THE GDPR IS COMING. ARE YOU READY?

Introduction

If you do business anywhere in the world, there is a good chance your organization processes data about individuals in the context of selling goods or services to citizens of a European Union (EU) country. And if so, then you will need to comply with the General Data Protection Regulation (GDPR). What is the GDPR? It's a regulation intended to strengthen and unify data protection for individuals within the EU. It was approved and adopted by the EU Parliament in April 2016 and will be in force May 2018.

The GDPR is being called the most important change in data privacy regulation in 20 years. It not only applies to organizations located within the EU but it will also apply to:

- Those outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects;
- All companies processing and holding the personal data of individuals residing in the European Union, regardless of the company's location.

The data it refers to includes any unique information related to a person that can be used to directly or indirectly identify said person. It can be anything from:

- A name,
- A photo,
- An email address,
- Bank details,
- Posts on social networking websites,
- Medical information, or
- A computer IP address.

In the GDPR, conditions for consent have been strengthened and companies will no longer be able to use vague terms and conditions full of legalese. Consent must be:

- "Clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language;"
- As easy to withdraw consent as it is to give it;
- Explicit for processing sensitive personal data. In this context, nothing short of "opt in" will suffice. However, for non-sensitive data, "unambiguous" consent will suffice.

The Cost of Compliance and Non-Compliance

The enterprise model breaks down traditional departmental silos and brings disparate units and data-sets together for the common goal of ensuring a value-driven patient experience, keeping people safe and healthy, all while saving money. But how does an organization actually get to that point?

There is a tiered approach to financial penalties, and organizations can be fined up to 4 percent (€20 million) of annual global turnover for breaching GDPR. This is the maximum fine that can be imposed for the most serious infringement, such as not having sufficient customer consent to process data or violating the core concepts. Less serious infringements have a max fine of €10 million. It is important to note that these rules apply to both controllers and processors; meaning clouds will not be exempt from GDPR enforcement. There is a provision for class action and individual prosecution depending on the breach.

In addition to fines and penalties, there is also the cost of compliance to consider. As an example, if every EU visitor to an American theme park in the last few years requested deletion of any of their data, the company that owns the park may be forced to spend a fortune to identify all the patrons and photos taken of them on systems throughout the park and delete them.

As a general trend the regulatory environment is getting more complex and prescriptive. There is recognition that data is an asset and hence the focus on data will continue to rise. With just under a year until the regulation comes into force, time is critical and companies should start planning for GDPR now.

Are You Prepared?

Board and executive management support is critical for ensuring the organization's culture shifts from healthcare consumption to value-based healthcare. Communication is important, and ensuring every stakeholder has a seat at the table is necessary. But all the talk in the world isn't enough without quality, meaningful data. Technology that unites data for risk management is critical, but alone it isn't enough if the different business units aren't equally engaged in the end goal of moving to an enterprise model.

According to Gartner, 50 percent of organizations will be non compliant by end of 2018 and facing the prospect of heavy fines proposed for non-compliance. This will be a significant transformation, involving the whole gamut of things, which at a high level will include:

1. **People.** Appointment of a Data Protection Officer, establishing ownership around data security and training of personnel.
2. **Processes.** A risk-based approach to data protection. Significant changes to processes to comply with the new clarifications around data subject rights, availability of information, complaints management, data security assessments and audits, interaction with the supervisor, complexity to deal with third-party data processing and overall governance.
3. **Tools.** The selection of a tool to enable the required efficiency and effectiveness.

Each organization will have its own approach to address this based on the business, geography, processes (data security and wider), infrastructure and the unique cultural landscape. At a high level, recognition of the impact given the possible consequences of non-compliance and initiative with the right level of senior sponsorship within the organization will be key. Working backward from May 2018, when the EU GDPR regulation comes into force, organizations should have an inventory of the processes impacted followed by a high-level definition of the framework for the organization to comply.

As a strategic view, given the regulatory environment will be getting more complex while the cost pressures will continue to exist, to drive efficiencies while meeting regulatory needs a technology solution will be key. To meet the regulatory timeline at a high level this should be done in the first half of 2017 with a tool selected and implementation of a technology solution in by end of the year, giving time for the solution to bed in before the regulation comes into force in May 2018.

Organizations can address the GDPR compliance with a consultancy-based approach or a solution-based approach. The former being engaging professional services firms for definition of the data assessment framework, taxonomy, and processes. To meet the tight timelines, a solution-based approach might be an attractive option. This includes leveraging the solutions available in the market then adapting and configuring the solution and the internal data framework to meet the compliance needs.

The Importance of the Right Technology

Given the depth and breadth of the scope of the regulation, organizations should secure an easy-to-use, flexible, scalable (internally and externally to third parties) and most importantly, integrated, tool to meet the data security compliance demands of the enterprise. Some core functionalities to consider are:

- A risk-based approach to data protection;
- Automation to drive efficiencies (i.e., general efficiency with workflows, notifications, etc., but also to capture and leverage agreements for future similar requests); and
- Compliance and adaptability for future regulatory and individual company needs.

To further break down those functionalities, having the following features within the technology are important for ensuring your organization's ability to comply with the GDPR:

1. **Process and systems inventory.** Identify your processes/systems and establish data ownership.
2. **Internal audit.** Assess the processes/systems and third parties for the data security compliance using questionnaires, workflows and notifications.
3. **Issue and action management, including breach notifications**. Prepare detailed actions plans to address the gaps identified in data security assessments.
4. **Regulatory interaction**. Manage interactions with regulatory and internal stakeholders within the solution for a complete view of your data security needs in one place.
5. **Management of Contracts and Corporate Policies**. Keep a central repository of all contracts and policies within the solution.
6. **Ongoing data sharing request management**. Automate data sharing requests processes efficiently with pass-throughs based on existing data sharing contracts.
7. **Data request management and governance**. Manage requests for information.

8. **Vendor risk management**. Manage your third parties and their ongoing data security access requirements assessments.
9. **Reports and dashboards**. Provide comprehensive analytics and and audit trail of the data security activities within the organization for ongoing monitoring/assessment and regulatory needs as required.

Conclusion

The GDPR and its hefty fines for non-compliance are coming in a little over a year. Businesses must also consider the cost of compliance and begin preparing now to get the proper people, processes and tools in place. In addition, organizations can expect that in the current regulatory environment, there is recognition that data is an asset and the focus on data will continue to rise. When considering technology, one that is easy-to-use, flexible, scalable and most importantly, integrated, is vitally important to the success of complying with this regulation as well as what may come in the future.

About Riskonnect, Inc.

Riskonnect is the trusted, preferred source of Integrated Risk Management technology, offering a growing suite of solutions on a world-class cloud computing model that enable organizations to anticipate and manage strategic and operational risks across the enterprise. For more information about Riskonnect, contact us at www.riskonnect.com, email info@riskonnect.com or call **770-790-4700**.