What Does “Appropriate Technical and Organizational Measures” Really Mean under GDPR?

Sometimes when we read something, it can be easy to consume the words without truly grasping the impact of their meaning. There are many use cases in life where this is true – both personally and professionally.

As security professionals who spend a lot of time thinking about privacy and regulations, words like ‘appropriate’ always catch our eye and cause us to look a bit closer. ‘Appropriate’ is one of those words that we can sometimes gloss over when in fact, we might want to slow down and unpack what it actually means. For example, the phrase “Appropriate technical and organizational measures” is prominently mentioned several times though GDPR.

The Overlooked Gem of GDPR

Article 32 – Security of Processing is “an overlooked gem” of the GDPR. It does not mandate how to implement security, but only that organizations must implement appropriate security commensurate with their level of risk, “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”. These are a lot of factors to consider, but it also gives your organization plenty of leeway to assess and act.

Keeping It Simple and Flexible

“Appropriate” is the operative word here. Oftentimes the complex and prescriptive nature of commonly used regulations and certifications lead organizations to emphasize task based, check-the-box type execution with a minimal focus on the practical effectiveness of their security program and whether it is in line with the sensitivity of the information they handle. This is ***not*** the case with GDPR. The word “simple” is seldom associated with GDPR, but in the case of data security, it is certainly relatively simple and flexible. The emphasis on the implementation of “***appropriate*** technical and organizational measures” provides your organization with two key benefits:

> First, it allows for a scalable and adaptive interpretation of the law. It will not require changes to the language as threats and technologies evolve.

> ***GDPR is not a fully prescriptive regulation. It requires your organization to do your homework, own your risks, and come up with “appropriate technical and organizational measures” specific to the organization.***

> Second, it allows organizations to tailor their security programs based on their own specific risks and processing operations, while also complying with the spirit and letter of GDPR.

Flexibility is a Double-edged Sword

However, this flexibility can be a double-edged sword: your organization’s choice on one edge and responsibility on the other. GDPR is not specifically prescribing how to protect personal data and individuals’ privacy, rather the how must be determined by your organization. The regulation gives companies the flexibility, but at the same time the responsibility, of choosing what are “appropriate” measures… that is a huge responsibility. While GDPR’s security requirements are foreboding, they do provide your organization with an opportunity to advance your data security programs along the maturity curve (Figure 1) based on your organization’s own priorities, objectives and risk profile.

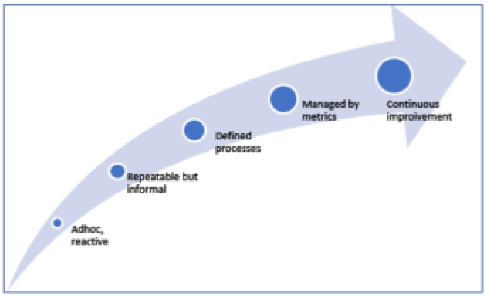

Figure 1 Information Security Maturity Curve

There is No Quick Fix to GDPR Security

Compliance with GDPR's security requirements will certainly not happen overnight. However, it is important that your organization has proactively assessed its risks and can demonstrate risk mitigation and forward progress across many domains (refer to the infograph GDPR: Article 32 and the Many Domains of Security). This "self-executed" data security as a fundamental principle is closely tied to GDPR's accountability principle, which in short means that your organization must be able to demonstrate its compliance with GDPR in a number of ways. Figure 2 uses the encryption domain as an example to demonstrate practical progress while also reducing risk. In contrast, standing still and maintaining the status quo is not a viable strategy, especially in the eyes of the data protection authorities. A practical and prioritized approach, one that demonstrates risk management and forward progress, is indispensable.

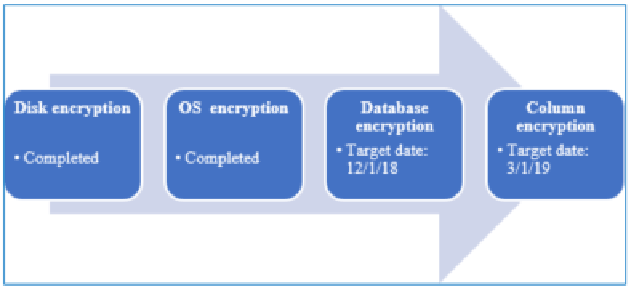

Figure 2 Reducing Risk with Encryption

A Practical Approach

Your organization's practical, but comprehensive approach should include:

> Performing a risk assessment in relation to your data processing activities, as well as each technical and organizational control with all required factors of GDPR in consideration (e.g. state of the art, costs, and nature of the data processed). As a result, creating a risk register recording all applicable risks from accidents and insider threats to malicious attacks.

> Developing a prioritized remediation roadmap.

> Implementing technical, organizational, policy, and process improvements to progress along the remediation roadmap.

> Documenting the overall control environment including strengths, weaknesses, and intended future state.

In line with GDPR's accountability principle, the artifacts from these processes must be detailed enough and retained to demonstrate your organization's level of compliance and risk management efforts. Your risk register and remediation roadmap are used to demonstrate that the weaknesses in processes and technologies have been evaluated and prioritized, and the documentation of your control environment provides a comprehensive representation of your organization's security program.

There is a lot to deliver on. However, evaluating your organization's security controls in the context of Article 32 is a valuable exercise. Assessing the level of maturity of the many security domains will provide a thorough understanding of challenges, a roadmap to mitigate risks, and ultimately provide a mechanism for demonstrating your organization's level of compliance.

Online advises organizations to "Be in Motion" and "Assess and Act". To get started, determine what is "appropriate", identify gaps, develop a roadmap, and execute. Last but not least commit to GDPR compliance by documenting your current state, future state, and forward progress. There is no quick fix to the Security of Processing as established in Article 32, but your diligence will be well worth the effort.

If you need assistance, Online Business Systems is available and committed to partner with you by providing resources and expertise to help meet your GDPR and privacy requirements.

online
business systems

Contact:
Online Business Systems
1.800.668.7722
rsp@obsglobal.com

About Online Business Systems

Founded in 1986, Online Business Systems is an information technology and business consultancy. We help enterprise customers enhance their competitive advantage by designing improved business processes enabled with robust and secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart. Today we have nearly 300 business and technical consultants throughout Canada and the US.