The GDPR is a big dog

Preparing for the GDPR requires organizations to understand the regulation, develop best practices for success and avoid common pitfalls.

The General Data Protection Regulation (GDPR) is like a big dog—you can either fear it, or tame it and make it your best friend. The GDPR builds upon the principles of the EU Directive 95/46EC\(^1\) however instead of directing Member States to pass data protection laws, the GDPR is a regulation, therefore it is law. The GDPR is effective immediately—this means that the Member States will have to comply on 25 May 2018. It also takes precedence over any legislation that may be passed by a Member State after the enactment. However, Member States may pass local laws that supplement or are more stringent than the GDPR.

The GDPR is more than mere law, it is a philosophy designed to protect the data privacy rights of European Citizens, wherever they may reside, and anyone who is in territorial EU. This philosophy is expressed simply as Privacy by Design. Europe has been more zealous in protecting privacy rights of data subjects than other jurisdictions. The 1995 Directive was a giant step forward at the time, but the GDPR moves the evolution even further by harmonizing the individual laws passed by the Member States. It expands coverage of protected persons, introduces significant fines, and mandates breach notification. It would appear that the EU has benefited from the experience of the United States with regard to breach notification laws. According to the National Conference of State Legislatures, 48 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have all enacted breach notification legislation.\(^2\) Like the GDPR, these laws indicate what data is considered personally identifiable information (PII), what kind of entities need to comply with the law, the elements of a breach according to the law, notice requirements and time frames as well as any exemptions.

Addressing the GDPR is much like making friends with a big dog. You learn what makes it tick, you provide training and you constantly monitor the animal’s behavior. So it is with the GDPR. Planning and support begins at the top. Executive management must embrace the “Privacy by Design” philosophy and direct or drive the organizational support necessary to fund and implement the policies, procedures, technology and training needed to ensure implementation. Processes and technology are the keys to success. The volume of data and the operational tempo of Data Subject and Regulator requests mandate that they must be automated in an efficient, transparent, yet secure manner. While the GDPR itself does not specify technology, it is clear that contextual access, network security, data security and especially visibility and rapid response are paramount.

---


Anatomy of the GDPR – Data protection principles and data subject rights

The GDPR has 7 data protection principles and its hallmark is that data subject rights are the center of gravity for the regulation. The principles of personal processing are set forth in Article 5 and Recital 39 of the GDPR. Organizations that are data controllers (responsible for the data) will be responsible for the design and implementation of secure automated processes to address these rights, the ability to properly deal with breaches, and the ability to demonstrate compliance with the principles. Here are highlights of the principles. The data subject’s data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected and processed only for “specified, explicit and legitimate purposes” and not for anything that might be inconsistent with the Data Subject's Consent
- Limited to only what is necessary to accomplish the purpose (data minimization)
- Accurate and “where necessary, kept up to date” taking reasonable steps to ensure the accuracy to include quickly correcting or erasing as appropriate
- Kept in such a form that “permits identification of data subjects for no longer than is necessary for the purposes”
- Processed in a manner that “ensures appropriate security of the personal data”

The GDPR details data subject rights and the processes to manage them. Most of these rights are pretty self-explanatory. However, rights related to automated decision making and profiling were crafted to prevent harm to data subjects caused by decisions that are made without people because of the potential negative financial impact on those denied credit, mortgages, and perhaps even jobs, because their resumes didn't pass the automated screener. Here again effective policies and procedures are the keys to successfully complying with this provision. Data subject rights specified by the GDPR are the right to: be informed, have access, rectification, erasure, restrict processing, data portability, object, not be subject to automated decision making and profiling.

Figure 1 GDPR rights and challenges

What is really different?

More teeth – Penalties
Fines under the GDPR are considerable. Section 83.4 notes fines up to “€10 Million or 2% of worldwide annual turnover, whichever is higher. Violations involving the principles (Articles 5, 6, 7 and 9); data subject rights (Articles 12 to 22) and data transfers (Articles 44 to 49) shall be €20 Million or 4% of worldwide annual turnover, whichever is higher.” Article 83.2 lists the elements of computing the severity of the fine which can include intent, gravity of the harm, number of data subjects, and others. Many of these elements harken to the classic theories of tort law, especially negligence. Historically, regulatory agencies go after the deepest pockets first and this is likely to be the case with enforcing the GDPR. For this reason, organizations outside the EU should not feel they are beyond the reach of the EU.

Data protection by design and by default
Large organizations are victims of data sprawl and, as such, have a specific duty to know what data they are storing and where it is stored. When personal data is on endpoint devices and used by applications such as email and spreadsheets—meeting the data subject privacy requirements such as rectification, erasure, and portability becomes a daunting task. Meeting the requirements of GDPR implies a high degree of centralization which controls access, offers visibility to all data across the organization and protection against data loss, damage or accidental exposure. Article 25 addresses the need for information security. While the section is silent on specific technology, the clear intent is to protect the privacy and integrity of the data wherever it may reside. Article 32, Security of Processing, offers some insight and guidance, but is technology-agnostic. Section 1 of the article indicates that “the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.” Chief among the sub-sections is “(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing and systems and services.”

Article 32 Security of Processing requires that “Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing"

The section goes on to give guidance on risk assessment, mechanisms to demonstrate compliance with Article 32. It also admonishes controllers and processors that any individual who has access to personal data must comply with the GDPR and instructions from the controller unless contravened by Union or Member State law.
Lawful processing

Article 6 of the GDPR introduces the concept of “lawful processing.” Section 1 of the article describes the 6 paths to lawful processing:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Best practices and practices to avoid

Organizational
There are a number of best practices from an organizational standpoint—top among them are identifying responsibilities and getting commitment and support from top management. Thinking globally is also essential to ensure uniformity of policies, processes and technology across the organization. Policies and procedures need to be reviewed globally to ensure compliance. Organizations should set up a cross functional team that includes a wide range of stakeholders i.e. corporate management, legal, IT, HR, and business operations wherein there are clear lines of responsibilities for each stakeholder. Likewise, there is a need for a wide-reaching training program so that anyone who handles personal data understands the nature of their responsibilities for processing, storing and securing that data under GDPR.
The GDPR may lack specificity in some areas, but it is clear that the duty to secure the data runs with the data. This means that organizations need to ensure that their subcontractors, agents and other third parties are also compliant with the GDPR. Compliance needs to be assured with contract terms and appropriate technology. Third parties must have the same level of information security as the principals they serve.

The GDPR mandates that certain organizations as described in Article 37 must have Data Protection Officers (DPO). Article 38 provides further guidance on the position and Article 39 indicates specific tasks the DPO must perform. A best practice for any organization that is not required to have a DPO is to appoint a senior individual with the same capabilities and responsibilities as the DPO to act as the organizational focal point for data security matters.

**Information security**

The GDPR does not specifically dictate what specific information security measures need to be in place. It is clear that international standards such as those promulgated by the International Standards Organization documents are well regarded as due diligence. For example, organizations can perform a business level risk analysis employing ISO/IEC 27005 (“Information security risk management”). They can also employ ISO/IEC 27018, which addresses PII in public clouds. Privacy by design is the default perspective so that organizations should adopt an architecture that allows for processing of personal data for different purposes consistent with GDPR principles and data subject rights.

Organizations need to have up to the minute situational awareness concerning their data. This includes adopting an organizational wide technology that enables data inventory and continuously monitoring the infrastructure security with an eye on early detection of potential data breaches. Establishing and testing breach notification systems and procedures is necessary to ensure that they are ready and able to meet notification deadlines. Article 33 employs the term “undue” delay and sets a 72-hour window for notification after becoming aware of the breach. The breach notification is part of the organizations rapid response plan to deal with breaches, regulator inquiries, etc.

GDPR compliance implies an extensive array of processes that ensure life cycle management of personal data to include policies for data retention and documented destruction of data. Restricting access to personal data is another core principle of the GDPR. The use of unique login role-based access controls (RBAC) can be employed to restrict the scope of processing of personal data so that processing remains consistent with the consent of the data subject. This type of access control should also facilitate detailed visibility and auditability of user access to track exactly how and by whom personal data has been accessed. It should be noted that the GDPR favors encryption as a means to prevent personal data from being read, copied, altered or deleted by unauthorized personnel during transmission, transportation or at rest.

The GDPR includes physical safeguards to the equipment that contains personal data so that organizations must ensure that all database servers are located in secure data centers and that only authorized persons can access the equipment. We have stated that the duty to manage the data runs with the data. Consequently, you need to include all manner of devices—mobile devices, CCTV, and others you may not have initially considered. Many of these devices are likely to contain personal data. The GDPR requires a high degree of security for these devices, and they should include key features such as: file self-destruct, limited downloading of personal data, permissions management, user restriction, and remote wipe.

---

1. [https://www.iso.org/standard/56742.html](https://www.iso.org/standard/56742.html)
Worst practices

Just as there are best practices, there are also some practices to avoid. First among them is to consider the GDPR as a fixed date in time. The GDPR must be considered an on-going process and a new way of thinking whenever personal data is processed. Secondly, avoid trying to separate the processing of EU data from the organization’s other data processing. This “separate but equal” approach has been shown to be faulty because today’s organizations’ IT operations are so intertwined as to make a parallel process not only difficult to implement, but insecure as well. Lastly, the ostrich approach of burying one’s head in the sand and just waiting and see how things go is another major mistake. It is very clear that sooner or later most organizations will be impacted by the GDPR and will have to adapt the Principles and Data Subject Rights within it. The GDPR is emerging as a "test" for more than just data privacy protection, but for due diligence in protecting information and electronic assets as well.

Conclusion and recommendations

Make the big dog your friend. The GDPR can offer your customers and other stakeholders assurance that you are a good organization to work with. In some cases, compliance with the GDPR can be a competitive advantage while in other situations, organizations will not be able to compete unless they are GDPR compliant. The GDPR is more a regional legal mandate. Organizations in nations outside the EU will be impacted by the GDPR. Investors and others are using GDPR compliance as a litmus test to gauge whether or not organizations are secure enough to be appropriate investments. As the GDPR implementation spider webs throughout Europe, it will spread to other nations that are major trading partners. The nature and complexity of the GDPR mandates a robust combination of policies, procedures and technology to properly implement. This is especially true of information security measures designed to provide visibility and auditability while transparently safeguarding the confidentiality, integrity and availability of personal data.

There are several topics where the GDPR has not provided definitive guidance. Good sources of information include UK Information Commissioner’s Office Blog and their main website.

About Tal Global

TAL Global is an international security consulting and risk management firm that provides a comprehensive array of investigative, disaster mitigation planning and risk management services, including Executive Protection, Counter Terrorism and Critical Infrastructure Protection, Cyber Security Consulting, and School and Hospital Security. Our extensive international network of professionals enables us to provide our clients with the highest level of security and loss prevention services around the globe.

Legal disclaimer

This document provides a general overview of the EU General Data Protection Regulation (GDPR) and is not intended as and shall not be construed as legal advice. Citrix does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure compliance with any law or regulation. Customers are responsible for ensuring their own compliance with relevant laws and regulations, including GDPR. Customers are responsible for interpreting themselves and/or obtaining advice of competent legal counsel with regard to any relevant laws and regulations applicable to them that may affect their operations and any actions they may need to take to comply with such laws and regulations. © 2017 Lawrence D. Dietz. All rights reserved. Used here with permission from the author.