployed in a few cases, such as those involving data subjects' right to access. However, the solutions in use have not yet matured sufficiently to capture the full complexity of the requests expected under the new regulation.

Solutions for unstructured data in user-defined applications have seldom been a priority in the first wave of implementation. Managing and minimizing this data will continue to be a challenge. So far, most companies have put their faith in staff training and customer caution, but technical solutions may emerge in time.

Reporting of data breaches. Only 25 percent of the companies we surveyed said they would be able to meet the new requirement to report any data breach to regulators within 72 hours of management becoming aware of it. For a large decentralized organization, reporting appropriately and quickly can be difficult. Companies are likely to experience a sharp rise in mandatory interactions with regulators; estimates suggest that incidents needing to be reported may increase a hundredfold or more. To cope, companies will need to ensure they have enough staff, adequate training, an appropriate process, and a ticket system equipped to handle related requests.

Automation

Article 30 of the GDPR requires businesses to keep a record of 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. However, keeping the Article 30 record updated will require such surveys to be run on a regular basis. Although full automation remains in its infancy, companies could introduce automated tools to ease part of the burden.

Some businesses are already using tools for orchestrating the update of the Article 30 record, such as collaboration platforms that provide data storage capabilities. In addition, tools for identifying personal data based on artificial intelligence and business rules are now mature enough to use for updating the Article 30 record. And tools for identifying data-processing activities and the personal data within them are starting to emerge and could be adopted for this purpose in time.

Organizational challenges remain

The challenges companies face after May 2018 are not confined to IT. Businesses must also ensure that the processes designed during GDPR preparations work in practice and deliver the expected results. Enabling data subjects' rights, handling breaches and crises, and managing audit processes during the implementation of the GDPR are areas of particular concern.

The many companies that were late beginning their implementation have had insufficient time to pressure-test new processes and run war games on them. And the uncertainties over the numbers and types of requests and breaches that may occur once the GDPR comes into force have added to the complexity involved. So has the fact that the GDPR and data protection can increasingly be seen as a strategic asset that underpins a company's sustainable growth.

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 perceive they are not treated fairly. Regulatory reporting requirements and rising customer expectations also put pressure on companies to respond quickly if an adverse event should occur.

For these reasons, we expect many companies to continue working to improve their GDPR compliance as part of wider efforts to streamline their organization and processes. New IT solutions should ideally 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 solutions are implemented in a more controlled manner.

* * *

Companies will need to increase automation and streamline their organization if they are not to be overwhelmed by the challenge of sustaining GDPR compliance over the long term. Key building blocks will include tool support, continuing investment in cybersecurity, and improvements to internal processes. The lion's share of investments in organizational and technical security measures will be made after May 2018.

Understandably, businesses are currently focusing on deploying solutions based on a minimum viable product to ensure they meet the imminent regulatory deadline. However, if they wish to fulfil the expectations of customers as well as regulators in future, it is high time they started to address the road map to sustainable compliance after May.

Authors

Daniel Mikkelsen is a Senior Partner in McKinsey's London office.

Henning Soller is an Associate Partner in McKinsey's Frankfurt office,
where **Marie Wahlers** is a Specialist.

Malin Strandell-Jansson is a Knowledge Expert in McKinsey's Stockholm office.

Risk Practice
April 2018

Design contact: Visual Media Europe
www.mckinsey.com