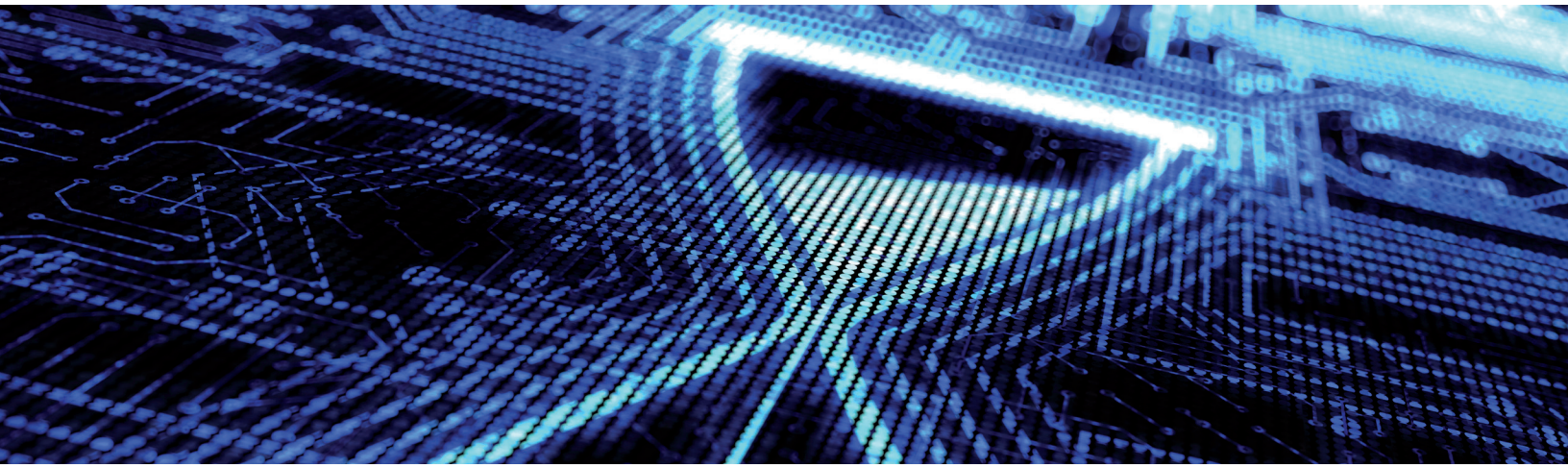
AUGUST 2017



© alengo/Getty Images

RISK

Tackling GDPR compliance before time runs out

Data protection has always been important. Now it's becoming urgent. Here's a primer on how companies can adapt to the new rules.

Daniel Mikkelsen, Kayvaun Rowshankish, Henning Soller, and Kalin Stamenov

Europe is on the brink of a sea change in its data-protection laws. In fact, when the General Data Protection Regulation (GDPR) takes effect on May 25, 2018, the effects will reverberate far beyond the continent itself. The GDPR goes further than harmonizing national data-protection laws across the European Union and simplifying compliance; it also expands the reach of EU data-protection regulation and introduces important new requirements. It seeks to ensure that personal data are protected against misuse and theft and to give European Union residents control over how data relating to them are being used. Any entity that is established in the European Union or that processes the personal data of EU residents in order to offer them goods or services or to monitor their behavior—whether as customers, employees, or business partners—will be affected. Any failure to comply with the regulation could incur severe reputational damage as well as financial penalties of up to 4 percent of annual worldwide revenues (see "The GDPR: Key facts," on page 3, for a synopsis of the new rules).

After an initial wait-and-see approach, many companies in Europe and beyond—including those in Asia, the Middle East, and the United States—are starting to set up sizable compliance programs. Yet our recent surveys of major companies revealed that a third of the executives in the sample felt their organizations still had a long way to go on the road to compliance.[1] As the GDPR is based on principles rather than rules, the onus is on individual companies to determine implementation in their particular context (exhibit). This process

Exhibit

The General Data Protection Regulation sets out guiding principles for data protection.

Principle	Explanation
Lawfulness	Data should be processed only when there is a **lawful basis** for such processing (eg, consent, contract, legal obligation)
Fairness	The organization processing the data should provide data subjects with **sufficient information** about the processing and the **means to exercise their rights**
Transparency	The **information provided** to data subjects should be in a **concise and easy-to-understand format** (eg, the purpose of consent should not be buried in a lengthy document of terms and conditions)
Purpose limitation	Personal data may be collected only for a **specific, explicit, and legitimate purpose** and should not be further processed
Data minimization	The processing of personal data should be **adequate, relevant, and limited to what is necessary** in relation to the purposes for which those data are used
Accuracy	Data should be **accurate and kept up to date**
Storage limitation	**Data should not be held** in a format that **permits personal identification any longer than necessary**
Security	Data should be processed in a manner that **ensures security and protection against unlawful processing, accidental loss, damage, and destruction**
Accountability	The **data controller** is responsible for **demonstrating compliance**

Source: Regulation (EU) 2016/679 of the Council of the European Union, European Commission, and European Parliament

is fraught with uncertainty, and many companies are struggling to understand how they can best interpret, measure, and monitor compliance. Below we examine some of the main stumbling blocks and identify the steps that successful companies are taking to overcome them.

Why businesses are struggling with GDPR compliance

From our survey and conversations with executives, we have identified a number of ways that compliance efforts are falling short:

- *Underestimating the scope of the regulation.* Some of the executives who responded to our survey were not fully aware of the breadth of the GDPR, regarding it as merely an enhancement to existing regulations. Conversely, others felt that complying with the new provisions—especially the business and IT implementation of data-subject rights—would be onerous for their organization, and were doubtful they would reach full compliance by May 2018. Indeed, only one of the 19 participants in our European survey believed his/her company would fully comply by the deadline.

The GDPR: Key facts

The scope of the General Data Protection Regulation (GDPR) is broad, covering any information that can be linked to an identifiable individual (such as search-engine entries, employee authentication, payment transactions, closed-circuit-television footage, and visitor logs) in any format (structured or unstructured) and in any medium (online, offline, or backup storage). The regulation introduces stringent consent requirements, data-subject rights, and obligations on organizations that gather, control, and process data. Its core requirements cover the following:

Documentation. Organizations should maintain a record of data-processing activities and be ready to present it to the regulator at any time.

Legal basis. All data processing should have a legal basis, such as the consent of the data subject or the need to fulfill a contract or legitimate business purpose.

Rights of data subjects. Organizations should implement rights such as the right to be forgotten (or, more accurately, to data erasure), the right to data portability, the right to object, the right to revoke consent, and the right to restrict processing.

Security. Organizations should protect data through means such as encryption or "pseudonymization" and have effective operational procedures and policies for handling them safely.

Third-party management. Vendors and suppliers, including outsourcing partners, should be required to protect personal data and should be monitored to ensure that they do so.

Privacy by design. Any organization planning a new technology, product, or service should consider data-protection requirements from the beginning of the development process.

Breach notification. Data breaches resulting in risk to individuals' rights and freedoms should be reported to the authorities within 72 hours, and subsequently to the data subjects as well in certain cases.

The new regulation will be enforced via national supervisory authorities within the European Union that are granted wide-ranging enforcement powers and sanctions, such as the power to ban data processing. The fines for failure to comply will be high, as much as 4 percent of annual worldwide revenues. The GDPR also allows individuals to seek civil actions (including class-action lawsuits) against organizations that violate their data-protection rights.

- *Uncertainty about how to interpret the requirements.* The GDPR sets out a number of principles that organizations should observe in processing personal data, but most companies have yet to decide how to put these principles into practice. For instance, under the principle of lawfulness, any organization processing personal data must have either the consent of the individuals concerned or some other lawful basis for that processing. Although the GDPR provides guidance on what might constitute a lawful basis—such as to carry out a contract, to comply with a legal obligation, or to serve the legitimate interest of the data controller or a third party—that guidance leaves a great deal of room for interpretation. In practice, we see

organizations taking very different views on issues such as the extent to which new consents are required from customers. In all these matters, companies will need to consult with lawyers. And lawfulness is not the only principle in the GDPR where there is uncertainty over interpretation. Take the accuracy principle, for example: it requires organizations to keep personal data up to date and take every reasonable step to rectify inaccuracies, but it is left to the organizations themselves to decide what steps they consider reasonable.

- *Slowness in identifying the additional security measures needed.* As the GDPR uses similar language to the current directive, many organizations are relying on their existing security measures, including protocols for particular customer segments, for compliance. However, as they build their records of processing activities, they will need to ensure that these measures are proportionate to the risks pertaining to different types of personal data. This calls for a structured approach to defining data risk and the measures necessary for mitigation—"pseudonymization," anonymization, encryption, deletion, and so on.

- *A struggle to build and maintain a comprehensive inventory of all their personal-data-processing activities.* To satisfy this requirement, most of the banks we spoke with are relying initially on manual methods, typically using an internal survey to identify relevant data-processing activities within their organization. Such an approach may suffice for creating the inventory in the first place, but it is unlikely to be adequate to the task of keeping the inventory current and readily available to the regulator on demand. Sustainable processes and tools for maintaining detailed records have proved elusive so far for many organizations.

- *Lack of capabilities to fulfill their obligations.* Many companies are struggling to identify and develop the capabilities they will need to execute data subjects' rights in a timely manner. Consider, for example, the right to data portability. If a wealth-management firm receives a request from a customer to hand over all of her personal data to a different institution, what capabilities will it need to compile these data and transmit them to the new wealth manager? Under the GDPR, the data covered by the portability requirement are not confined to the personal data an individual provides and the transactions they perform, but includes observed data, such as search history, location, and so on. Building IT capabilities to fulfill these requirements may require banks to consolidate data from disparate systems, create new authentication methods, and introduce external application programming interfaces (APIs).

Steps to a successful GDPR effort

Drawing on our industry observations and regulatory experience, we have identified a number of actions that contribute to a successful GDPR effort and can help overcome some of the difficulties outlined above. Our advice is to check whether your institution is already taking these steps, and, if not, act now while there is still time.

- *Assign ownership of the program to a cross-functional task force.* A typical GDPR program does not have a natural owner in the organization; the challenge of ensuring compliance requires an approach that cuts across functions and businesses. All of the teams involved—legal, compliance, the business, IT, risk, and others—must commit to and share responsibility for a road map for change. Senior leadership approval and buy-in is vital so that the program is securely anchored in a company's overall strategy.

- *Define the scope of your GDPR program, and use a business lens to determine what should be ready for May 2018.* Most of the companies we surveyed believed they would not be fully compliant by the implementation date, so it is important to identify which aspects of the regulation and which data assets are critical to compliance and make them a priority. This means not only understanding legal requirements but also defining what risks the business is willing to accept, and what value it seeks to extract from the program.

- *Develop an in-house interpretation of GDPR requirements* that identifies the big strategic questions they pose and seeks to address them early on. The approach should reflect the most likely scenario, take the industry view into account, and neither downplay nor exaggerate the impact of the regulation. Adopting a black-or-white legalistic approach may not be helpful, so it will be important to stay close to peers as well as regulators and see what practical steps they are taking to comply. As your program progresses, take regular pulse checks to keep it on track. Given the heavy IT requirements, your program validation should be performed well before the second quarter of 2018 to allow time for course correction, if needed.

- *Assess your GDPR readiness to uncover any gaps* and plan measures to fill them, whether that involves modifying marketing processes to secure customer consent, developing new in-house data-protection measures, or carrying out vendor evaluations. Bear in mind that adopting manual solutions to satisfy requirements such as ensuring data portability can lead to high ongoing running costs. Building an automated solution at the outset—such as APIs for data transfer—could simplify compliance and reduce costs in the long run if you believe there will be sufficient demand (for instance, for data portability) to justify the investment involved.

- *Begin building a "golden record" of every personal-data processing activity* in the organization to ensure compliance and traceability. This goes beyond documenting the system inventory and involves maintaining a full record of where all personal data comes from, what is done with them, what the lawful grounds for processing are, and whom the data are shared with. Map business or functional activities that use personal data and get the owners of these activities to complete a detailed questionnaire about the data processing involved. In parallel, work with vendors and internal IT experts to build tools and processes to maintain the inventory in steady state. This can be done as part of your software-development life cycle and data-protection impact assessments. Some companies adopt special data tools to discover personal data assets and provide compliance reporting, but these tools have yet to be proven at scale in the marketplace.

- *Define your organizational setup for data protection.* Designating a data-protection officer (DPO) is not enough. Companies also need to weigh the pros and cons of different organizational setups to arrive at a reporting structure that enables the DPO to operate independently; interact effectively with the chief information-security officer, chief privacy officer, and heads of legal, compliance, and risk; and report to the highest level of management. Having decided on the new structure, companies then need to determine the resources required to support it and fulfill their data-protection responsibilities more broadly.

- *Define the uncertainties in interpreting the GDPR requirements, and identify unacceptable*

risks to your business and IT. Many aspects of GDPR will be gradually resolved through industry practices and codes of conduct, regulatory guidance, or the court system. Interpretations of what is legally acceptable may also change over time. Frequent interactions with legal and business partners on compliance, legal issues, cybersecurity, application development, third-party vendor management, operations, marketing, and so on will help companies build a shared understanding of what they need to do. Beyond pure compliance, IT and the business should work together to define where the program should go the extra mile to minimize reputational risk, maintain customer trust, and avoid last-minute IT scrambles. This may involve implementing more stringent consent requirements, prominently announcing opt-out possibilities, implementing tougher-than-necessary security measures, and setting a high bar for sending personal data to third parties.

- *Consider strategic value.* Half the chief information security officers in our sample regarded GDPR as primarily a hindrance to their business. Undoubtedly the regulation will impose a burden on organizations, and with a matter of months to go before implementation, companies are racing to limit any negative impact it may have. However, what many leaders miss are the benefits that can be realized through a GDPR program. A well-conceived program can help an organization to build customer trust, improve customer relationships, establish better data controls, and improve internal data handling and availability. One company is taking advantage of its GDPR program to reengineer its master data-management platform so that all parts of the organization have a complete picture of all personal data on any given customer. Other companies are using GDPR-inspired reforms as an opportunity to build greater flexibility into their data platforms so that they can not only comply with the new provisions but also respond more readily to future regulatory changes. Seen in this light, a GDPR program can be an opportunity to embark on a wider data transformation that will benefit the whole business.

The steps above will help any institution get on the right track to meet next year's implementation date. GDPR should not be taken lightly. Organizations that fail to comply could face high fines, civil actions, and reputational damage, while those that use their GDPR program to spur a broader data transformation may be able to capture additional business flexibility and value. These are compelling reasons to treat the new regulation as a high priority for the whole organization, not just the risk, legal, and compliance functions. And with the implementation date imminent, companies need to act fast.

[1] We surveyed 19 executives at McKinsey's European General Data Protection Regulation (GDPR) Roundtable in February 2017; most were chief information security officers. In May 2017, we conducted an informal online poll of eight US executives who were leading GDPR efforts.

Daniel Mikkelsen is a senior partner in McKinsey's London office. **Kayvaun Rowshankish** is a partner in the New York office, where **Kalin Stamenov** is a consultant. **Henning Soller** is an associate partner in the Frankfurt office.

The authors wish to thank Malin Strandell-Jansson for her contributions to this article.

Copyright © 2017 McKinsey & Company.
All rights reserved.