Presented by information management | SourceMedia Marketing Solutions Group

5 THINGS TO KNOW

and Do—To Get Ready For GDPR

Sponsor content from collibra™

Market research indicates that most organizations lack significant knowledge about GDPR.

The Global Data Protection Regulation is a vitally important—but not widely understood—mandate for safeguarding individual data for Europeans. It affects large numbers of international organizations, not just those based in Europe, and its implications are substantial. Read this paper to get up to speed on the regulation and what you should do today to avoid regulatory, financial, and operational problems.

Anyone working for an organization doing business with European consumers needs to know about—and get ready for—the Global Data Protection Regulation (GDPR). Passed in 2016 as a key part of the European Digital Single Market initiative, it aims to align personal privacy statutes already in place across different European states by harmonizing data protection requirements and methodologies. Although the regulation won't go into effect until May 2018, the window is closing fast on organizations to come into full compliance in order to avoid hefty financial penalties for violations.

Data governance professionals, as well as executives and employees from legal, security, IT and most lines of business, will be deeply involved in planning, implementing, managing, and monitoring their organizations' progress with GDPR. Unfortunately, most organizations have yet to fully grasp the magnitude and complexity of GDPR compliance, as well the tools and systems necessary to meet the mandate's requirements.

THE AWARENESS AND READINESS GAP

Market research indicates that most organizations lack significant knowledge about GDPR. In fact, a recent study shows that more than four times as many survey respondents said they have never even heard of the regulation than those who said they are very knowledgeable about it.[1]

This massive gap in GDPR knowledge and readiness levels is important on several levels. First—and perhaps foremost—is the potentially large financial penalty for non-compliance. Regulators have warned that fines for non-compliance may reach as high as 4% of annual revenue. Second, organizations risk loss of consumer confidence and trust that their personal information will be properly safeguarded against current—and future—threats. This undoubtedly can result in substantial loss of revenue and profits. Third, organizations risk major damage to their hard-fought brand reputations that will be exploited by competitors to further undermine buyer confidence.

And, it's important to note one stark and unyielding requirement of the regulation: organizations must report on data breaches within 72 hours of their occurrence. Just think of some of the highest-profile data breaches in recent years—Target, Sony, Yahoo, and others—and how long it took before breaches were uncovered and reported.

[1] "GDPR: Perceptions and Readiness," Dimensional Research, September 2016

Data governance and GDPR compliance are inextricably linked because they each require an absolute commitment to the accuracy, accountability and timeliness.

DATA GOVERNANCE'S ROLE

In order to safeguard data privacy for European consumers and ensure regulatory compliance, organizations need to make data governance a top priority. Data governance and GDPR compliance are inextricably linked because they each require an absolute commitment to the accuracy, accountability and timeliness of the data, as well as an ability to identify the state, source, and usage of the data.

This alignment is not accomplished for a single point in time or solely to ensure an organization can pass an annual GDPR audit. It must be a long-time, continuous process that is as much about improving operational efficiencies in how personal data is handled as it is about avoiding penalties and the ignominy of damaging headlines around data breaches.

For many organizations, this necessitates further commitment to the data governance function, which has not yet become a universal part of how organizations manage data. Without the central role of data governance, GDPR compliance will be elusive, at best, with major negative implications.

WHAT ORGANIZATIONS SHOULD KNOW, AND DO, ABOUT GDPR

There are a number of important things organizations need to know about GDPR in order to prepare for the regulation and limit the potential impact on the enterprise. But even more important, there are vital steps organizations should be taking—now—to ensure compliance. Remember: Time is of the essence.

1. Keep in mind that **GDPR applies to every organization doing business with individuals in Europe and collecting personal data—not just those organizations based in the EU.** Of course, even those organizations not currently collecting personal information on Europeans for business reasons should assume they will be doing so at some point in the near future, and thus will need to be ready for GDPR.

2. There is **no "grace period" for compliance, nor is there any wiggle room for reporting within the 72-hour notification timeframe** after a breach occurs. Any organization that has done business in Europe knows they take personal data privacy very seriously, so it's important to look at those requirements as mandates, not as threats.

3. **Get real-world advice on the legal and operational angles of GDPR compliance.** Chances are that your legal department—and if not them, certainly outside legal experts—will already know many of the ins and outs of the regulation, and will be ready to advise accordingly. There also are consulting firms with expertise beyond the legal issues, such as how to align processes for data handling, data categorization, and data retention with systems and infrastructure for the right amount of data protection for specific use cases.

An organization's successful GDPR implementation requires the right use of the right people and the analysis and deconstruction of relevant business processes.

4. **Build your GDPR compliance team, starting with data governance professionals**. In fact, organizations should consider hiring or appointing a chief data officer (CDO) to lead the charge. Gartner predicts that 90% of large organizations will have a CDO in place by 2019, due to such intersecting factors as compliance, legal protection, the use of data as a competitive advantage and the need to become most cost-efficient in the use of data. If you have a data governance office in place, chances are it already incorporates team members from IT, finance, legal, security, and other line-of-business functions. If not, be sure you populate your GDRP compliance team with a diverse cross-section of skills and experiences. Locating and working with creators and owners of business data is essential.

5. Remember that **GDPR is really much more than a compliance mandate**. Yes, it has many of the common elements of regulations such as rules, penalties, and audits. But ensuring that private data is protected with rock-solid security and smart rules on data handling also has tremendous operational benefits. Successful GDPR compliance is predicated, to a large degree, on tight alignment with business goals and the involvement of line-of-business executives from customer-facing functions such as sales, finance, service/support, and marketing. Tight collaboration also means honest, two-way communication on how GDPR compliance could impact normal business processes, such as where data is stored and what kind of authority or role is required to access or edit it within databases.

BRINGING IT ALL TOGETHER: SELECTING THE RIGHT TOOLS

Of course, much of an organization's successful GDPR implementation requires the right use of the right people and the analysis and deconstruction of relevant business processes. But make no mistake: it also requires purpose-built technology solutions based on the guiding principles of data governance that are optimized for GDPR compliance.

In order to properly implement GDPR solutions that minimize risk and ensure compliance, organizations should look for solutions that provide:

- A centralized inventory of personal data items across business applications and technical infrastructure, as well as classification of these data elements.
- Governance accountability and personal data workflow over the full data lifecycle
- Searchable, end-to-end traceability of personal data
- Centralized regulatory and legislative rules
- A clearly defined, compliant, incident management process
- Data impact assessments within the governance framework

One solution that addresses all these issues—and more—is the Collibra Data Governance Center, an enterprise-wide platform that automates data governance and data management. The Collibra platform is designed to address a broad spectrum of capabilities that are integral to GDPR compliance, as well as to the day-to-day operational issues that the regulation touches on.

If your systems aren't in place, and aren't operational, on May 25, 2018, your organization will risk non- compliance fines, sanctions and negative publicity.

For instance, the Collibra platform places a high priority on rapid notification of potential breaches of personal data. Its search, data classification, and data helpdesk functions are designed to enable easy visual impact assessment and reduce the time required to find critical answers to breach-related questions.

Additionally, Collibra helps organizations deal with the all-important issue of individual consent on the capture, storage, and usage of personal data with an integrated, automated policy management function.

Collibra also accommodates cross-border data transfers and supports vendor management with data sharing agreements, policy management, and data classification. It also enables adherence to codes of conduct through certification of data stores and processing activities by collaboration and metadata ingestion.

As a leader in data governance, Collibra provides a solid platform upon which GDPR compliance and operational agility are built, extending and enhancing the value of organizations' governance systems.

Finally, never lose track of the fact that there is a specific, looming deadline. If your systems aren't in place, and aren't operational, on May 25, 2018, your organization will risk non-compliance fines, sanctions and negative publicity. Don't wait any longer.

For more information on how Collibra can help your organization prepare for, and absorb, the impact of the imminent GDPR mandate, please visit **www.collibra.com/GDPR**