Crowe

July 2018

Data Security Best Practices to Maintain GDPR Compliance

An article by Pamela S. Hrubey, CIPP-US, CCEP

Though the much anticipated General Data Protection Regulation implementation date has come and gone, compliance efforts undertaken by security and compliance groups within many global organizations are far from achieved. In fact, in many cases, the work is just beginning.

As a risk-based regulation, the GDPR requires organizations to determine and implement data security best practices. These best practices apply differently depending on the circumstances of specific organizations.

As most organizations have learned by now, the GDPR applies to any organization that processes the personal data of European Union citizens and residents or provides services to EU residents. Organizations in any industry or sector, including profit and nonprofit, operating in the EU or selling goods and services to EU residents are in scope for this regulation.

One of the main goals of the GDPR is to address the lack of accountability seen under previous data protection regulations such as the EU Data Protection Directive. To increase data-related protections given to data subjects requires organizations to define what best practices should be implemented and, perhaps more importantly, to create a plan to continually monitor and adjust these best practices as technologies used by organizations and cybercriminals evolve.

GDPR and data security

With organizations relying more heavily on big data and the resulting business intelligence derived from such information, personal and corporate data is now more valuable than ever. At the same time, this business intelligence is more at risk.

Given that accountability and enforcement are two of the key aspects of GDPR, organizations must look closely at operational behaviors and evaluate how those behaviors tie into their current and future approaches to information security. Furthermore, because Article 30 of GDPR requires records of processing, it is imperative for organizations to know how and why data is being collected, stored and processed.

Specifically, organizations need to establish information security best practices to ensure that data is:

- Collected for specific purposes.
- Processed securely, limiting risk of compromise.
- Stored for a defined amount of time.
- Wiped to remove personally identifiable data when necessary.

In addition to the records criteria touched upon in Article 30, GDPR also requires full disclosure of processing activities through privacy notices (Article 13) and identification of legal basis for data processing (Article 6), and it also lays out conditions for obtaining data subject consent (Article 7).

All these requirements mandate that organizations establish ongoing, risk-based due diligence internally, and for any third party that might access or process their data. While data controllers and processors have different roles under the GDPR, the potential of large fines and associated reputational damage for noncompliance means that all involved parties must take exceptional care with information security practices.

Establish best practices

As organizations continue honing their approaches to information security to address GDPR-related requirements, they will need to fill the historic gaps typically found with out-of-date and often antiquated practices.

Organizations can begin to shift focus from detection and remediation efforts to more proactive measures by embracing current security-related best practices including:

- Establishment of more robust data protection policies for current and forward-looking privacy principles.
- Creation and enforcement of appropriate mobile device management policies and standards, including operating system policies, passwords, encryption, remote wipe, bring-your-own device criteria, lost or stolen device policies, and apps policies and management.
- Development and effective maintenance of up-to-date encryption standards for servers, systems, laptops and mobile devices.
- Establishment of a formal, physical, and logical security training program for all personnel and a well-planned and rehearsed approach to incident response.

Security-related best practices can address critical components of GDPR compliance. However, by establishing such robust practices, organizations can also begin to realize a significant return on investment.

Consumers want to know their information is safe, properly secured, and handled appropriately, which is increasingly reflected in their spending habits. Employees also want to trust employers' handling of their personal data, so organizations interested in securing the best talent should take GDPR compliance seriously. Organizations that understand the importance of GDPR compliance can better attract and serve consumers and engage talented employees.

Get proactive

Data is the most valuable asset for organizations today. The related information security practices put in place to secure that data are not only critical for compliance and governance issues, but for aspects of operational, reputational, and fiscal concerns as well. As organizations move deeper into 21st-century technology and data requirements, they can use increasingly stricter regulatory requirements to help propel business forward.

Though it might seem an onerous task, the GDPR and efforts to maintain compliance could bring improved efficiencies, savings, and cost benefits to organizations that embrace it. Even more, consumers and employees might be more likely to gravitate toward companies that prioritize maintaining privacy rights and strong information security.

Learn more

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

This article was originally published online on July 9, 2018, by Information Management.

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document.
© 2018 Crowe LLP.

RISK-19003-003A