General Data Protection Regulation (GDPR) Implications Are Profound and Global – It's Necessitating Data Governance and Master Data Management

Global Impact: GDPR applies to any company that does business in the EU and the fines are substantial (per violation up to the greater of 4% of the organization's global annual revenue or 20 million EUR) – The deadline for compliance is May 2018 and many organizations are remiss in implementing data governance and master data management which are seen as a strategic imperative to ensure compliance. What's your plan?

Introduction

There is a good chance that 2017 will be the year of (the single version of) truth for many organizations, particularly for those that count European residents among their customers. A massive driver of this change is the General Data Protection Regulation (GDPR). GDPR will provide natural persons in the European Union (EU) with additional protections and provisions to guard their personal data from unlawful use by third parties. The regulation which will enter force in May 2018 (without any additional grace period) imposes drastic fines for any violation.

Organizations that in the past have taken a wait-and-see approach or speculated with risking a financial penalty instead of investing in the necessary upgrades of their data processing environment may want to reconsider; the fines are really hefty (per violation up to the greater of 4% of the organization's global annual revenue or 20 million EUR) and may therefore dwarf any investment necessary to comply. Most importantly, GDPR's impact is global, as it does not only apply to entities domiciled in Europe or having European subsidiaries, but also to any organization worldwide that transacts with European residents!

What is GDPR about?

GDPR has been conceived to protect natural persons being in the EU with regard to the processing ("collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction") of their personal data.

GDPR extends the scope of what was previously considered "personally identifiable information." Within the regulation, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject')" whereas "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Who needs to comply with the provisions of GDPR?

Although GDPR originated in the EU, the implications of the regulation are definitely global. Affected organizations may fall into two main categories:

- Controller (defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data")
- Processor (defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller")

As part of a GDPR assessment, organizations must be able to identify if they fulfill a "processor" and/or a "controller" role concerning interactions with personal data of European residents.

From a geographic perspective, the regulation applies to

- Any entity worldwide that - for purpose of business or behavior monitoring - processes personal data of natural persons being in the EU regardless of whether that entity acts on its own ("controller") or on behalf of another entity ("processor").
  Examples:
  - *A US B2C business [controller] with customers residing in the EU*
  - *A British Cloud SaaS provider [processor] that - on behalf of a Canadian entity [controller] - hosts personal data about German residents in a CRM database on premises in India*
- Any EU entity that processes personal data of natural persons worldwide regardless of whether that entity acts on its own or on behalf of another entity.
  Example: A French B2C business with customers residing in the US

What are these obligations?

For organizations within the scope of GDPR, the obligations can be substantial. The first obligation is to understand the regulation and its potential impacts on the business. Then organizations need to put in place an education and governance framework to manage and control the inventory and flow of personal information in, through, and out of the organization. GDPR identifies several tasks and responsibilities, particularly in the following areas:

Structural Organization

- Appoint a Data Protection Officer ("DPO") [GDPR Art. 37-39]

Development of Business Processes / Applications

- Identify critical entities & attributes (for existing applications: datasets & data fields) that relate to personal data ("any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person") [GDPR Art.5]
- Analyze business processes / applications and document the flow of personal data including
  - the purpose (what) and location (where) of the processing as well as their processors (who)
  - the categories of data subjects
  - the categories of personal data
  - the security measures for personal data
  - the retention periods for personal data

  [GDPR Art. 30]
- Assess the risk level of personal data at rest (storage) and in motion (processing) [GDPR Art. 35-36]

- Establish standards for the collection of personal data [GDPR Art. 12-13]
- Adjust business processes / applications so that
  - the data subject can give its consent for a specific purpose of processing
  - the data subject can withdraw its consent for a specific purpose of processing
  - the status of consent is documented

  [GDPR Art. 6 – 7]
- Adjust business processes / applications so that the data subject can execute its right to
  - receive transparent and complete information about its personal data [GDPR Art. 14-15]
  - rectify its personal data [GDPR Art. 16]
  - "be forgotten" [GDPR Art. 17]
  - portability of its personal data [GDPR Art. 20]
  - restrict the processing of its personal data [GDPR Art. 18]
  - object to the processing of its personal data [GDPR Art. 21-22]
- Adjust business processes / applications so that they
  - are lawful, fair and transparent in relation to the data subject
  - use personal data limited to the specific purpose consented by the data subject
  - minimize the scope of processed personal data
  - foster keeping personal data accurate
  - limit the duration of storage
  - risk-appropriately protect personal data against unauthorized or unlawful processing, accidental loss, destruction or damage by measures of access control and masking (pseudonymization, anonymization and encryption)

  [GDPR Art. 5, 32]
- Set up contracts for sharing personal data with third parties [GDPR Art. 28, 44-50]

Operation of Business Processes / Applications

- Notify the supervisory authority and the data subjects of a breach of personal data within 72 hours [GDPR Art. 32-33]

Conclusion

Like many new regulations, GDPR could initially be perceived as just another burden upon an already resource and budgetary constrained organization. At second glance, the vast majority of regulations only formally express what should have been common sense and best practice for a long time (e.g. some foresighted organizations began to implement master data management (MDM) systems almost two decades ago). In fact, a functioning MDM system (at least for the domain Party) significantly facilitates achieving compliance with the provisions of the GDPR.

In this spirit, regulatory requirements such as the GDPR should be welcomed as an opportunity to lay the foundation for data governance and master data management which not only prepares an organization to react more flexibly to future regulations, but also transforms its capabilities to effectively manage data, provide transparency and build trust in its data assets.

How we can help

To meet the GDPR deadline, time is of the essence. However, hastily implemented solutions come with concessions in quality and increase the costs in a long term. Therefore, a solid, but flexible data governance framework is indispensable.

Infogix and Grandite have formed a partnership to help organizations build a generic and sustainable data governance framework based on Infogix Data3Sixty™ that can embed the provisions of GDPR, as well as other general or industry-specific regulations into a flexible and business-centric platform.

With an extensive background in metadata management as well as in IT audits, we have the expertise to coach and advise organizations on how to adjust the processes in development and operation to meet data governance requirements and achieve regulatory compliance.

Infogix Data3Sixty™ and Grandite's SILVERRUN constitute complementary tools that are highly configurable to seamlessly support the workflow within the data governance framework covering regulatory, business and technical aspects. Infogix Data3Sixty™ and SILVERRUN help to create a metadata inventory by reverse engineering existing application databases or simply capturing organizational knowledge. Together, they enable users to map out application data flows and assess related risks, as well as take it a step further delivering the functionality to model business processes and business data domains (e.g. master data), a prerequisite to reduce application silos and secure future systems. On the enterprise level, Infogix Data3Sixty™ and SILVERRUN assist in the blueprint for a long-term information map and define strategies to accomplish business goals through well-governed states of data management. Thus, Infogix Data3Sixty™ and SILVERRUN particularly accelerate the conversion of data obligations into valuable information assets.

About Infogix Data3Sixty™

Infogix provides best-in-class data management and governance solutions that seamlessly integrate into operations and allow clients to manage highly complex, data intensive business environments. Infogix Data3Sixty is the leading provider of cloud based data governance collaborative solutions. It leverages a streamlined approach that ensures quick time-to-market by providing a cloud-based deployment with a low level of internal IT dependencies. Infogix Data3Sixty is an intuitive platform which provides "day one" value by automatically connecting to value-add content sources and making that information immediately available to end-users.

Website: http://www.infogix.com

Contact: http://www.infogix.com/contact

About Grandite

Grandite is the Business Modeling and Software Engineering Company.

Grandite provides professional business process, data and UML modeling tools featuring the functionality necessary to successfully implement enterprise architecture development, master data management and data governance. Grandite complements its portfolio with product-related services, e.g. training classes, technical support and consulting.

Website: http://www.grandite.com

Contact: info@grandite.com

infogix

Infogix data and analytics solutions can save you time and money.
Visit www.infogix.com or call 1.630.649.6800 (US, Canada. and International), +44 1242 674 137 (UK and Europe).

twitter.com/Infogix facebook.com/Infogix linkedin.com/company/Infogix plus.google.com/+Infogix