schellman
Quality, above all.

a little PRIVACY please

Why ISO 27018 can benefit organizations seeking to comply with the GDPR

WHITEPAPER

Ever since it was announced that the General Data Protection Regulation (GDPR) would take effect on May 25, 2018, globally-minded organizations have been scrambling for solutions to meet its prescriptive (yet interpretive) requirements. The expectation that organizations should adopt strong security and privacy-related measures comes at a critical juncture in time, where data breaches and privacy concern s continue to abound each and every day. While cloud-based information system architectures have significantly improved organizational performance and efficiency, there are specific risks that organizations should consider when determining a strategy to help ensure that sensitive information is protected. One such solution includes incorporating the privacy control considerations to an organization's information security management system (ISMS) as defined by ISO/IEC 27018:2014 (henceforth ISO 27018).

WHITEPAPER

To understand the synergies between GDPR and ISO 27018, it is important to point out that the GDPR sets forth privacy-specific rules and regulations to follow, while ISO 27018 and by extension, ISO 27001 (the Information Security Management System standard), sets forth a framework to address privacy and security risks. When an organization establishes an ISMS according to ISO 27001 and aligns it to the controls set forth by ISO 27018, an organization is better suited to establish the means to address privacy and security-related risks head on. Having an ISMS aligned with ISO 27018 is like having a blueprint or a map to guide an organization with the means to address a broad range of requirements, including a number of those set forth by GDPR. Even further, it demonstrates that the organization is proactively addressing emerging risks and concerns specific to cloud service providers that may host personally identifiable information (PII), as opposed to merely reacting to a new set of rules and regulations. Organizations seeking to meet the GDPR's requirements without a framework may attempt to string together a Frankenstein list of ways to meet each requirement but may struggle to demonstrate to regulators exactly how they meet these requirements. This is where an ISO 27018-certified ISMS may prove invaluable.

Having an ISMS aligned with ISO 27018 is like having a blueprint or a map to guide an organization with the means to address a broad range of requirements, including a number of those set forth by GDPR.

In the world of security and privacy... sometimes things don’t always go according to plan.

In the world of security and privacy, it goes without saying that sometimes things don’t always go according to plan. As alluded to previously, security incidents abound, and data leakage is ubiquitous (both intentionally and unintentionally). However, oftentimes what matters most is not that problems never arise, but that problems are recognized, treated, and solved in the best way possible. An ISMS with ISO 27018 control alignment does not promise that problems will never arise, but it provides a process for dealing with privacy issues and instills a privacy-by-design approach (which just so happens to be one of the prescribed rules of the GDPR). Privacy-by-design suggests that an organization’s processes are established with privacy concerns at the forefront of the discussion. Instead of a reactionary, “tack on some privacy measures and this will all go away” approach, the organization may rather consider “if we add this new functionality to our platform, how can we ensure that our users are still aware of how their data is processed and stored?”.

Establishing an ISO 27018-certified management system communicates that a formalized framework has been created to broadly address privacy and security-related concerns. The mark of an effective ISMS should minimally demonstrate the following:

- ✓ That risks are being regularly considered through recurring risk assessments
- ✓ That the identified risks have corresponding treatment plans and ownership
- ✓ That those measures are considered and reviewed by management
- ✓ That key metrics related to security and privacy are routinely evaluated and monitored; and
- ✓ That all of these principles align with the organization’s objectives.

It is worth pointing out that an effective ISMS takes into account the applicable legal, regulatory, and contractual requirements relevant to the organization. From that standpoint, an organization with an ISO 27018-aligned ISMS should remain abreast of emerging requirements, and not just the GDPR. All things considered, instituting the controls set forth by ISO 27018 may not satisfy the legal requirements of the GDPR alone, but an effective management system that provides a framework for addressing privacy-specific risks and concerns would empower an organization to meet these requirements, and the perhaps more stringent requirements to come.
If you represent a cloud service provider, it may be time to consider how your organization can benefit from the implementation of an ISMS that aligns its controls with ISO 27018.

For more information on ISO 27018, you can view our webinar on-demand: Privacy in the Cloud – an introduction to ISO 27018.

Speak with an ISO Certified specialist about your organization's information security needs today.

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684