Enterprise Information Management and the GDPR: 7 Steps to Readiness

Written by Bob Larrivee,
VP Chief Analyst - AIIM Market Research

The GDPR

In April 2016, the General Data Protection Regulation (GDPR) passed in the European Union (EU) and will be enforced beginning in May 2018. The intention of the GDPR is to strengthen and unify data protection for all individuals within the EU. As with most regulations of this type, the impact is on businesses within the EU, but also extends beyond to any company transacting business within the EU.

In short, the GDPR has an international impact on how businesses manage and protect their EU related information and data assets. Aside from GDPR, there are implications businesses must be concerned with in relation to data privacy and protection.

In order to comply with the GDPR, businesses must manage and protect personal data of EU residents

---

A recent study by AIIM titled "Understanding GDPR Readiness in 2017" shows thirty-one percent of respondents reporting data loss or exposure within the last twelve months and the primary reasons cited are staff negligence or bad practices not technology or hacking. Sixteen percent of respondents reported internal or HR incidents due to unauthorized access. The result of these breaches is the exposure or loss of Personally Identifiable Information (PII) on employees, customers or citizens as a result of these data breaches. As an organization that does business in or with the EU, you must prepare and prevent this from happening.

Here are seven steps you can take to begin your path to readiness.

1 Understand the requirements and your obligations under the GDPR

First and foremost, it is important to have an understanding of the terminology, principles and impacts of the GDPR if any, to your organization. Some of the first things you need to know:

- What is your organization's role in the processing of personal data? Are you a data controller, data processor or both?
- Controllers and processors are free to appoint Data Protection Officers (DPO) but some organizations are required to do so. Are you obligated to assign a DPO?
- What is "personal data" and do you hold it?
- There are a handful of child-specific provisions in the GDPR. Do you process the personal data of children under 16?

2 Create a data map and classify information

Second, you should know what personal data you have and where you have it stored. This means that you must be able to identify, locate, and track all of the personal data under your control in all systems, repositories and databases across the enterprise. Some key steps:

- Create a data map of all physical and digital personal information across your organization, where that data flows in and outside of the organization, and who has access to it
- Understand the purpose for which it was collected and determine if and how consent is documented
- Classify and categorize personal data using metadata for identification, search, and lifecycle management

3 Secure and ensure the confidentiality of personal data

Third, it is your responsibility to safeguard that personal data is processed in a manner that ensures appropriate security and confidentiality, regardless of where the information resides. In order to aid in providing tighter control, you can do the following:

- Prevent unauthorized access to or use of personal data by applying technology enablers such as access controls, permissions management and encryption
- Leverage audit trails to monitor user activity and provide chronological evidence as proof of data integrity
- Gain visibility to what your 3rd parties are doing around security and privacy for data they process on your behalf

4 Create a unified view across your enterprise

Fourth, have a greater overall view of your content across the enterprise, one that is unified rather than scattered and sewn together. By connecting your data and content you'll have better control and ability to meet portability, correction and deletion requirements. Some strategies include:

- Tie data embedded in line-of-business applications to unstructured information repositories
- Enable users to improve data quality and remove redundancy
- Remove content silos and increase information accessibility

5 Limit purpose and enforce data minimization

Fifth, when you capture information, limit it to a specific purpose (for which you have consent) and dispose of it when processing for that purpose is complete. The "capture as much data as possible for use to be determined later" approach is one that could potentially put you at risk. When developing your capture strategy, consider the following:

- Collect data to be used only for specific, explicit, and legitimate purposes
- Ensure that personal data are kept only for their required length of time
- Implement automated deletion processes based on retention and disposition rules

6 Review and update information management policies and procedures

Sixth, organizations must review all policies and procedures to ensure they reflect privacy principles and requirements, and if they do not, that they are updated to be compliant. Staff and 3rd parties must be trained on the new ways of working. A few things to help you in this area include:

- Reviewing policies related to information classification, security, consent collection and records retention
- Developing new or updating procedures may be required such as data breach notification and responding to information requests
- Formalize education and awareness programs to ensure that all staff and 3rd parties who interact with personal data are trained on the new regulation

7 Establish data protection by design and by default

When developing designing, selecting and using systems, services, and products that process personal data, organizations should take into account data protection principles. While this is a short interpretation, measures you can take include:

- Take into account the principles of data protection by design and default when in discussions with technology and service partners, as well as in the context of public tenders for products and services
- Ensure that by default, only necessary personal data for specific purposes are processed
- Choose technologies that provide automated metadata classification, access controls, and analytics capabilities to help identify and process personal data in a compliant manner

Ask yourself this

- Do you understand your obligations as a data processor, data controller or both?
- Do you know what personal you process, where it is stored, and who has access to it?
- How do you document what consent has been given, for what purpose and when it expires?
- How is personal information secured throughout its lifecycle internally and if it needs to be shared with external parties?
- What processes are in place to dispose of personal information or to present it upon request, in accordance with GDPR requirements?
- Do you have routine audits and reviews to ensure your information governance practices are being followed and what corrective measures are in place when infractions are found?

In Conclusion

The GDPR is not just an EU regulation, it is regulatory reform with global impact reaching any and every organization that interacts with EU residents. Non-compliance can result in severe fines and worse, loss of customer or citizen trust. However there is still time to prepare. Follow these steps toward good enterprise information management, and you'll be well on your way to GDPR readiness.

(Note: While the information contained in this document provides insight that can be beneficial, it is in no way intended to serve as or be considered as legal guidance. AIIM strongly recommends businesses seek professional, legal advice, and services in addressing compliance needs related to GDPR.)

[1] *Reference: EU Data Protection Regulation: All You Need to Know*

Developed in partnership with:

opentext™

OpenText enables the digital world, creating a better way for organizations to work with information, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

www.opentext.com/gdpr

aiim

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education, and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators, and consultants.

www.aiim.org/Training

AIIM (www.aiim.org) AIIM is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data.

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
+1 301.587.8202
www.aiim.org

AIIM Europe
Office 1, Broomhall Business Centre
Broomhall Lane, Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.org