FEATURE

# The Road to GDPR Compliance

## Overcoming the Compliance Hurdles

**Do you have something to say about this article?**

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

***https://bit.ly/2QCsZwl***

The passage of the EU General Data Protection Regulation (GDPR) has brought unprecedented attention to data protection legislation and the protection of personal privacy, accompanied by the increased obligations of certain organizations processing personal data. GDPR has wide extraterritorial scope, which means it extends beyond the borders of the European Union, thereby affecting organizations operating in different locations across the globe. The legislation aims to protect the privacy of individuals in relation to the processing of personal data and the free movement of these personal data. Given the basic fundamental right to privacy, there is little doubt as to the importance of safeguarding this human right. As a result, organizations must show that they have implemented appropriate technical and organizational measures to enable the processing of personal data that will meet the requirements of GDPR and protect the rights of data subjects.

The increased obligations placed on organizations that are controllers or processors, irrespective of the size of these enterprises, suggest that a structured and systematic approach to compliance must be undertaken. The risk of huge fines as the result of noncompliance, breaches of personal data and reputational damage are too high for these organizations to ignore.

Now more than ever, customers and business partners will be looking at the privacy profile of organizations and their general attitudes to the protection of personal data. This shift in perspective will have a significant impact on the profitability and reputation of organizations, targeting the core of an organization's business value and competitive advantage.


**Corlane Barclay,** Ph.D., PMP
Is a consultant specializing in information and communications technology issues, particularly data privacy, protection and security. She assists organizations to meet their data protection requirements and has successfully managed GDPR compliance projects. She is also an attorney-at-law and legislative drafter.

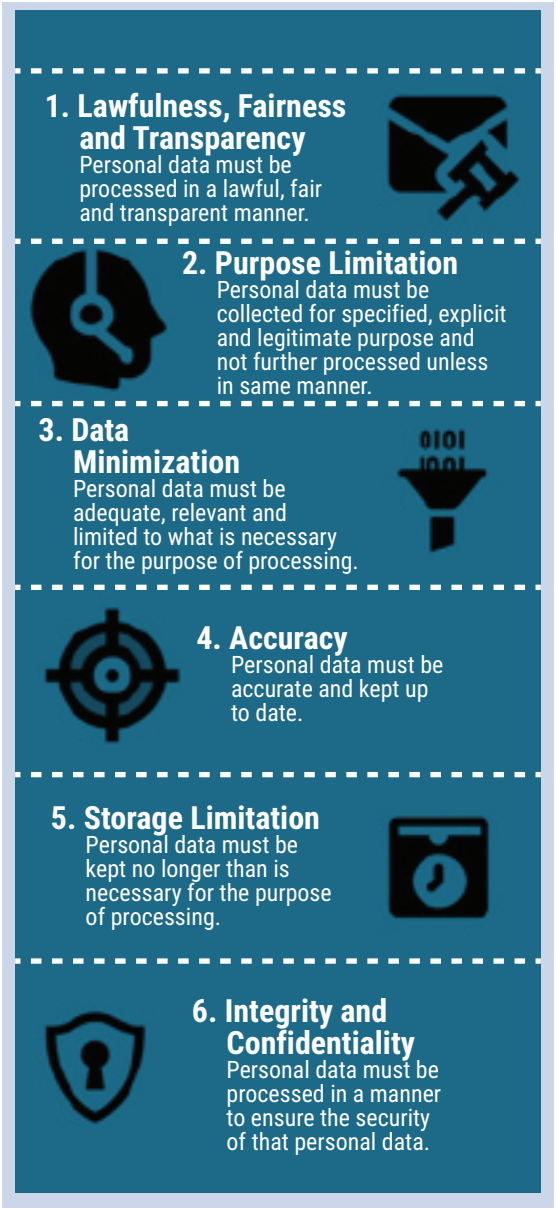
### Accountability and Compliance

According to Article 5(2) of the GDPR, a controller must be accountable for implementing six privacy principles (**figure 1**) and thereby be able to demonstrate compliance with:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

This obligation will likely impact all areas of an organization's operations since it affects the systems and services involved in the processing of personal data; the internal and external users of these systems and services; and the policies, processes and procedures employed to enable proper execution of this mandate. Therefore, GDPR compliance requires a holistic and strategic approach that will most likely require a seismic shift in how organizations operate and manage personal data; this is particularly true of smaller organizations. The compliance process will also require improved alignment with business areas

**Figure 1—Critical Areas of Accountability of Personal Data for Business**




and active engagement with its stakeholders to achieve success.

From the processors' perspective, Article 28(1) provides that where processing is to be carried out on behalf of a controller, the controller must use only processors that provide guarantees to implement certain measures to ensure that processing will be compliant with GDPR. Therefore, it is reasonable to expect that the processors are required to undertake similar implementation practices to be able to demonstrate compliance.

## Challenges in Meeting Compliance Requirements

Compliance activities are undoubtedly daunting. According to *Forbes* Insight, "compliance is viewed as an ever-moving target that can become overwhelming if organizations allow it."[1] Despite the business and regulatory necessity, organizations may be inclined to shy away from compliance programs, given their intricate mix of activities, varying requirements and diverse expectations. Therefore, it is unsurprising that a significant portion of organizations are still scrambling to meet the GDPR compliance requirements even after its coming into effect. A 2018 survey of 600 legal, information technology and privacy professionals in the United States, the United Kingdom and EU countries revealed that only 20 percent of these organizations considered themselves GDPR compliant.[2] While it is expected that this figure will likely improve in 2019, the survey underscores the complex dynamics in understanding the nuanced GDPR compliance requirements and meeting them thereafter.

There are several factors that may impact the readiness of these organizations to satisfy the legislative requirements under GDPR (**figure 2**), notably:

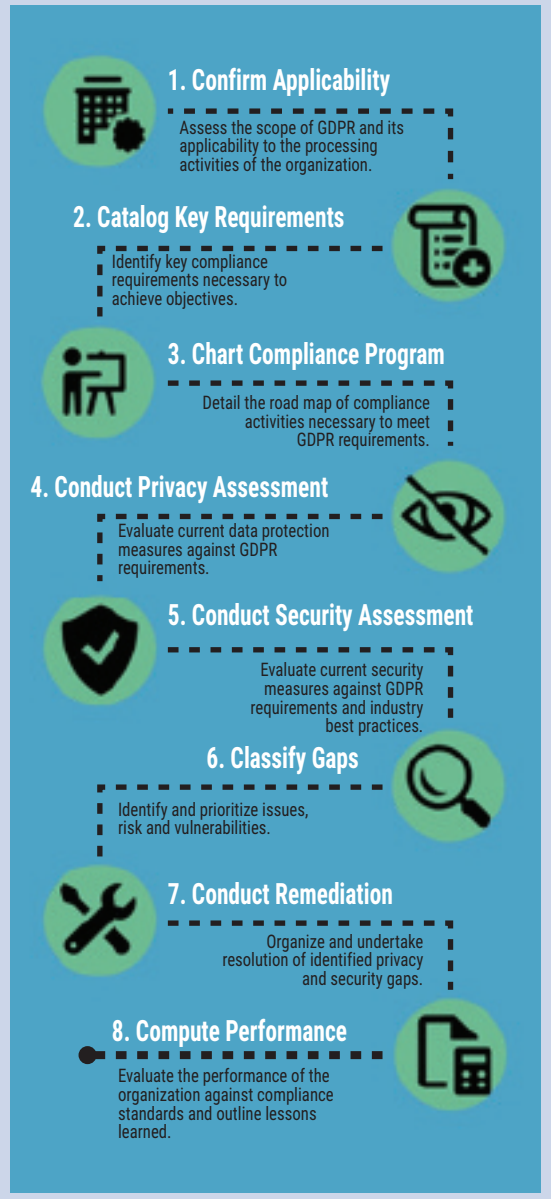
**Figure 2—Factors That Impact GDPR Readiness**

- **The complexity of the legislation**—There are 99 articles supported by 173 recitals outlining specific obligations for organizations that process personal data. Understanding these requirements and their impact on the business requires a mix of technological, privacy and legal competencies that are not always readily available in a single organization.
- **Limited awareness or preparedness by organizations**—Experience in the industry has also shown that a number of US organizations were caught off guard, despite the two-year implementation period, resulting in a delayed start to their GDPR compliance program. Additionally, it has been revealed that many organizations do not feel adequately prepared for GDPR and are concerned about their ability to report data and provide adequate transparency.[3]
- **The constraint of limited resources**—There is a high demand for human, technical, operational and infrastructural resources to sufficiently manage a data protection compliance program. This state is further exacerbated in micro, small and medium-sized organizations, thereby placing them at a severe disadvantage.
- **The high cost of compliance**—Fortune Global 500 companies will spend approximately US $7.8 billion combined to become compliant with GDPR.[4] While the figure for smaller organizations is likely less, the cost to mobilize resources and manage the impact of compliance activities on the business (such as the review and revision of third-party contracts, development of new consent forms and web pages, and the search and acquisition of new software tools) is certainly significant.
- **Low data-privacy maturity**—Based on the requirements of GDPR, many organizations did not have certain measures reflected in their operations, processes, policies or procedures. Insights gathered from compliance projects showed that a number of organizations were still in the process of developing their privacy notices and policies, consent forms, and other required documents days before the 25 May 2018 deadline. As a result, the low level of readiness had an impact on the number of technical and operational measures required to be implemented in order to become GDPR compliant.

## The Eight Cs of GDPR Compliance

The systematic steps (**figure 3**) that organizations can adopt to assist them in overcoming their respective compliance hurdles and improve their chances of meeting their GDPR obligations are:

**Figure 3– Steps to GDPR Compliance**



1. **Confirm applicability of GDPR**—This crucial step, which may be taken for granted, is to assess the applicability of GDPR to the organization. This step is especially relevant to controllers and processors who operate outside of the European Union. Assessing the applicability of GDPR involves understanding its scope and the operational outlook of the organization. It is necessary to determine whether the organization is offering or envisioning offering goods or services to data subjects in any of the EU member states. Elements that may make the applicability more apparent are whether:
   - The organization uses a language or a currency generally used in one or more member states, with the possibility of ordering goods and services in that language
   - There is mention of customers or users who are in the European Union
   - Individuals who are in the European Union are tracked on the Internet with the intention of analyzing or predicting their personal preferences, behaviors and attitudes[5]
2. **Catalog key requirements**—A controller, processor or third party has varied requirements under GDPR and will, therefore, need to undertake different paths to adopting and implementing appropriate technical and organizational measures to become compliant. Some examples include:
   - Organizations with fewer than 250 employees may deviate from the obligation with respect to record keeping.[6]
   - Controllers are required to have the requisite breach notification procedures that include reporting to the relevant supervising authority.[7]

   These scenarios reflect the different types of impact the role or function of the organization plays with respect to processing of data and the resulting approach that is necessary to meet GDPR compliance requirements. Alternatively, however, appropriate measures to meet data protection by design principles should be a principle core compliance objective for organizations regardless of their size, location or type of processing activities undertaken.
3. **Chart the compliance program**—This stage involves detailed planning and coordination of activities necessary to achieve data protection by design and meet other specific GDPR compliance objectives. Given the likely impact on the organization's processes, procedures, policies, systems and services, a sound strategy for the compliance program to demonstrate compliance across these various areas must be in place. Other activities include:
   - Confirmation of the scope of the compliance program
   - Identification and procurement of the requisite resources (e.g., human resources and technological tools)
   - Risk identification and management
   - Clarification of roles and responsibilities, especially where external resources are utilized
   - Identification and scheduling of key tasks
   - Management of stakeholders' expectations

> "PRIVACY ASSESSMENTS ARE NECESSARY, BUT NOT SUFFICIENT MEASURES TO MEET GDPR REQUIREMENTS."

4. **Conduct a privacy assessment**—The privacy assessment process is used to evaluate the organization's current measures against GDPR requirements and consists of a determination of privacy maturity, the types of personal data and sensitive data being processed, the legal basis for processing the data, the types of persons/roles and systems and services that interface with the system, and so on. A privacy assessment goes beyond an impact assessment or data protection impact assessment (DPIA), which is, nonetheless, prudent to undertake although not a GDPR requirement for all organizations. The impact assessment provides the organization with insights into the processing ecosystem and the associated risk to processing and, as such, is a useful tool.

## Enjoying this article?

- Read *Implementing the General Data Protection Regulation*. *www.isaca.org/Implementing-GDPR*
- Learn more about, discuss and collaborate on information security management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

5. **Conduct a security assessment**—Privacy assessments are necessary, but not sufficient measures to meet GDPR requirements. It is necessary to determine whether appropriate security measures are implemented to protect the personal data and their processing across all phases of the data life cycle. The security assessment is three-fold and involves an assessment of the security measures that support data protection, the identification of risk factors and vulnerabilities, and the determination of opportunities for data protection by design elements in the processing of personal data throughout the organization. Article 32 of GDPR provides key measures an organization can adopt such as the pseudonymization and encryption of personal data and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the organization's systems and services. Each organization would determine the most appropriate methods and tools to effect such requirements.
6. **Classify compliance gaps**—The GDPR readiness check undertaken during the privacy and security assessments will typically unearth various issues, risk factors and vulnerabilities that must be addressed to improve the security and privacy profile of the organization. These gaps may be categorized by the level of risk to achieving GDPR compliance (i.e., risk to processing of personal data and the levels of protection of critical systems and services) and may be broadly categorized into technical and organizational areas. Some common gaps include lack or insufficient inventory of processing activities, poor contractual arrangements with processors and third parties, insufficient documented policies and forms, and internal systems vulnerabilities.
7. **Conduct remediation**—Having a clear plan as to how to execute the remediation activities will be dependent on the previous steps. Some activities will require immediate actions, while others can be completed over a longer time frame and may range from the introduction of formal training and awareness campaigns and the development of appropriate contractual arrangements to the resolution of critical vulnerabilities found in the systems and services.
8. **Compute performance**—This stage involves the evaluation of the performance of the organization during the compliance program from the perspectives of a compliance process and a compliance program. Certain considerations may be ascertained, such as whether:
   - Compliance program objectives were met.
   - The organization is now GDPR ready.
   - There are certain technical and operational measures that can be improved, irrespective if GDPR compliance is met.
   - Business partners (e.g., a controller-processor relationship) understand their GDPR compliance requirements and have satisfied them.
   - There are certain elements that can be improved to increase overall efficiency in the next series of compliance activities.

## Conclusion

GDPR is transforming the way organizations operate and how business is transacted. The legislation impacts the full organizational ecosystem. Despite the challenge, organizations need to adopt a robust compliance program that takes into account the people, processes, procedures, policies, systems and services that interface or touch and concern the processing of personal data. The eight-step compliance program presented involves understanding the applicability of GDPR to the organization, the relevant requirements to assist in safeguarding the processing of personal data of EU data subjects, determining a road map to achieve the required objectives, assessing GDPR readiness, and implementing appropriate technical and organizational measures to ensure compliance. The steps are intended to be intuitive and serve to help organizations, particularly micro, small and medium-sized organizations, to overcome the compliance hurdles and meet GDPR requirements, with the full understanding that compliance is a continuous journey and not a destination. Furthermore, organizations will likely experience a number of benefits from adopting a robust

compliance program, such as improved customer trust, improved trade opportunities and a healthy privacy posture.

## Endnotes

1 *Forbes* Insight, "3 Ways to Excel at Regulatory Compliance and New Business Models," 5 February 2018, *https://www.forbes.com/sites/insights-deloitte/2018/02/05/3-ways-to-excel-at-regulatory-compliance-and-new-business-models/#70df93752275*
2 TrustArc, "New Report Benchmarks GDPR Compliance Status Post May 25th Deadline for US and EU Companies," July 2018, *https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_LP.html*
3 *Ibid.*
4 Khan, M.; "Companies Face High Cost to Meet New EU Data Protection Rules," *Financial Times,* November 2017, *https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc*
5 Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), recitals 23 and 24, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*
6 *Ibid.*, recital 13
7 *Ibid.*, recital 85