Toward privacy in the digital market:
How the General Data Protection Regulation will affect your business

Introduction and context
Published in the Official Journal of 4 May 2016, the General Data Protection Regulation (GDPR) entered into force on 24 May 2016, and will be applicable across the European Union from 25 May 2018 onward. Indeed, unlike a directive, a regulation does not have to be transposed into national law to become applicable.

The GDPR is the result of a lengthy revision of the European directive 95 / 46 / CE from 1995. The objective behind this new text is to provide a unified data protection framework applying directly to all EU member states as well as to all EU citizens to guarantee a high level of protection for citizens while playing the role of enabler of the digital single market.

With this new regulation, the EU intends not only to strengthen citizens’ control over the use of their personal data, but also to simplify the regulatory landscape for businesses.

The GDPR will impose high standards and uniform rules that strengthen consumer rights, boost European competition, and kick-start innovation.

Consequently, the GDPR will have an impact on all layers of the operating model of organizations where personal data could be used—both personal data of its customers and of its employees. The GDPR will require to assess the “as is” in order to identify the gaps with a compliant “to be” as a target, taking into account that both existing activities as well as new personal data processing activities will fall under the GDPR.

Beyond compliance, the GDPR should also be thought in the light of the digital market, as its implementation will enable organizations to gain a competitive edge by enhancing consumers’ experience and trust.
How will the GDPR affect your business’s operating model?

Governance and Organization

The entire GDPR is built on the principle of accountability, and clearly defines and expands the roles and responsibilities of controllers and processors. Controllers, as well as the potential processors, will have direct obligations to implement organizational and technical measures such as privacy policies, appropriate security measures, maintenance of records of personal data processing, and performance of privacy impact assessments. They will also be requested to notify data protection authorities of personal data breaches, and, in specific cases, to appoint a DPO.

In complement, the role of controller will not be limited to implement measures, such as data protection policies, to comply with the GDPR; he will also have the responsibility to demonstrate compliance if requested to do so by its national data protection authority (DPA).

Maintaining documentation on the processing of personal data and on measures implemented to safeguard personal data will be key to demonstrate compliance. To ease accountability, organizations should thus identify owners in charge of maintaining the necessary documentation.

Accountability will make top management leadership essential in the setup of a data protection governance and organizations should make sure that decision makers and key people are aware not only that the law has changed to the GDPR but also of the potential impacts brought by this change.

Although not new, with the GDPR, the role of Data Protection Officer is further developed. Appointing a Data Protection Officer may even become, in specific cases, mandatory. The DPO, who is in charge of monitoring compliance with the GDPR, advising its organization, and cooperating with data protection authorities, will have to define clear communication channels with internal stakeholders (authorized management sponsors, business owners of the processing of personal date, employees, etc.) as well as with external stakeholders (clients, third party service providers, data protection authorities, etc.). The DPO will also have to sustain subsequent communication, supported by authorized management sponsors. This will affect the organigram of organizations, which will have to consider whether to appoint a DPO and where to position him in the organigram.
The GDPR will have an impact on all layers of the operating model of organizations.

Business Processes
Organizations should review, for each of their business processes, the legitimate ground(s) for processing personal data to confirm and document that they legitimately process personal data. Among the grounds legitimating processing of personal data, organizations should take special care of consent since the GDPR will make the conditions for consent more stringent. Indeed, the burden of proof will be on the controller, who is required to demonstrate that the data subject has freely consented to the processing of his or her personal data. Therefore, organizations should take into consideration that consent will be more difficult to obtain and not always ensure a strong level of certainty, since the data subject may withdraw his or her consent at any time.

The GDPR formally gives its place to the risk-based approach. Data Protection Impact Assessments (DPIAs) should be performed to identify risks to the data protection rights of individuals of specific processing, for example when
the purpose of the processing aims at systematically evaluating personal aspects or when it involves the processing of special categories of data (e.g., health data) on a large scale. Whenever risks are identified, it is expected that organizations formulate measures to address them. This assessment should be performed prior to the start of the processing.

The GDPR makes explicit reference to direct marketing, to which data subjects have the right to object. It also strictly frames profiling activities by setting limits. In certain cases, organizations may be allowed to design processes using profiling to make decisions but should implement appropriate measures to safeguard the rights of data subjects. Organizations should review their business processes to ensure that suitable measures safeguarding that the rights of data subjects are embodied. In the context of the profiling, this means foreseeing the possibility, for data subjects, to obtain human intervention to express his or her point of view and to contest the decision.

**Personal data**
The GDPR expands the rights of data subjects by introducing, among other things, the right to be forgotten and the right to data portability requiring both organizational and technical measures to be implemented. For example, data portability implies that data subjects may request to receive their personal data in a structured, commonly used, and machine-readable format. They will also be able to request that the personal data be transmitted directly from one organization to another.

As a result, organizations should be ready to handle requests requiring the implementation of data management processes. In this context, they should know what personal data they hold, from where it came, and whether the personal data are transferred. Information audits may be performed across the organization, or within particular business areas to map this information.

**Beyond compliance, the GDPR should also be thought in the light of the digital market, as its implementation will enable organizations to gain a competitive edge by enhancing consumers’ experience and trust.**

The regulation contains a personal data breach notification obligation that should be taken into consideration by organizations in the frame of their data management processes, notably due to prescriptions in terms of timing (i.e., without undue delay, but in principle, no later than 72h after having identified the breach) and of communications means (e.g., when the personal data breach is likely to result in a high risk for data subjects, controllers will have to communicate the personal data breach to them). Communication is required to be in clear and plain language, and should describe the nature of the personal data breach.

Therefore, organizations will have to review their information security management procedures and operational processes to ensure that personal data breach can be detected, reported, and investigated, and that notification requirements will be assessed and, where necessary, satisfied.

---

1 Art. 56.2 of the GDPR
2 Already established in 2014 by the “Google v. Spain” ruling of the EUCJ
The GDPR requires organizations to ensure a level of security appropriate to the risk presented by the processing. The regulation lists both concrete technical measures such as “pseudonymization” and encryption of personal data, as well as results to be achieved through the measures such as the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. Other measures would suffice, such as the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. In addition, organizations should monitor the measures implemented to ensure their continuous effectiveness. Therefore, organizations will have to design and implement risk assessment methodologies in their project management procedures to be able to determine proportional technical and organizational measures right from the start (privacy by design). Besides that, they should clearly identify personal data in their information assets and, to ease compliance, may embody GDPR security requirements in their information security framework.

**The GDPR as a way to gain a competitive edge in the digital market**

**Data privacy in the digital area: “Smarter, faster, better”**

In today’s digital era, data privacy is becoming increasingly critical for businesses, pushed forward not only by the EU legislator but by EU customers as well, who are even more aware of data protection matters. With legal texts such as the GDPR, it is now necessary that data privacy issues are included in the digital initiatives of organizations. Indeed, organizations should adopt a proactive stand on privacy matters, which, on top of enabling compliance, creates and reinforce consumers’ trust and fidelity.

**Supporting systems**

As described above, the GDPR requires organizations to have clearly identified their information assets and the systems hosting them to be in a position to meet the requirements of structured communication to data subjects or of handling erasure requests. Organizations should review their information asset classification and management and should assess whether their system configuration allows them to meet the forthcoming requirements or whether additional technical or organizational measures should be implemented.
By complying today with the GDPR, organizations will be able to gain a competitive edge tomorrow. They should not hesitate to advertise to their customers on why, how, and what personal data they process. Transparency toward customers demonstrates the benefit of the service, fostering customers' willingness to see their personal data processed since they do know which data are actually processed and why. On top of this, it will consequently allow organizations to perform direct marketing and profiling activities efficiently.

**Regulatory synergies and limitations**

Data privacy is not a novelty and was in existence before the GDPR. Therefore, organizations are likely already subject to existing laws and regulations governing this matter and requiring controls similar to GDPR. Such a legacy may be built on to reach compliance with the GDPR faster and at a lower cost.

Implementations of other regulations should take the requirements of respecting the GDPR into account, especially if these regulations imply the monitoring or profiling of the activities of the company’s employees or clients.

**How to move forward?**

The GDPR will call for actions by organizations. This may be complex, as it will require the assessment of the existing framework against the new requirements, in order to identify possible gaps, set up an action plans with measures to be implemented in order to support the affected layers (governance, business processes, personal data, and supporting systems), and accordingly define a roadmap of implementation with May 2018 as a deadline.

**Conclusion**

This regulation will affect organizations at various levels. Rather than seeing it as a constraint, organizations can make the best of it by using the GDPR as leverage to gain a competitive edge. Besides that, existing laws and regulations should also not be put aside, since on one hand, they can provide synergies and ease future implementations, and on the other hand, some requirements will need to be considered in the light of the GDPR obligations. The regulatory agenda may have other developments on this topic, such as expected delegated acts to be produced by the EU Commission to further detail the GDPR requirements or the topic of the “privacy shield framework,” enabling organizations to transfer personal data to the US.

On 12 July 2016, the European Commission has adopted the EU-US Privacy Shield framework with an adequacy decision. By notifying the member states, the new framework for EU-US personal data transfers enters into force immediately. The adoption of the Privacy Shield signals a return to normality for transatlantic data transfers, after the previous Safe Harbor framework became invalidated by the European Court of Justice on October 2015. As of 1 August 2016, US companies will be able to self-certify with the US Department of Commerce operating the Privacy Shield.