What is the GDPR?

Effective May 2018, the European Union General Data Protection Regulation (GDPR) enhances protection of personal data, and replaces the EU Data Protection Directive and its local implementing laws. This regulation could have significant impact for organizations and how they manage data pertaining to customers, consumers, partners, staff and other 'data subjects'; where a 'data subject' is an individual. The GDPR impacts the storage, processing, access, transfer, and disclosure of an individual's data records as well as having some potentially very large penalties for violations.

Who is affected?

These protections apply to any organization established in the EU and to any organization (anywhere in the world) that processes the personal data of EU data subjects when offering them goods or services or when monitoring or tracking their activities.

How does this impact you?

The GDPR imposes a range of additional requirements beyond what was formerly required under the EU Data Protection Directive. For example, the GDPR expands existing data subject rights and creates entirely new ones, such as the right to data portability. The GDPR will require organizations to fully understand how they utilize current and future information assets to incorporate these new data privacy requirements. For many, the associated changes to information management practices will require a thorough evaluation of current and future data capabilities.

Is there a governing body?

The GDPR will be enforced by each Member State's supervisory authority. As a regulation, the GDPR will be directly effective in Member States without the need for local implementing laws. The GDPR has established mechanisms to help harmonize its implementation across the various Member States.

What are the basic controls that must be met before May 25th, 2018?

Among the key requirements of the GDPR are: (1) the ability to facilitate data subject rights, such as access, correction, objection, erasure and data portability, and (2) the implementation by design controls of the data protection of lawfulness, fairness and transparency; purpose limitation, data minimization (including thought psuedonimization); accuracy; storage limitation integrity and confidentiality; and accountability.

How can Informatica help customers with their GDPR compliance?

GDPR poses many challenges, but it also has the potential to result in opportunities around the use of data to an organization. Informatica's depth in data management can help organizations address challenges on their GDPR initiative journey and introduce innovative data management capabilities to

maximize the potential opportunity. Informatica delivers integrated and intelligent software solutions for governance and compliance to support organizations in their GDPR initiative.

Below is a highlight of how Informatica can help across challenges and use cases.

To provide the foundation for your GDPR journey, you need to define and assess your data. See the first two descriptions below. Depending on your goals, you might consider looking at controlling access to your data or even looking to centralized your data across your organization as outlined below.

Goal	Challenge	Capability Requirement	Technology Use Case
Define	How do I define & govern in scope data?	Policy Interpretation	Enterprise Data Governance
Assess	Where is all our in-scope data?	Sensitive Data Discovery & Risk Analysis	Sensitive Data Intelligence
Control	How do I prevent unauthorized access?	Enabling Data Security Controls	Sensitive Data Protection
Manage	How do we manage subject data information?	Personal Data Management	Data Matching, Linking and Mastering

Next, we'll look at each of these in more detail:

How do I define and govern in-scope data?

Challenge: Digital transformation and the growing amount of data affects every industry globally. A significant percentage of this data can be attributed to individuals, which potentially falls under the scope of the GDPR. As data proliferates in an organization, the ownership, control and management of this data becomes more challenging. In some cases, you know your risks but you need to know what you don't know. GDPR initiatives will be optimally achieved through an enterprise-wide approach to data governance.

Capabilities Needed: Policy interpretation is a capability to capture both business and technology understanding of policies, responsibilities, processes, data terms, logical and physical models. Crucially, it is also the location where understanding of the technical environment is linked to the understanding of the business environment. This linkage provides an organization with a holistic view of information about their in-scope data Domains and forms an integral part of an approach to managing their data assets,

Recommendation: A holistic data governance and compliance initiative powers the data-driven results you need to succeed in the digital age. Adopting a data governance solution that enables business and IT functions to work together towards the common goal of data governance gives you a competitive advantage. **Informatica Axon** enables non-technical business analysts and LOB managers to efficiently operate data governance programs to optimize business outcomes such as regulatory compliance and

risk. Axon enables users to define and manage processes, policies, systems, people, and data using a crowdsourced, collaborative and automated methodology.

Axon is powered by Enterprise Information Catalog (EIC), providing a machine-learning-based discovery engine to index, curate, and increase the understanding of all enterprise data assets.

Benefit: Quick and easy contribution from all subject matter experts, to define the processes, policies and data entities the organization to rapidly build a holistic data governance capability for in-scope data and processes.

Where is all our in-scope data?

Challenge: Data in most enterprises is siloed and scattered across many systems, applications and sources. Organizations should not only consider data in core application systems, but also spreadsheets, local databases and big data solutions. Organizations also need to consider "what if" planning for informed prioritization of remediation, prioritize their budget as well as accuracy and scalability to complete assessments of thousands of data stores.

Capabilities Needed: Sensitive Data Discovery & Risk Analysis is a capability to discover sensitive data across a wide range of technology solutions. Along with this sensitive data, other sources of information such as the amounts of actual data and data proliferation, are used to create a risk score for data. The risk score helps organizations understand where the highest risk data is stored so that any potential remediation or security control requirements can be prioritized, based upon it's risk score. Tracking the risk score over time shows whether remediation or control activities have improved the data risk position. If the risk score hasn't improved, the risk score history tracking enables organizations to target new efforts that address the data stores with the highest risk data.

Recommendation: Informatica's **Secure@Source** helps discover the locations of in-scope data, classify the data, monitor data proliferation including protection status and assign risk scores. Tracking over time, shows how changes are positively or negatively influencing compliance efforts.

Benefit: Provide insights into not just the location and movement of data but also rank data according to risk in terms of the GDPR scope. This helps support budget justification and prioritization of remediation activities such as controls or protection.

Additional data management needs you might have on your GDPR journey:

How do I prevent unauthorized access?

Challenge: Data security controls are needed to ensure privacy data is not viewed by unauthorized users. There is a requirement on from IT viewpoint to encrypt, remove, mask or pseudonymize production data used for all purposes; internal processes, customer services, order processing, analytics, reporting, etc. Data access control for personal data at a user level in applications should be reviewed for compliance purposes.

Capabilities Needed: Enabling data security controls is a capability to provide access control and protection of information on data subjects. Data Subject information is often exposed to many different

individuals across an organization and its ecosystem. Data security controls are used to remove or hide data subject information from those who shouldn't have visibility of it, whilst making the information available to those that should.

Recommendation: Adopt solutions that can help with privacy and security of data assets. Informatica **Persistent Data Masking and Dynamic Data Masking,** could be used to help to automatically limit the number of people and systems that have unrestricted access to personal data. Informatica **Secure@Source** provides data security remediation by orchestrating updates to security controls via Ranger, Sentry and extensible to support other third party protection systems.

Benefits: Introduce automation into data masking to reduce risk of breaches of personal data and help ensure that personal data is not proliferated without suitable protection.

How do I manage data subject information?

Challenge: As a direct result of the diverse usage of data in complex IT environments, creating a single view of all information for individual data subjects is challenging. This challenge stems from the fact that different systems use very different mechanisms to store and index data. Without a complete view of an individual data subjects' data and how this is stored, managed or processed within an organization, GDPR compliance will be challenging, especially around individual data subject's rights. Companies with a poor consent mastering system will see data as a risk, and will take a defensive position to avoid penalties, affecting the business agility and losing competitive advantage.

Capabilities Needed: Personal data management is a capability to identify data subject records within all identified sources, match and link records together for each individual data subject and create a Data Subject repository, which delivers a 360 view of personal data and all the associated consents. This repository provides a source of high quality data on what actual data records are held across the in-scope sources and how each piece of data is linked to an individual data subject. The 360 view can act as the authoritative source of data when organizations are responding to Subject Access Requests, Right of Erasure Right to be Forgotten or Right of Portability requests. For these types of requests, organizations need to be able to quickly identify all the data they hold about an individual data subject, regardless of location or system that data is held in, so a 360 view can help provide that capability.

Recommendations: Adopt solutions that gather data subject records and consents from all channels, using advanced algorithms to match all data related to the same data subject, regardless of where the data is stored. **Informatica MDM** provides the foundation for a single view of all party data and their relationships, providing a purpose-based perspective for each subject required for each process. As part of the market's only end-to-end MDM solutions, **Informatica MDM – Multidomain Edition** leverages advanced algorithms to identify data associated with the same data subject from any domain (customers, prospects, employees, visitors). Informatica MDM BPM capabilities permits the organizations to govern workflow-based operations such Right to be Forgotten and Right of Portability.

Benefits: A single view of individuals has shown to have business benefits beyond GDPR. This is especially true if the individual in question is a customer, who are increasingly expected tailored personal experiences. From a GDPR viewpoint, the ability to link all data for each individual data subject will ease the burden of enabling individual's rights. This includes the right to understand data usage, right to be forgotten and ensuring consent is correctly applied. With correct management of the

consents, data will no longer be viewed as a risk. It will be viewed as an asset, providing organizations more agility, gaining competitive advantage.

Ongoing partnership for your compliance journey?

Informatica is committed to continuously supporting you on your GDPR journey. As regulations are constantly being updated, we deliver the solutions and services to help you be successful. We also work together with highly trained and skilled partners to offer a holistic approach based on your needs to provide a deep understanding of governance and compliance.