Crowe

September 2017

Six Tips for Approaching Implementation of the General Data Protection Regulation

An article by Mindy R. Herman, PMP, and Pamela S. Hrubey, CCEP

Companies across the globe are grappling with the complexities associated with privacy and data protection. While the General Data Protection Regulation (GDPR) was established, in part, to "simplify" and coalesce compliance requirements across countries within the European Union (EU), few leaders – whether privacy officers, audit executives, ethics and compliance officers, or information executives – will find the new regulation, effective May 25, 2018, to be simple to implement.

Preparing to comply with the terms and conditions associated with the GDPR is a daunting task. Some companies are at higher risk for early regulatory action, and many have made considerable progress on their compliance road map. If compliance with the GDPR will be an organization's first attempt at establishing a comprehensive, global privacy and data protection program, getting started will be extremely challenging. This article describes six suggestions for companies to consider early in their efforts to comply with the requirements of the GDPR.

1. Identify and Establish a Core Team

Organizations have different levels of understanding and maturity of compliance programs and state of compliance with existing data privacy directives. Some organizations are just beginning to understand the business imperative associated with processing regulations covering personal data and with developing data privacy efforts. But no matter how mature an organization's program or state of compliance might be, one of the first things it can do about the GDPR requirements is to establish a core team and framework to spearhead the compliance effort. Team members should include individuals who play key roles in the organization, specifically in units where use of personal data is a business necessity. Such business units might include marketing, sales, finance, human resources, information security, internal audit, compliance, procurement, third-party management, and privacy. Using a core team framework can help facilitate early efforts and secure additional approvals for the resources necessary, whether internal or external, to support compliance activities.

2. Start Something

Numerous companies are spending precious time debating what to do to establish compliance with the GDPR. Because the regulation expects organizations to be prepared to perform numerous tasks that may deviate from previous directives or regulations, it is natural to desire simultaneous strategic assessment and operational action. Unfortunately, contemporaneously engaging in these activities can create a significant delay in implementation. Despite reports that numerous U.S.-based companies anticipate being in a state of only partial compliance on the implementation date of the GDPR, regulators have signaled that an extension of the compliance deadline is unlikely.

From a practical standpoint, many organizations begin with a gap assessment or an inventory of personal information. If the organization does not have a high-level inventory of its business practices that includes personal data, it will be important to have some context of this for gap assessment activities. Organizations should consider comparing the obligations associated with their existing information security and data protection-related policies with the provisions of the GDPR as a starting point. If an organization does not have existing policies and procedures, it should draft policies that address the provisions of the GDPR and that take the procedural implications into account in light of the organization's current situation so that gaps can be understood.

3. Work Incrementally

Compliance with the GDPR might require more than one evaluation of a specific topic before full adherence to the regulation is established. For example, the "right to be forgotten" provision within the GDPR requires organizations to understand the full extent of personal data processing across the global enterprise so that they can remove a specific individual's personal information from any system or repository within the organization. Companies may discover, after building an initial data map, that previously undiscovered uses of personal data may necessitate updates to data maps. Post-acquisition integration activities are yet another source of unexpected data uses.

The GDPR also requires that organizations conduct privacy impact assessments (or data privacy impact assessments) when new systems might require use of personal information. Conducting periodic assessments to maintain a current perspective about where personal information is stored across the organization is a worthwhile undertaking.

4. Recognize Potential Challenges With Compliance

The GDPR moves privacy and data protection beyond the existing boundaries associated with the EU Data Protection Directive and other country-specific laws and regulations. This new approach places individuals firmly in a position of power when it comes to uses of or associated with their personal information. Organizations must be able to determine – before using an individual's personal information – why, how, where, when, and for how long an individual's personal information will be processed. Organizations must obtain consent from individuals in advance, and the language associated with the consent must be explicit and easily understood.

Determining the possible uses of personal data before collection may require organizations to remediate existing data governance processes – or launch new ones – since past practices may have relied on examination of the collected data to determine relevant uses instead of aligning consent provided with allowed use. Organizations should consider including business representatives in data governance processes, when possible, to help business leaders understand the related implications associated with individual data subject control over the uses (or halt to uses) of personal data, unless otherwise prohibited by law. Thinking strategically – well in advance of requesting data subject consent – about how data will be used increases the likelihood of obtaining explicit consent, enables individuals to understand how data will be used, and allows the organization to limit such use to the consent received.

5. Capitalize on Existing Work

Over the last few years, many organizations have focused on improving the status of their information security programs in light of what some have described as the ongoing war against cyberattacks. Fortunately, organizations can often springboard from their foundational information security programs when addressing GDPR-related compliance obligations.

Specifically, organizations are expected to maintain numerous information security-related practices, including data breach protocols. Organizations are also expected to address third-party information security practices, since while data processors providing support for data controllers have specific accountabilities under the regulation, data controllers continue to be responsible for specifying the ways in which personal data will be processed. As such, data controllers have heightened exposure, and organizations must consider ways to review the practices of data processors before and after contractual agreements are reached.

Organizations that have adopted robust information security audit programs can use the results of associated audits to highlight compliance with the GDPR or to identify associated compliance gaps so that appropriate mitigations can be designed and deployed. Organizations without robust information security audit programs may find that now is the right time to introduce additional information-related controls with associated compliance-related inspections or oversight.

In a similar manner, third-party risk programs are valuable tools that support contractual requirements between data controllers and data processors. Such programs help data controllers verify compliance with GDPR-mandated requirements as well as the implications associated with subcontractor oversight.

6. Take Advantage of Existing Projects

Compliance with the GDPR requires a simultaneously practical and strategic approach. Strategic thinking affords the organization the ability to grasp the broad, enterprisewide implications of the regulation. Approaching implementation from a practical mindset helps organizations identify and use existing initiatives that might be related to managing personal data. Additions to existing project portfolios may be less expensive than creating independent projects.

Organizations should enthusiastically engage business leaders in GDPR-related compliance efforts. Despite decades of compliance with sector-specific privacy laws in the United States, for example, many organizations are finding compliance with the GDPR to be a heavy lift. Getting and maintaining buy-in across the organization is critical both in the short term, in the race to the implementation deadline, and in the longer term, since it will take time for the GDPR-related compliance obligations (including privacy by design, privacy impact assessments, and more) to feel like business as usual.

Compliance Journey

Some of these tips are likely to resonate no matter where an organization is on its compliance journey. Expectations and their associated regulatory enforcement are shifting. If those expectations are not met or if compliance is not achieved, consumers, employees, and regulators can negatively affect your company's brand and finances. If your organization is not progressing toward compliance, it's time to start.

Learn More

Mindy Herman
Principal
+1 317 706 2614
mindy.herman@crowe.com

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

crowe.com

Text created in and current as of September 2017; Cover and artwork updated in May 2018.

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. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2018 Crowe LLP.

RISK-18400-029A