Getting to the GDPR: Four key use cases to jumpstart your efforts

IBM Security Guardium helps simplify preparation for the General Data Protection Regulation

Highlights

- Act swiftly and embark on an assessment and readiness campaign for the General Data Protection Regulation (GDPR)
- Support key data protection elements of the GDPR to support personal data protection
- Leverage an end-to-end, adaptable approach to data protection with IBM® Security Guardium®
- Get started with the Guardium GDPR Accelerator, which provides prepackaged functionality to help jumpstart your GDPR efforts

The European Union (EU) made an impact across the globe with passage of the GDPR in May 2016. When it goes into effect on May 25, 2018, all companies—including international firms—doing business with individuals located in EU member nation territory must comply with the law's far-reaching provisions. All living EU individuals' identifiable personal information—regardless of where it is sent, processed or stored—must be protected, and proof of protection must be verified. The regulation states, in fact, that the protection of personal data is one of the "fundamental rights… of natural persons."[1]

Conversations with industry analysts reveal that many organizations have not recognized the potential impact of this game-changing regulation and may be ill-prepared to sufficiently meet its demands. Many non-EU-based organizations, for example, have yet to realize that the GDPR applies to them, too. Companies are not exempt from the GDPR just because they don't have offices in the region or don't process data in an EU member state: Failure to prepare for the regulation could have serious consequences—to an organization's bottom line, customer relationships and brand image. Noncompliance with the GDPR could cost as much as EUR20 million in fines (approximately USD22.3 million) or up to four percent of their total worldwide revenue for the preceding financial year, whichever is higher.[2]

GDPR preparation will take time. IBM believes that now is the time for organizations to begin allocating budget and resources to implement governance processes and controls, and to identify tools to help with compliance. To assist, IBM Security has created a GDPR Readiness Assessment to help uncover privacy and security gaps and recommend remediation plans. Additionally, Guardium provides prebuilt templates and assets to help accelerate your work to comply with several of the key GDPR data-protection obligations.

Data privacy and protection of the individual is the impetus for the GDPR

Cloud, mobile computing, big-data platforms and the Internet of Things (IoT) have all heightened the challenge of sharing, managing, governing and securing information. And within this context, there also has never been more awareness of the need to protect personal data, which could include national IDs, email addresses, or location data; biometric, physical, physiological, genetic or mental health data; economic, cultural or religious sentiment data; social, political or gender preference data; and more.

The GDPR aims to protect individuals and their personal data through unified, modernized standards, and a set of meaningful rights for individuals. Some of the GDPR obligations include:

- **Condition for consent**, mandating that organizations obtain explicit consent to gather information from individuals (known as data subjects)—and be able to prove that they have done so. Consent is limited to specific purposes, and data subjects have the right to withdraw consent at any time.[3]
- **Right to access and obtain data**, allowing data subjects to request access to information held about them, and to learn how it is accessed, the purpose of the access, where it is being accessed, what categories of data are being accessed and who has access.
- **Right to erasure**, giving data subjects the right to request the deletion of personal data if they do not wish to allow its use.
- **Right to rectification and objection to profiling**, granting data subjects the right to request corrections in personal data if it is inaccurate and allowing them to object to profiling that may result in discrimination against them.

These data subject rights raise a daunting question: How does an organization get started on a GDPR compliance program and successfully meet its obligations?

The GDPR: Are you ready?

The GDPR notes that an organization should exhibit consideration and commitment to individuals' data privacy by implementing a "data protection by design" approach "when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task."[4] It is prudent for companies dealing with personal to build privacy and security protections into their applications, services and products from the start. Unfortunately, many organizations have now been thrown into a position where they may have to catch up—and catch up fast.

To help speed organizations down the path to GDPR readiness, IBM Security recommends conducting an assessment of the organization's data privacy and security practices. The goal is twofold: identify areas of risk, and design processes for mitigating those risks. The findings from the assessment can help you form your foundation for a GDPR roadmap that should support four key activities to help manage and protect personal data.

1. Assess data protection readiness to identify and mitigate security vulnerabilities
2. Discover and classify personal data

3. Implement controller and processor governance to track where personal data is processed and create an audit trail
4. Manage personal data breaches and notify the organization if and when a breach occurs

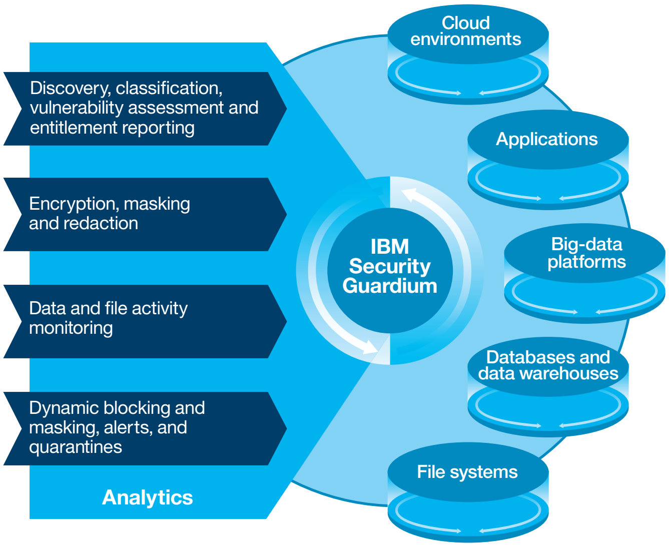
For both the short and long term, companies may view GDPR obligations as a catalyst for organizational change—an opportunity to reassess and think smarter about data protection and the positive impacts of a solid approach to data security, privacy and protection. Organizations that embrace the competitive advantages of a structured yet evolving data protection program—including helping in enhancing customer trust and loyalty, as well as empowering employees with the right level of data access—can reap benefits for years to come.

Track data subject access rights

As part of a global security initiative, a major French bank needed to control database access to its 400 servers via strong authentication mechanisms on 150 sensitive applications. The bank uses Guardium as its tool to help track data subjects' access rights and automatically modify, delete and transfer data as required by the GDPR.

Guardium allows the organization to:

- **Automatically import access rules from the bank repository into the Guardium system via application programming interfaces (APIs)**
- **Capture, monitor and report on database commands used to build, modify or manipulate database content, and enforce change controls affecting database entries**
- **Report on detailed SQL, including source and date**
- **Track and report failed logins and block unauthorized users and non-network logins**


Discovery, classification, vulnerability assessment and entitlement reporting
Encryption, masking and redaction
Data and file activity monitoring
Dynamic blocking and masking, alerts, and quarantines
Analytics
IBM Security Guardium
Cloud environments
Applications
Big-data platforms
Databases and data warehouses
File systems

Guardium: Accelerating data protection and privacy to support the GDPR

Best practices encourage a strong data privacy and protection program. Designed to safeguard personal data across a broad number of environments, Guardium is a data protection solution that offers an end-to-end approach to protecting valuable data, including personal data, intellectual property, proprietary information, partner data and more that organizations rely on to run their businesses. As an adaptable, modular platform, Guardium empowers security and compliance teams to automatically analyze risk, prioritize efforts and respond to what is happening across their data repositories in real time.

Guardium can help provide answers to some of the key questions about personal data access and control that the GDPR mandates:

Help identify and mitigate security vulnerabilities

- Identify threats and security holes in databases that could be exploited by hackers, and provide detailed mitigation guidance
- Scan database infrastructures to identify exposures such as missing patches, weak passwords, unauthorized changes or misconfigured privileges

Discovery: Where is the personal data located?

- Discover and classify personal data and uncover compliance risks based on your criteria
- Analyze data usage patterns to help rapidly expose and remediate risks with advanced, automated analytics and machine learning
- Support centralized management and heterogeneous integration into the existing environment; and adapt to changes in the environment, such as new users, or expanding volumes of data

Monitoring: How is data being used—and by whom?

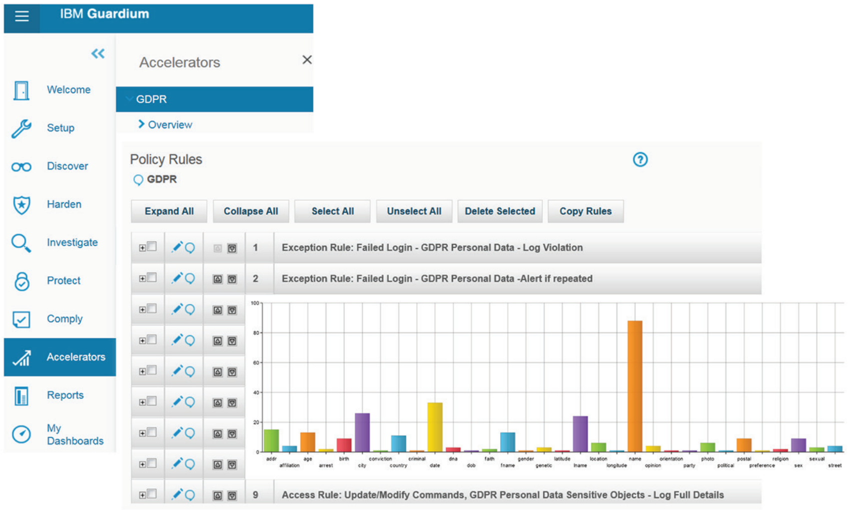
- Monitor who is accessing and reading data, spot anomalies and stop data loss with near-real-time activity monitoring and alerting across the enterprise
- Aid in preventing unauthorized data access and receive alerts on changes or leaks to help ensure data integrity
- Reduce operational costs through streamlined control and tracking of privileged users' shared ID access

Encryption, masking, redaction and blocking: How is data being protected?

- Employ rigorous entitlement reporting, encryption, masking, redaction, dynamic blocking and alerting to protect personal data from being accessed, used, lost, or changed, whether it's at rest or in motion
- Help shield the business from data loss and liability proactively with automated risk analysis, validation, automated compliance workflows and extensive audit capabilities
- Alert and dynamically block illicit internal and external data and file access in real time across a broad range of platforms—including databases, files and file systems, big-data environments, mainframe environments, and more

Compliance and audit reporting: Is it streamlined with automation?

- Capture compromised privileges and user entitlements
- Use automated analysis and compliance controls to detect and stop data access and use that violates compliance requirements
- Deploy quickly with prebuilt templates and assets that help accelerate your compliance efforts
- Support your entire data security protection journey—from GDPR readiness to providing real-time, automated data protection policies and controls—with a common, adaptable infrastructure and approach



1 Exception Rule: Failed Login - GDPR Personal Data - Log Violation

2 Exception Rule: Failed Login - GDPR Personal Data -Alert if repeated

9 Access Rule: Update/Modify Commands, GDPR Personal Data Sensitive Objects - Log Full Details

Accelerate GDPR readiness and data protection efforts

To be ready to meet their GDPR obligations, IBM believes that organizations need to start preparing now. Some obligations are may be relatively simple to meet, while others, such as enabling systems to support the right to be forgotten, may be more difficult to achieve since they may require business process changes. With the clock ticking, there's no time to waste before getting started. To help you get started, Guardium offers a GDPR Accelerator. This Accelerator provides prepackaged functionality to help jumpstart your efforts to address your GDPR risks and exposures by providing:

- A GDPR Data Security Impact Assessment that scans for data sources that contain GDPR personal data (as described above).
- Classification patterns to help identify GDPR personal data such as age, date of birth, gender, sexual preference, political opinion, email address, name, religion, religious opinion, international passport information, location information, genetic information, criminal record, biometric data, photo, address, city, postal code, country and more.
- Predefined sets of policy rules and groups that help monitor, audit, record and provide alerts on any unauthorized activities related to personal data by privileged and unprivileged users and applications. These same rules are also used to create audit trails for data subject requests, such as requests for personal data access, rectification, erasure or transfer.
- Reports to identify who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed—all of which can be used to send notifications to auditors, controllers and data protection officers using the data security compliance review process that is part of the Accelerator.

Let's take a look at why these capabilities are valuable, and how you may be able to leverage them to get ready for the GDPR.

The GDPR Accelerator provides a wealth of insight into GDPR personal data access by both regular and privileged users. But unless you know where personal data is stored and what it looks like, it cannot be monitored or protected. Therefore, a first step to tackling the GDPR requirements is identifying the personal data and where it is stored. The prebuilt classification patterns that come with the GDPR Accelerator help simplify and speed up this process.

As you get started, it's also important to assess the other vulnerabilities within your environment and across your data sources, so that you know where your additional weaknesses and risks are and can address them. The GDPR Accelerator provides prepackaged data security assessment tests, so that you can quickly perform vulnerability assessments on the personal data sources that you've identified and get guidance to help close the gaps. Once you understand the gaps and exposures, you may take steps to address those gaps and harden the personal data sources, so that unauthorized users cannot change the configurations or authorization settings of those sources. Using deep IBM expertise and proprietary methodologies, the GDPR Accelerator data security impact assessment can help identify these risk areas and help support audit-readiness for the GDPR.

Using these prebuilt assets helps streamline and speed the process of identifying personal data within an organization, and helps identify and assist in remediating risk on those personal data sources, so that you can start monitoring your identified data sources that contain personal data and take action as you determine if any suspicious behavior occurs. The GDPR Accelerator includes prebuilt policy rules and groups, to help you begin performing that continuous monitoring more quickly. The prebuilt policy rules help protect data sources with personal data from unauthorized access and activities—including changes, removal or replication, or deletion of records. The GDPR Accelerator also processes reports (which you can select on a by-user, by-controllers, or by-application basis) for data activity monitoring for all authorized and unauthorized activities to personal data. In addition, audit reports may be used to assist with incident response by providing a detailed activity report.

The Accelerator also help you to track and provide detailed audit trails on data subject access requests such as access to personal data, data rectification, erasure or transfer. Information such as the application user, database user, SQL, and timestamp is captured to an audit repository. Customizable reports are included that you can share with your compliance teams, auditors and others. The credentials for authorized individuals handling these data subject requests can be further secured by using IBM Security Privileged Identity Manager to manage credential check-out, check-in, and even detailed session recording that can be tied back to your Guardium audit reports.

The capabilities of the GDPR Accelerator, along with interfaces to a variety of tools in the underlying system, are organized in a tabular fashion by requirement, which can speed the implementation process and reduce time to value.

Finally, the Guardium GDPR Accelerator provides an automated workflow audit review process to support GDPR readiness. This capability automates the notification and review process for simplified and faster escalations and sign-off on the prebuilt audit reports for personal data activity, such as access, deletion, and updates by authorized and unauthorized users and applications, which should be documented, recorded and reviewed.

Why IBM?

Every organization operating in the EU or doing business with EU nations needs a comprehensive, enterprise-wide approach to data protection and GDPR compliance. Guardium provides best practices that help organizations to know their data status, reduce risks, tighten policies, and monitor and audit for compliance and policy violations.

Guardium helps provide an integrated and scalable data security platform that helps clients analyze risk to sensitive data, protect sensitive data and adapt to changes in the IT environment. Analytics makes it possible to deal with data complexity and data patterns, while governance and centralization assist in making the entire data protection functionality—addressing security, privacy and compliance—manageable within the array of heterogeneous data sources required to run an IT environment.

Additionally, Data Privacy Consulting Services from IBM can help you identify areas that may be impacted by the GDPR and provide guidance to help you create and deploy comprehensive privacy policies, standards, guidelines and operating procedures to align with best practices to assist with GDPR compliance obligations. Just as auditing is a part of data privacy governance, an upfront assessment is key to readiness. As you prepare for the GDPR, IBM Services can help optimize your level of control by establishing a data protection strategy that not only implements but also integrates resources, such as 24x7 data activity monitoring with global advanced threat intelligence and analytics.

Whether at the start of a compliance readiness initiative or broadening an existing program, organizations can effectively use the Guardium best practices roadmap to build in data protection safeguards to help prepare for the GDPR.

For more information

To learn more about IBM GDPR solutions, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/guardium

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♻ Please Recycle

[1] Article 1. 2. “Regulation (EU) 2016/679 of the European Parliament and of the Council,” April 27, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[2] Article 83, 5. “Regulation (EU) 2016/679 of the European Parliament and of the Council,” April 27, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[3] Article 7, “Regulation (EU) 2016/679 of the European Parliament and of the Council,” April 27, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[4] Paragraph 78, “Regulation (EU) 2016/679 of the European Parliament and of the Council,” April 27, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC