How meeting GDPR benefits your business

Accelerate adoption to drive competitive advantage with your data

IBM **Cloud**

Introduction

Thanks to recent regulations, the landscape of data privacy and protection regulatory compliance evolves almost weekly. There's the EU General Data Protection Regulation (GDPR), the US California Consumer Privacy Act (CCPA) expected to go live in January 2020, and Brazil's privacy regulation that is expected to go live in February 2020. Other countries like India, and multiple American states are progressing their own regulations, too.

Organizations must now enact, comply and sustain their readiness to these regulations where applicable. IBM Unified Governance and Integration solutions provide a key framework to help organizations in this journey. These solutions help clients keep less data on hand, with demonstrable accountability of the purpose and use of the data in their custody. These solutions establish data controls that can help organizations develop more transparent and trusted relationships with customers for the long term.

GDPR and other privacy regulations can function as a roadmap for organizations to establish a strong information and data governance program. According to a study, two-thirds of customers say they feel more empowered to share data when they trust it.

Governance helps build confidence in your data, which can increase productivity and reduce risk. Organizations with effective governance can:

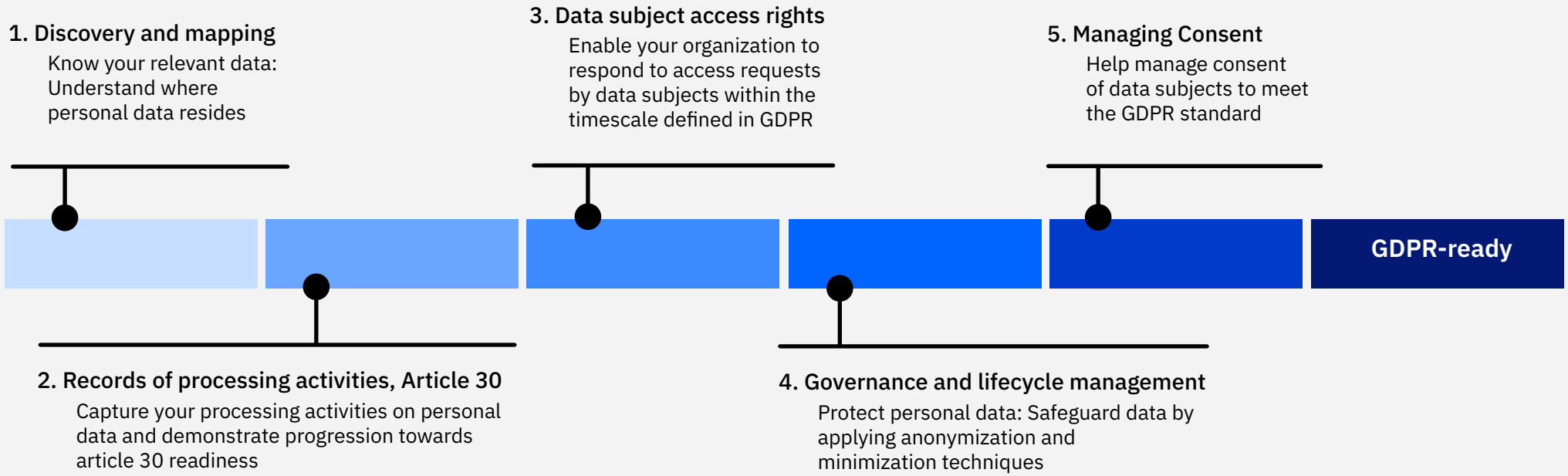
- Enhance brand value and loyalty
- Support new planned digital offerings and channels for clients
- Reduce costs for future digital and IT transformation projects
- Achieve competitive advantage by supporting data subject requests
- Create transparency by publishing ethical standards
- Become data-driven using specific customer insights and targeted marketing
- Prepare for compliance readiness and business productivity
- Serve as a base for artificial intelligence initiatives around trusted data

GDPR is not simply a regulation requirement for EU data subjects' personal data, but a wise way to help grow your business through a client– and data-centric transformation, no matter the privacy regulations that apply.

IBM offers multiple solutions for personal data discovery and mapping, processing activities, lifecycle management, data subject access rights, and the governance and management of personal data and consent. IBM solutions come with specialized accelerators to expedite your GDPR journey. These solutions also use machine learning accelerators that can process vast amounts of unstructured or structured data to discover, define, catalog and protect your personal data at scale.

5 building blocks to prepare for GDPR

There are 5 key building blocks to develop to reach full compliance. Which one you start with depends on where you are today. Assessment is the first step—a clear picture of where you stand today will prepare you for a complete view of where you need to go.



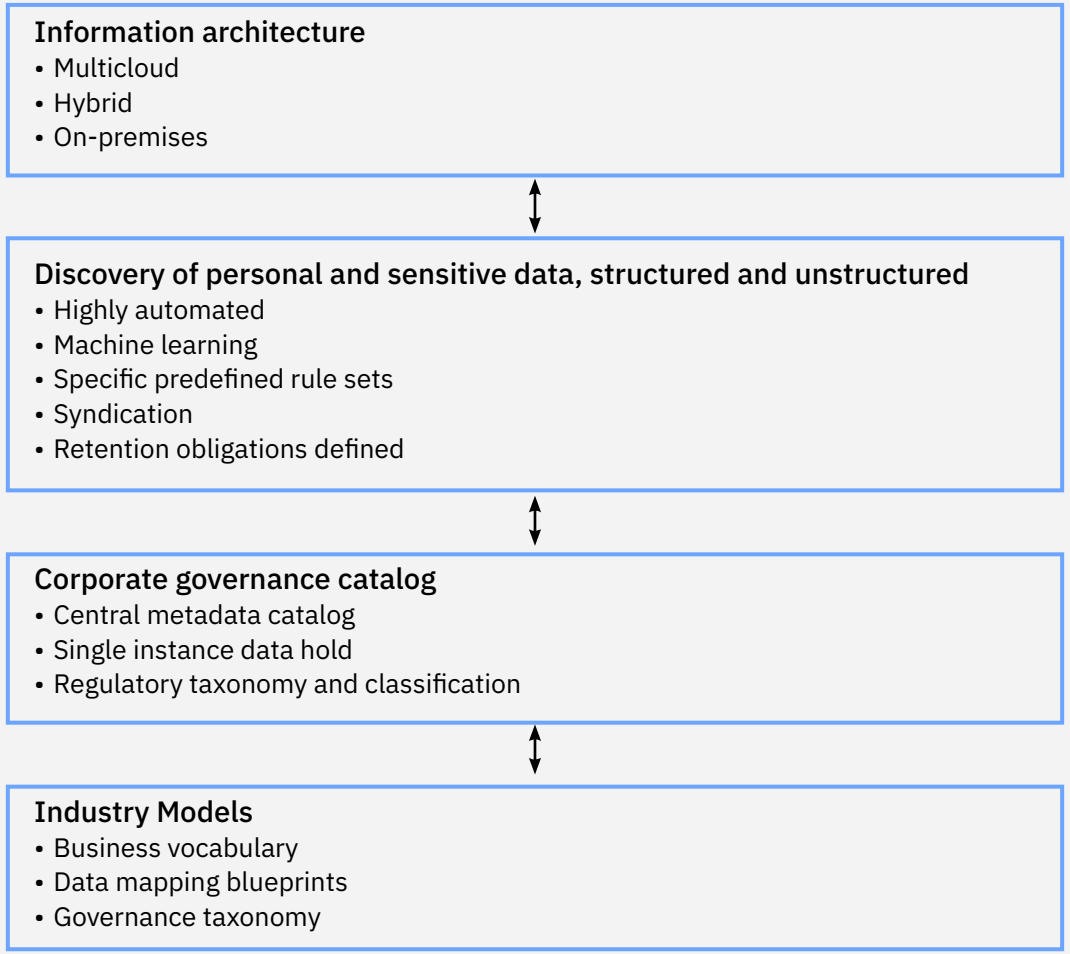
Discovery and mapping

You can’t manage data if you don’t know what it is or where it is. Discovery and mapping is a foundational step where structured, semi-structured and unstructured data is reviewed and classified, helping define the location and type of personal data that’s stored in your information system. This step allows you to discover existing personal data in your information assets and helps visualize processing activities.

According to a recent IBV study, data discovery and ensuring data accuracy are the biggest focus areas for organizations. GDPR content in IBM industry models is designed to support data mapping and provides an accelerator blueprint for personal data for specific industries. Structured and unstructured data discovery requires different and specific techniques. IBM solutions can meet the spectrum of your data needs by helping you to:

- Understand where your data resides
- Define your inventory of personal data
- Discover where personal data is stored with preset definitions of personal data patterns using regular expressions and machine learning
- Reveal shadow data repositories
- Process structured and unstructured data and store results in a common privacy catalog

IBM offers solutions across four main areas for discovery and mapping



Records of processing activities (ROPA)

A requirement in Article 30 of GDPR is to maintain records of processing activities to document your handling of personal data. You need a strong, scalable and flexible central source to understand what personal data you hold, how you have captured it, what it's doing and where it's stored. IBM helps enable companies to address these requirements through appropriate tooling and by using artifacts provided by the IBM GDPR template.

From the template dashboard, administrators can visually track processing activities by selecting filters like data controller, data processor or location. Companies with multiple brands can report by line of business and location. The dashboard is customizable and provides an idea of how data governance can be implemented. It also provides an assessment of an organization's security infrastructure and information handling procedures.

Data subject access rights

As defined in Article 15 of the GDPR, organizations are to complete data subject access requests (DSARs) within one month. This risky burden can be demanding for organizations, particularly those with millions of customers. Automated processes can make the difference between being compliant by meeting these requests and failing to meet stated expectations.

IBM solutions hold your governance information map and make it actionable, helping you focus on which subset of data sources may contain relevant content. Streamline the DSAR decision-making case management process with repeatable and personalized responses to the data subject. IBM solutions provide auditable tracking, management and execution of DSARs for Article 15 using a single catalog that processes criteria for each data subject.

Governance and lifecycle management

Under the GDPR, organizations are responsible for protecting personal data in their systems. Many look to techniques like pseudonymization, which replaces the primary identifying fields within a data record by one or more artificial identifiers, or pseudonyms. The data is processed in such a way that it can no longer be attributed to a specific data subject without the use of additional information. This supports the business through decreased storage costs, and prevents information loss by providing the IT team with a solution that supports a common way of protecting data.

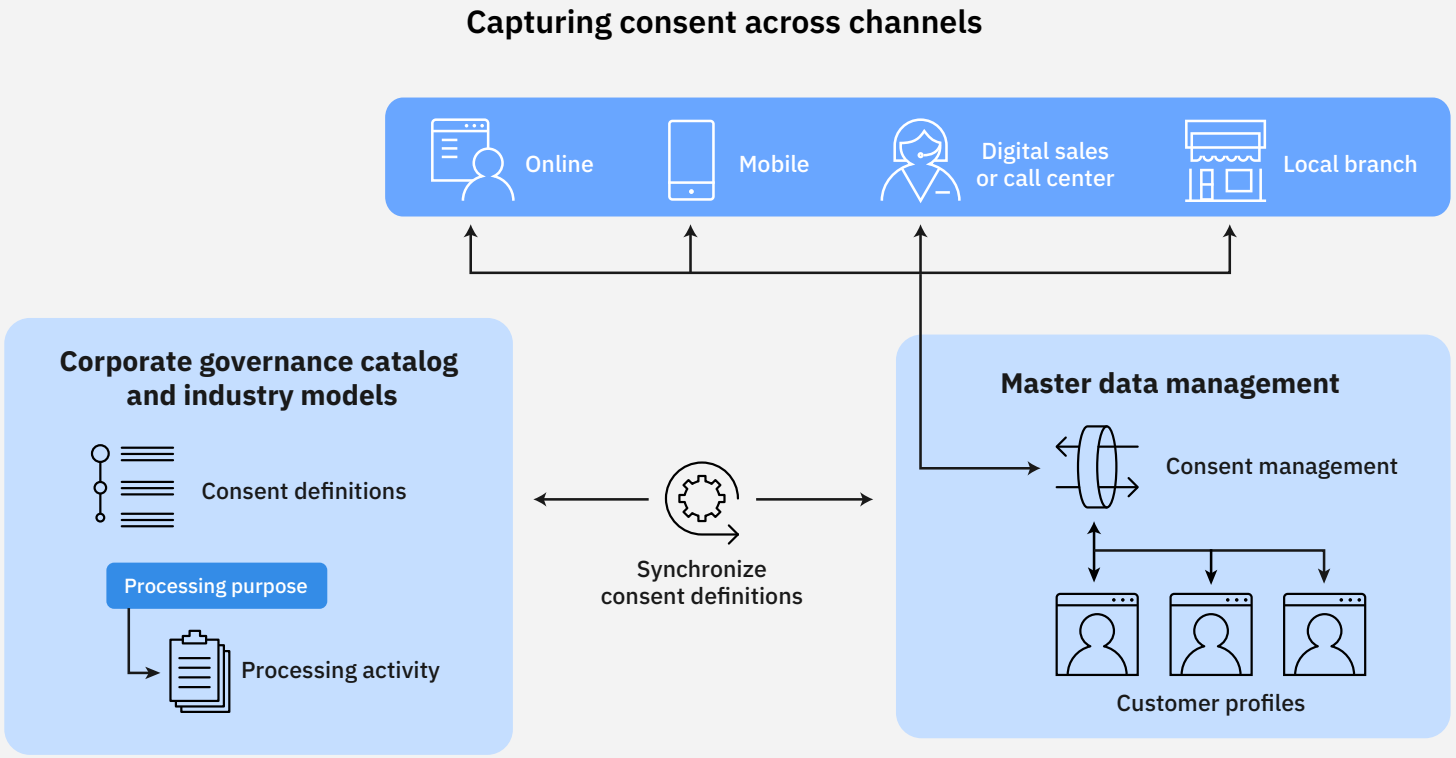
IBM solutions help organizations obfuscate data, so it no longer contains personal and sensitive information. This anonymization and minimization reduce the risk of exposure. This technique can mask business objects across heterogeneous databases and applications. You can also archive and remove data that's not being used. By applying retention policies, these steps automate the disposal of old data, reducing the inventory of personal data in your organization going forward.

Protect and manage data at virtually any stage with governance and lifecycle management

Manage consent

Under the GDPR, consent is one of the six lawful bases for processing data. Consent can also legitimize use of sensitive and personal data, special category data, and the restricted processing, automated decision-making and overseas transfers of such data. Previously, organizations might gain consent by offering users a tick box to express acceptance of certain terms and conditions. With the GDPR, consent is to be managed on a more granular and transparent level.

Each processing purpose is associated with one or more processing activities, which define how personal data is processed, stored, recorded or disseminated. With the consent management feature of the IBM Master Data Management solution, you can manage an individual's consent regarding the processing of their personal data. The consent stored in the MDM solution can be associated with profiles of data subjects that are either saved in an external profile system or in a virtual or physical MDM repository. You can also define and govern processing activities and sync those definitions into your MDM solution. This step adds activities to your consent management process.



Why IBM

Compliance with the GDPR is part of building a trusted analytics foundation that exceeds discovery and mapping of personal data. Your organization needs to be able to understand, trust and use its data. True governance is an ongoing journey that's weaved into the daily activities of your organization to make it sustainable. With a strong, scalable platform, an organization is poised for success across many business needs.

Three-fifths of respondents to a recent IBV study see GDPR as an occasion for transformation or to spark new data-led business models. Increased agility allows data users to achieve business results, across many of their regulations.

To learn more about how IBM Unified Governance and Integration can accelerate your GDPR journey, and to learn more about how IBM managed its journey, visit ibm.com/analytics/gdpr.

IBM GDPR Disclaimer

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2018