McKinsey&Company

The EU data-protection regulation—compliance burden or foundation for digitization?

Risk January 2017

Daniel Mikkelsen
Henning Soller
Malin Strandell-Jansson

The EU data-protection regulation—compliance burden or foundation for digitization?

Enhanced data protection creates a challenge, but it also offers a catalyst for digitization.

As the economy becomes more digitized, companies increasingly manage large data sets and use them to conduct business. These data sets often include critical—and sensitive—personal data about individuals, both customers and employees, gathered in the course of doing business. Companies also acquire data from other sources, such as social media and Internet sites or specialized companies, to understand consumer behavior and find new ways to target customers. Companies such as banks, retailers, telecom operators, and other consumer-facing companies are amassing huge amounts of personal data, which is increasingly seen as essential for competing in the digital era.

This data is an invaluable asset, but it also comes with responsibilities and significant risk. To maintain trust, companies need to assure customers that their data will not be stolen or abused. When that trust is violated, the reaction is swift and devastating: after German social-media platform StudiVZ attempted to sell customer information, the site lost its user base within months. When 77 million Sony PlayStation accounts were hacked, the company faced 65 separate class-action lawsuits that took three years to settle. EU regulators state that not having trust in data security is one of the key inhibitors for further investment in digital.

By now the time is high to act immediately, as the European Union has taken the lead with the General Data Protection Regulation (GDPR), which goes into effect in May 2018. The regulation has strict rules about how personal data such as customer and employee data may be used and protected. The rules are directly applicable to all EU member states and EU citizens—thereby also affecting international companies with EU operations or customers. The regulation sets a 4 percent administrative fine, based on worldwide revenues, for noncompliance (Exhibit 1). The European Union is not unique in this field, although the GDPR to date is seen as the strictest framework in the world. For example, the Asia–Pacific Economic Cooperation privacy framework is intended to provide regulation in Asia and in the United States, and the Federal Trade Commission and relevant sector regulators enforce regulations and engage in various initiatives to protect personal data and privacy.

The implementation time of this regulation can easily take more than the 18 months left before compliance needs to be demonstrated, and the cost can be significant (more than €10 million), depending on the starting position of the company.

However, while we see that companies are increasingly aware of the existence of the GDPR mandate, many are still not clear about how to proceed with implementation. Some are moving ahead, but in ways that incur unnecessary costs. In a survey of 60 major European companies, we found that only 10 percent have mature cybersecurity risk-management practices. And 45 percent of respondents said they would need to make significant investments in basic tools to comply with GDPR requirements.

Among clients that are addressing GDPR, we find a tendency to combine the compliance effort with other data initiatives that may serve a valid business need, but they are either not enough or not required for compliance and raise costs. In this article, we look at the challenges that companies face in implementing GDPR and offer a structured approach that focuses efforts on specific GDPR requirements, avoiding the "gold plating" or additional initiatives that can add 70 to 80 percent to costs.

Exhibit 1

The EU General Data Protection Regulation provides the most comprehensive global framework.

Covered areas and topics

General provisions	• Subject matter and objectives • Scope • Definitions
Principles	• Principles • Lawfulness of processing • Conditions for consent • Processing of special categories
Rights of data subject	• Transparency and modalities • Information and access • Rectification and erasure • Right to object and automated, individual decision making • Restrictions
Controller and processor	• General obligations • Security of personal data • Impact assessment • Data-protection officer • Codes of conduct and certification
Transfer	• Transfer with adequacy decision • Transfer by way of appropriate safeguards • Binding corporate rules • Derogations for specific situations
Independent supervisory authorities	• Independent status • Competence, tasks, and powers • Activity reports
Cooperation and consistency	• Cooperation • Consistency • European Data Protection Board
Remedies, liability, and penalties	• Complaints and judicial remedies • Compensation, administrative fines, and penalties
Specific situations	• Freedom of expression and information, public interest, scientific, historical research, or statistical purposes, etc.

Source: EU data-protection regulation 2016/679, Official Journal of the European Union, May 4, 2016, Volume 59, eur-lex.europa.eu

Will GDPR hinder digitization?

Many companies see the new GDPR rules as a hindrance to digitization. They fear that stricter data-protection rules could limit what they can do in digital commerce, and that they will need to implement new procedures to protect both customer and employee data. Companies also worry that the money they will need to spend to comply with GDPR will divert resources from other digital initiatives. In addition, they are questioning whether the stricter European rules will put European companies at a disadvantage in global competition.[1]

While we agree that these are valid concerns, we also believe that strong data protection is a critical enabler for enhanced service offerings and digital commerce. Regulations that assure consumers that they can trust vendors make for a positive outcome, because they encourage consumers to do more business. The Dutch telecom operator KPN, for example, has conducted research that shows that the higher the customer-confidence level is regarding data security, the more data consumers are willing to share. This information can be used to improve and target offerings. At the same time, consumers are likely to shun companies that they regard as careless with data. A recent survey by Gemalto, a data-security vendor, found that 64 percent of consumers worldwide say they are unlikely to shop or do business again with a company that has experienced a data breach in which financial information was stolen; almost half (49 percent) said they would be unlikely to patronize companies that had data breaches in which personal information was stolen.[2]

Adequate handling of data protection also affects investments. According to the findings of a survey

by Brunswick Group, 77 percent of investors in the European Union said being more transparent about data breaches would improve the investment climate, and company value is at risk if companies do not communicate more effectively.[3] A recent press release from the European Council also points out that lack of trust in digital systems hampers investment in the European Union.

Done well, we believe that GDPR compliance can actually boost digital business in Europe. For example, GDPR makes it easier for companies within the European Union to operate across borders by harmonizing various national data-protection regulations. The compliance process will also force companies to review their data-handling practices and understand the amount and types of data they possess. This affords an opportunity to assess whether data can be used to create competitive advantage and if the company's data-handling practices are optimized from both a business and end-user perspective. In this way, preparing for GDPR can be a catalyst for taking the necessary steps to build strong digital capabilities, such as adopting sophisticated techniques for customer master data management.

Selecting an implementation model for data-regulation compliance

To turn the GDPR mandate into an opportunity will, however, require a high level of management awareness, the right organization, efficient tools, employee education, and an effective implementation model. In our work with clients, we often see that the responsibility for GDPR is mainly left with one of the following departments: IT, risk, legal, or compliance. However, based on our experience from more than 50 large-scale data-regulation implementation projects, we find that only a combined implementation model is effective in achieving and demonstrating compliance. Combined efforts are typically required to achieve a clear mapping of regulatory requirements to the entire organization and all its operations, including IT. This ensures "privacy by design," as required by the GDPR rules. Privacy by design means taking data protection into account at every step of a company's processes, from R&D and business development to marketing and sales. With its wider management focus and with project groups across different functions—such as legal, marketing, and IT—it also helps with strategic

considerations, since it reviews what customer data is collected, how it is used, and how it could be done better to create competitive advantage.

A structured approach using McKinsey's tool set can help reduce implementation cost and time

McKinsey has developed frameworks and tools to help companies understand the requirements of the regulation and to help implement a focused compliance process—one that avoids unnecessary costs but ensures a comprehensive review of data-handling processes and strategies. We have defined a set of key data-protection elements that all companies will need, including data-protection policies, a framework for data quality and control, and ways to meet specific requirements relating to data and infrastructure. These elements cover all relevant aspects of the regulation, including designating a data-protection officer to oversee the GDPR control framework; implementing, as the regulation specifies, "appropriate technical and organizational measures to ensure a level of security appropriate to the risk;" and adopting procedures to review and update technical and organizational measures when necessary.

McKinsey has also developed a proprietary tool that companies can use to fast-track IT and compliance efforts for GDPR. The tool maps each requirement for compliance, for each paragraph of the regulation, to a solution component in our framework. This allows for a focused implementation of initiatives and, by leveraging our extensive database of data-remediation programs, it allows for a benchmarking against peers (Exhibit 2).

Exhibit 2

This framework provides complete information on the current status compared with peers and compared with the regulatory requirements.

We have performed a peer comparison …

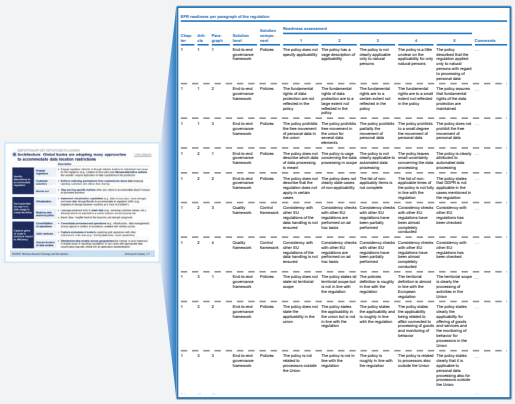
Using this mapping we have made an industry-level assessment against the compliance of each element of the regulation …

Key questions

- Where do we stand compared to industry peers?
- Where do we stand compared to the regulation standards?
- How can we learn from others?

… and developed a project-review logic for prioritization of compliance activities.

… and we will assess our clients using the project-review logic, per paragraph of the regulation, to identify the key areas for action.



Key questions

- How far are we from compliance?
- What is required in which area?
- Where do we need to clarify with the regulator?

Source: McKinsey analysis

The tool was developed to help companies create a targeted data-protection compliance program. Based on our experience, we often see companies having difficulties in framing their programs. Typical approaches focus on cybersecurity or improved data security. Those approaches provide improved capabilities in specific areas but do not provide a comprehensive view of GDPR requirements. Other approaches either deprioritize relevant issues or over-specify and add unnecessary initiatives to the GDPR project, which do not contribute at all or only indirectly to the capabilities required for GDPR.

We find that GDPR implementation costs often go over budget, because they have been burdened with additional projects that are not necessary for compliance.

For example, we have seen companies include a $30 million to $50 million investment in customer databases in their GDPR-compliance efforts. Such inclusions risk diluting and diverting the focus of a GDPR-compliance program and are not required from a compliance point of view. In our view, a good compliance program focuses on the requirements of the regulation—while simultaneously ensuring a process for capturing ideas for new business opportunities or improved processes. These should, however, be considered separately, as individual business cases, where costs and benefits have been estimated, and they should be pursued only if they are financially and strategically important. For example, a customer master database that allows for improved marketing campaigns and improved analytics—which might suggest

the product that a customer should buy next—can easily justify an investment if implemented correctly. Such investments can add 70 to 80 percent to the entire GDPR budget.

Our tool helps to drastically reduce inefficiencies and streamline necessary initiatives. It has therefore helped to reduce implementation costs by 25 percent and implementation time by 40 percent. Hence, GDPR costs can be significantly lowered while, at the same time, ensuring that business drives implementations for benefit and not for regulatory compliance. ■

Daniel Mikkelsen is a senior partner in McKinsey's London office, **Henning Soller** is a consultant in the Frankfurt office, and **Malin Strandell-Jansson** is a regulatory expert in the Stockholm office.

[1] Jonas Ryberg, "Digitization slowed down by EU data protection," *NyTeknik,* February 1, 2016.

[2] "Global survey by Gemalto reveals impact of data breaches on customer loyalty," Gemalto, December 10, 2015, gemalto.com.

[3] "2016 Global data valuation survey," Brunswick, December 5, 2016, brunswickgroup.com.

January 2017
Designed by Global Editorial Services