Ready, set, GDPR

Find the data you need to protect—and the security gaps that need filling

Highlights

- Swiftly embark on an assessment and readiness campaign for the European Union (EU) General Data Protection Regulation (GDPR)
- Get started with IBM® Security Guardium® GDPR Accelerator (functionality included in IBM Security Guardium Data Protection for Databases, IBM Security Guardium Data Protection for Data Warehouses, IBM Security Guardium Data Protection for Big Data, IBM Security Guardium Data Protection for z/OS® and IBM Security Guardium Vulnerability Assessment), which provides prepackaged tools such as prebuilt templates for GDPR-specific groups, GDPR-specific policies, and GDPR reports, all based on the IBM Security GDPR Framework
- Enrich your data protection efforts with data classification, risk assessment, activity monitoring, encryption and key-management capabilities

The EU made an impact across the globe with the adoption of GDPR in April 2016. The regulation describes the protection of personal data as one of the "fundamental rights… of natural persons."[1] In the years immediately following GDPR's announcement, many non-EU-based organizations did not realize that GDPR would apply to them, too. But when GDPR goes into effect in May 2018, all organizations doing business with individuals located in the 28 EU member states must comply with the regulation's far-reaching provisions. All EU data subjects' personal information—regardless of where it is sent, processed or stored—must be adequately protected, and proof of protection must be verified.

Analysts are now seeing increased queries and questions—from EU and non-EU-based organizations alike—regarding GDPR and its impact on organizations' operations and compliance cost.

1 Article 1. 2. "Regulation (EU) 2016/679 of the European Parliament and of the Council," April 27, 2016.

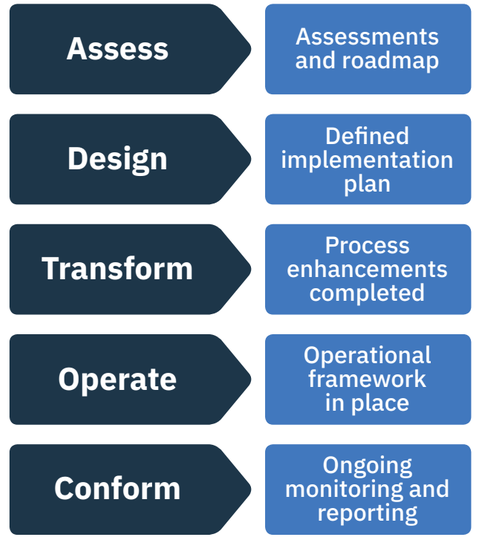
Why the time is now for GDPR compliance

Even firms without offices or data-processing operations in an EU member state are not exempt from GDPR—and failure to comply with the regulation could have serious consequences to an organization's bottom line, customer relationships and brand image. Noncompliance with GDPR, in fact, could cost an enterprise as much as EUR20 million in fines, or up to four percent of its total worldwide turnover for the preceding financial year, whichever is higher.[1]

GDPR compliance can affect company proceedings from sales to operations to record keeping, so enterprises are likely evaluating their privacy policies, security measures and processes to minimize the risk of a breach—or of noncompliance. Compliance teams are deploying tools and processes to:

- **Assess** risks, understanding which data is covered by GDPR and where it is
- **Design** standards for collection, use and storage of data, while balancing business risks and objectives
- **Transform** procedures, processes and tools to put data subjects first
- **Operate** new programs, continuously managing the data, its access and usage with respect for the rights of data subjects—the individuals to whom the data applies
- **Conform** to GDPR standards for monitoring, auditing and reporting

For both the short and long term, companies should view GDPR obligations as a catalyst for organizational change: an opportunity to reassess and think smarter about data protection, and about the positive impacts of improved data security and privacy. Organizations that embrace the competitive advantages of a structured yet evolving data protection program—including the potential for enhanced customer trust and tailored data access levels for employees—can reap benefits for years to come.



The IBM Security GDPR Framework was developed to help organizations address both security and privacy needs related to GDPR using a phased approach.

Learn why you need an action plan for GDPR.

1 Article 83, 5. "Regulation (EU) 2016/679 of the European Parliament and of the Council," April 27, 2016.

Keeping deadlines in mind

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

Some organizations are rapidly putting security and data management solutions into place—because only then can they begin to examine the practical application of GDPR obligations, such as record removal at a data subject's request and notice of a data breach within 72 hours.

GDPR preparation takes time and comes with a deadline. GDPR is scheduled to take effect in April 2018. So if they are not already on their way, now is the time for organizations to begin implementing governance processes and controls, and to roll out and test compliance tools. For efficient implementation, IBM Security has created a GDPR Readiness Assessment to help uncover privacy and security gaps and recommend remediation plans. Additionally, the Guardium GDPR Accelerator—a tool within the IBM Security Guardium Data Protection products for databases, data warehouses, big data, IBM z/OS and the Guardium Vulnerability Assessment product—provides prebuilt templates and assets designed to accelerate efforts toward your compliance with several key GDPR obligations.

Under GDPR,

personal data can't simply be held forever. Every business will need to periodically review its data governance practices and purge data that's no longer needed.[1]

Learn how IBM can help you no matter where you are on your journey.

1 "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016," *European Commission*, April 5, 2016.

Putting data subjects' rights first

GDPR aims to protect individuals and their personal data through unified, modernized standards, as well as through a set of meaningful rights for individuals, backed by potential penalties for noncompliance. Any organization that holds or processes the personal data of EU data subjects is obligated by GDPR provisions to:

- Obtain explicit consent to gather information from data subjects—and documentation to prove that the enterprise has done so. (Consent under GDPR is limited to specific purposes such as maintaining current contact information, and data subjects have the right to withdraw their consent at any time.[1])
- Implement data subjects' right to access and obtain data, allowing individuals to request access to information held about them, and to learn how and why it is used, where it is being accessed, what categories of data are being accessed, and who has access.
- Put into practice the "right to erasure," giving data subjects the right to request the deletion of personal data if they do not wish to allow its use.
- Provide data subjects with a process to correct inaccurate personal data, and allow them to object to profiling.
- Some firms may also be required to appoint a Data Protection Officer, to foster accountability of those responsible for GDPR compliance (such as controllers or processors) across the organization.

As important as these data-subject rights are for individuals, however, they raise a daunting question for organizations: How does an organization get started on a GDPR compliance program and successfully meet its obligations?

A major French bank with 400 servers and 150 sensitive applications

uses Guardium to help track data subjects' access rights and automatically modify, delete and transfer data as required by GDPR. Guardium allows the organization to automatically import access rules, track and report failed logins and block unauthorized users.[2]

Learn what you need to know about data privacy for GDPR compliance in this podcast.

1 Article 7, "Regulation (EU) 2016/679 of the European Parliament and of the Council," April 27, 2016.
2 Based on IBM customer case study interview conducted in 2016.

Evaluating your enterprise's personal data risk surface

GDPR compels organizations to respect individuals' data privacy by implementing a "data protection by design" approach as they develop, design, select and use any "applications, services and products that are based on the processing of personal data or process personal data to fulfill their task."[1] A prudent approach for companies dealing with personal data is 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 have to catch up—and catch up fast.

To help speed organizations' GDPR strategies, IBM Security suggests first conducting an assessment of the organization's data privacy and security practices. The goal is twofold: to identify current risks and to 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:

- Assess data protection readiness by discovering and classifying personal data
- Identify security risks through vulnerability scanning to prevent and mitigate any exploits or ransomware attacks on personal data
- Implement controller and processor governance along with technical and operational measures to track where personal data is processed, and create an audit trail
- Manage personal data breaches and notify data security administrators if and when a breach occurs by alerting and blocking with deep forensics and incident response

Guardium tools are helping organizations meet their GDPR obligations. Some obligations are relatively simple to meet. Others, such as enabling systems to support data subjects' right to erasure, may require business process changes across your organization.

In 2016, IBM X-Force® research recorded the highest single-year vulnerability count yet seen:

10,197.[1]

Learn how IBM Data Privacy Consulting Services can help your enterprise evaluate your readiness for GDPR.

1 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, March 2017.

Accelerating GDPR and data protection efforts

To help you get started, Guardium offers a GDPR Accelerator, providing prebuilt functionality to help discover your GDPR risks and exposures:

- GDPR Data Security Impact Assessment that scans for data sources, whether structured or unstructured, that contain personal data.
- Classification patterns to help identify GDPR-covered personal data such as name, age, date of birth, gender, sexual preference, email address, religious affiliation, location information, genetic information, criminal record, biometric data, photo, address and more, in both distributed and IBM z/OS environments.
- 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 that is part of the accelerator.
- Predefined set of groups, policies and reports that help enterprise security and compliance teams secure personal data—whether distributed across an enterprise, or centralized in IBM Z® mainframe environments.

Guardium GDPR Accelerator can provide a wealth of insight into personal data access by both regular and privileged users. But unless you know where personal data is stored and what it looks like, the data cannot be monitored or protected. The prebuilt classification patterns that come with the Accelerator help simplify and speed this process.

Personal data for GDPR purposes includes any information traceable to an individual,[1] such as:

- **Genetic information**
- **Disease or disability condition or history**
- **Cultural, religious and other affiliations**
- **Trade union membership**
- **Political affiliations or opinions**
- **IP addresses**
- **Internet cookies**
- **Identifiers such as radio frequency identification tags**

▶ Watch a video demonstration to see Guardium GDPR Accelerator in action.

1 "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016," *European Commission*, April 5, 2016.

How Guardium can support your compliance efforts

Guardium offers a holistic approach to protecting structured or unstructured data, including personal data, across a range of environments. The adaptable, modular Guardium platform can help compliance teams analyze risk, prioritize efforts and respond to events across their data repositories. Guardium tools can analyze data usage patterns to help rapidly expose and remediate risks with advanced, automated analytics and machine learning, while supporting centralized management and smooth integration. Beyond initial compliance, Guardium helps enterprises continuously conform to evolving GDPR needs with its ability to adapt to new users and expanding data volumes, and with data classification support for multiple EU languages.

How is data being used—and by whom?

- Monitor who is accessing data, spot anomalies and stop data loss with enterprise-wide, near-real-time monitoring and alerts.
- Help prevent unauthorized data access and receive alerts on changes or leaks to contribute to data integrity.
- Potentially reduce operational overhead through streamlined control and tracking of privileged users' shared-ID access.

How is data being protected?

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

Is compliance and audit reporting streamlined with automation?

- Capture compromised privileges and user entitlements.
- Use automated analysis to detect and block unauthorized data access.
- Deploy quickly with prebuilt templates and assets.

Discover, obscure, defuse

Guardium can help you discover and classify personal data to speed pseudonymization, and IBM Multi-Cloud Data Encryption, IBM Guardium Data Encryption, and IBM Security Key Lifecycle Manager solutions can help you obscure this data and manage its access, from individual sections of a database to Teradata environments to massive cloud-storage ecosystems—all through a single, centralized console.

Learn about how Guardium can help secure your enterprise.

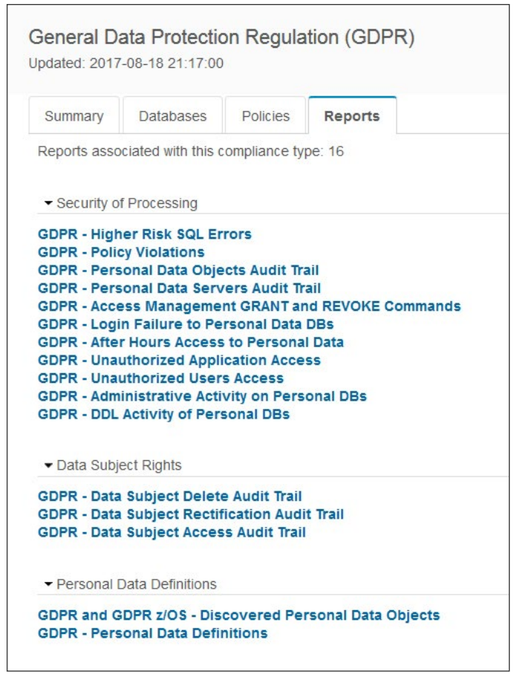
Heading off data breaches to help protect personal data

Data breaches impacting personal data require swift action to avoid noncompliance.[1] Only when you know where your security weaknesses and risks are can you address them. As you implement or refine GDPR solutions, it's important to address vulnerabilities within your environment, across all your data sources. Guardium GDPR Accelerator provides prebuilt data security assessment tests designed to help you quickly evaluate personal data sources' security. Besides closing any newly discovered gaps, you should also take steps to harden access to the personal data sources themselves, so that unauthorized users cannot change their configuration or authorization settings.

Across Z, big-data and distributed environments, the Data Security Impact Assessment provided by Guardium GDPR Accelerator can help identify these risk areas and support audit-readiness for GDPR with deep IBM expertise.

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 then take action if you determine that suspicious behavior has occurred.

Guardium GDPR Accelerator also includes prebuilt policy rules and groups to help you begin performing continuous monitoring more quickly across your enterprise, including distributed, z/OS, cloud and big-data environments. The prebuilt policy rules are designed to shield personal data from unauthorized access and activities—including changes, removal, replication or deletion of records. Guardium GDPR Accelerator also processes reports (which you can select on a per-user, per-controllers or per-application basis) to document all attempts to access personal data. In addition, audit reports can aid in compliance reporting to auditors and may be used to assist with incident response by providing detailed activity reports.



Guardium GDPR Accelerator helps speed and consolidate GDPR compliance efforts with user-friendly analysis of data holdings, risks and access history.

Read the data sheet to learn how IBM Security Guardium Vulnerability Assessment can help you evaluate your data risk.

1 Article 33, "GDPR Notification of a personal data breach to the supervisory authority," *Intersoft Consulting*.

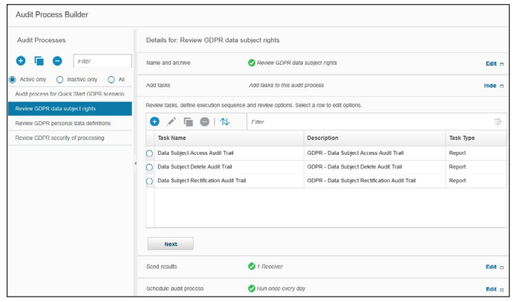
Preparing your organization for audit-readiness

In the event of a breach or an audit, and in fulfilling individuals' requests for data removal or modification under GDPR, your ability to provide an audit trail can't be only theoretical. You need to be able to produce reports that document and explain details of your data protection process. Guardium can help not only in the crucial stage of identifying personal data under your enterprise's control, but in answering key questions about access and control that GDPR mandates, supporting the move toward a more comprehensive data privacy and protection program across the enterprise.

Guardium GDPR Accelerator helps you to track and provide detailed audit trails on data subject access requests such as access to personal data, or data rectification, erasure or transfer. Information such as the identity of the application or database user, and relevant timestamps and SQL commands associated with the request are captured in 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 Guardium 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 improve time to value. The accelerator is built on the mature Guardium platform, which provides scalability from a simple, single-site network all the way to heterogeneous platforms spanning multiple data centers, and which helps organizations consolidate security information for use by IT personnel.

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



Guardium tools can help you easily trace the use and protection of personal data that your enterprise holds or processes.

Learn more about taking the pain out of regulatory compliance in this e-book from IBM.

Why IBM?

With decades of experience in building and securing networks, and protecting data across enterprises of all kinds, IBM offers an industry-leading mix of experience and capabilities directly relevant to data privacy protection. As a solution that integrates with IBM security and administration tools, including IBM QRadar® solutions, across enterprise data environments, Guardium can be the linchpin of your GDPR compliance strategy. Guardium helps implement best practices that enable organizations to know their data status, reduce risks, tighten policies, and monitor and audit for compliance and policy violations.

Guardium provides an integrated and scalable data security platform to help organizations 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 spectrum—from security to privacy to 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 GDPR and provide guidance to help you create and deploy comprehensive privacy policies, standards, guidelines and operating procedures. Just as auditing is a part of data privacy governance, an upfront assessment utilizing Guardium and other tools is key to readiness. As you prepare for GDPR, IBM services such as 24x7 data activity monitoring with global advanced threat intelligence and analytics can help optimize your level of control by establishing a data protection strategy that not only implements but also integrates resources.

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

In 2016,

more than 400 billion records were leaked—more than in the two previous years combined.[1]

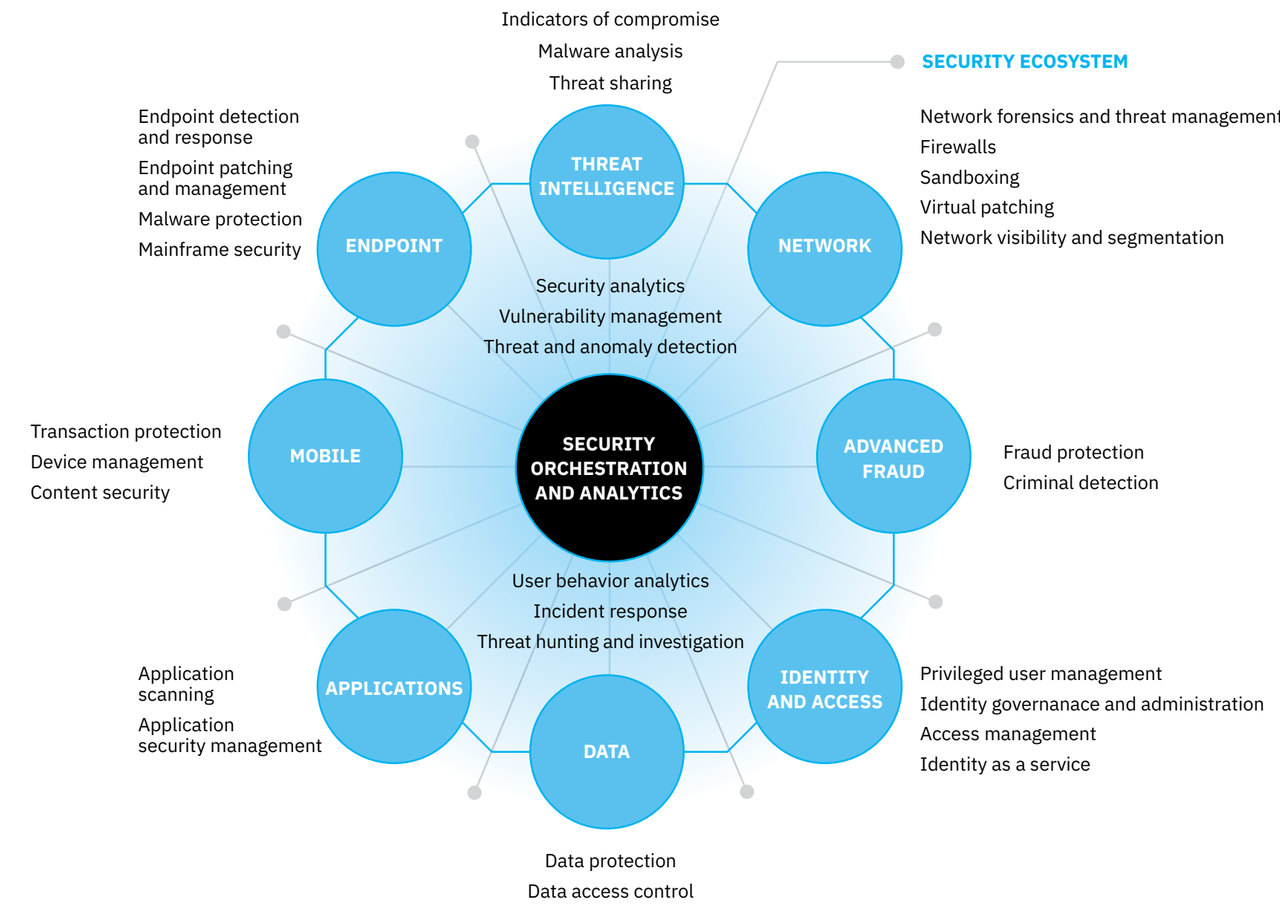
▸ Learn more about IBM cross-security GDPR solutions.

1 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, March 2017.

The IBM security immune system

The IBM Security portfolio creates an “immune system” that acts as an integrated framework of security capabilities that transmits and ingests vital security data to help gain visibility, understand and prioritize threats, and coordinate multiple layers of defense.

An integrated and intelligent security immune system



Learn more about the IBM security immune system.

For more information

To learn more about IBM Security Guardium 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 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
January 2018

WGS03123-USEN-00