IBM Security Thought Leadership White Paper

GDPR: It’s coming—and sooner than you think. Are you prepared?

The European Union’s General Data Protection Regulation has global impact

IBM Security

New law imposes significant safeguards on private information

There's no getting around it. Passed in May 2016, the European Union (EU) General Data Protection Regulation (GDPR) replaces the minimum standards of the Data Protection Directive, a 21-year-old system that allowed the 28 EU member states to set their own data privacy and security rules relating to the information of EU subjects. Under the earlier directive, the force and power of the laws varied across the continent. Not so after May 25, 2018.

Under GDPR, organizations are subject to new, uniform data protection requirements—or could potentially face hefty fines. So what factors played into GDPR's passage?

- **Changes in users and data.** The number, types and actions of users are constantly increasing. The same is true with data. The types and amount of information organizations collect and store is skyrocketing. Critical information should be protected, but often it's unknown where the data resides, who can access it, when they can access it or what happens once it's accessed.
- **Changes in data access and processing.** The cloud, social networking, smart cards, and an array of digital and mobile devices flung open the door to data security threats. Aware of this globally changed landscape, the EU enacted regulations that recognize that "the protection of natural persons in relation to the processing of personal data is a fundamental right."[1]

"Businesses operating in Europe or targeting European customers need to **get their act together and start preparing** *for the new regime."*

—The Register, *UK*[2]

Learn more about some of the changes you'll need to make for GDPR readiness.

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

2 John Leyden, "Europe's new privacy safeguards are finally approved, must invade EU nations by 2018," *The Register,* April 14, 2016.

Potential global and bottom line impacts of GDPR

While Europe has long been highly concerned with privacy, in other parts of the world, it can seem that concerns are low and oversight is lax. But GDPR makes such inattention foolhardy for any company collecting personal data on people located in the EU or for any company doing business in the EU. For these companies, GDPR compliance is mandatory and its reach is global. Regardless of where data is sent, processed or stored, GDPR requires that personal information be protected. Its underlying goal is to award greater control and transparency over one's own personal data.

To achieve this control, GDPR includes two key components:

- *Noncompliance:* Potential administrative fines up to EUR20 million (nearly USD22.3 million) or up to 4 percent of the total worldwide annual sales volume/revenue for the preceding financial year, whichever is higher.[1]
- *Notification:* Upon detecting a data breach, a company should notify the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[2]

In layman's terms, compliance with GDPR is enforced with the potential for substantial impact on the bottom line and a substantial demand on security and IT operations.

The personal information of* 157,000 customers *was hacked in an attack at a UK provider of telephone and broadband services.[3]

Learn more about steps you can take to prepare for GDPR requirements.

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

2 Article 85. "Regulation (EU) 2016/679 of the European Parliament and of the Council," April 27, 2016.

3 Sean Farrell, "Nearly 157,000 had data breached in TalkTalk cyber-attack," *The Guardian,* November 3, 2015.

Data breach incidents and costs on the rise

Only 72 hours to notify authorities of a detected data breach?

Reality smarts. According to research, the mean time to identify data breach incidents is 191 days, with the mean time to contain breaches an average 66 days.[1] And the longer it takes to detect and contain a breach, the costlier its resolution can become.

In 2016, enterprises faced an average data breach cost of USD3.26 million and suffered from data breaches that increased in size by an average of 1.8 percent.[1] Adding GDPR's potential penalty for any noncompliance that led to the breach, the impact can be staggering.

Risk—whether to personal, financial or other data—isn't going away. Every minute of every day, cybercriminals are devising, developing and introducing new and increasingly sophisticated threats. In fact, a global study found a 27.7 percent likelihood among the companies it studied that one or more data breaches involving 10,000 lost or stolen records would occur in the next 24 months.[1]

Yet many organizations remain unaware of the vulnerabilities that can affect their data. And as a result, they're also unaware of the consequences of a breach. Without understanding the magnitude of the threat, they never get around to identifying risks and remediating weak spots.[2] And that can be a costly misjudgment.

100 banks
in 30 countries lost USD1 billion in coordinated attacks over two years.[2]

Read more about the impact of a data breach in the recent Ponemon report.

1 "2017 Cost of Data Breach Study: Global Overview," Benchmark research sponsored by IBM, *Ponemon Institute,* June 2017.

2 "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.,* February 2016.

GDPR readiness: The time to act is now

We believe all companies need a data security strategy. Addressing the security vulnerabilities of data repositories, according to IBM® X-Force® research and development, should be part of every organization's basic security best practices.[1] That means implementing a comprehensive, layered plan that offers insight into how data is acquired, accessed, stored and protected. It also means integrating and utilizing the highest-quality knowledge and solutions. Investment of time and money in implementing strong security for the organization at large can also be a good investment toward GDPR readiness.

Governing bodies worldwide have enacted data protection regulations for diverse industries, including healthcare, corporate finance and consumer-related businesses. All these are driven by the need to protect sensitive data.[1]

Organizations that have allocated the budget, time and solutions to meet those existing regulations may be able to leverage the security programs they've put in place to prepare for GDPR.

Starting now, EU companies—along with all international companies operating in or doing business with individuals in EU member nations—have to understand the need for action. Organizations dealing with personal data—even simply the data related to their own employees—are affected by GDPR.

96,000 security vulnerabilities *worldwide have been documented in the IBM X-Force database.*[1]

Learn more about GDPR readiness and best practices in the monthly blog series at SecurityIntelligence.com.

1 "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.,* February 2016.

A framework for GDPR readiness

GDPR compliance is complex, because the regulation itself is complex. It outlines obligations for data holders that can affect all parts of a business, from data collection to customer communication practices. However, GDPR is also open-ended: it doesn't tell you in detail how to meet those obligations, or that any given technological approach will suffice.

That's why IBM has developed a straightforward approach to help simplify the ways you think about conformance. The IBM GDPR framework offers an actionable five-phase approach to GDPR readiness, which recognizes that readiness is a continuum: every organization will have a unique place on the journey to readiness.

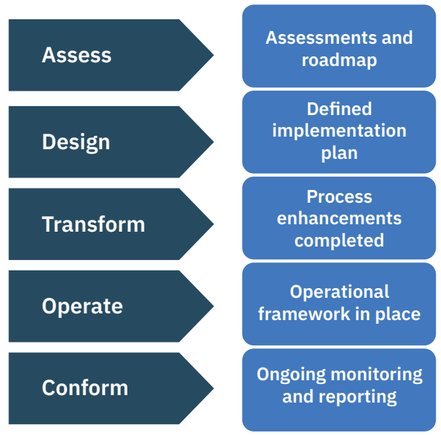
In Phase 1, you **assess your situation**. You figure out which of the data you collect and store is covered by GDPR regulations, and then you plot a course to discover it.

Phase 2 is where you **design your approach**. You need to come up with a solid plan for data collection, use and storage. And you need to develop an architecture and strategy that will balance risks and business objectives.

Your goal in Phase 3 is to **transform your practices**, understanding that the data you deem valuable to your organization is equally valuable to the people it represents. This is where you need to develop a sustainable privacy compliance program, implement security and governance controls (TOMs — Technical and Organizational Measures) and potentially appoint a Data Protection Officer.

By the time you get to Phase 4, you're ready to **operate your program**. Now you're continually inspecting your data, monitoring personal data access, testing your security, using privacy and security by design principles and purging unneeded data.

And Phase 5 — the final phase — is where you're ready to **conform with the necessary GDPR requirements**. Now you're fulfilling data subject requests for access, correction, erasure and transfer. You're also prepared for audits with documentation of your activities and ready to inform regulators and data subjects in the event of a data breach.



Learn more about how to get started.

GDPR readiness through the IBM Security lens

IBM Security offers further guidance on the five-phase IBM GPDR approach by outlining key objectives and activities that every enterprise should consider in achieving readiness.

IBM Security GDPR framework: Key activities to address GDPR

	Assess	Design	Transform	Operate	Conform
Privacy requirements	**PREPARE:** • Conduct GDPR assessments, assess and document GDPR-related policies • Assess data subject rights to consent, access, correct, delete, and transfer personal data **DISCOVER:** • Discover and classify personal data assets and affected systems • Identify access risks, supporting Privacy by Design	**ROADMAP:** • Create GDPR remediation and implementation plan **PRIVACY BY DESIGN:** • Design policies, business processes and supporting technologies • Create GDPR reference architecture • Evaluate controller or processor governance	**TRANSFORM PROCESSES:** • Implement and execute policies, processes and technologies • Automate data subject access requests	**MANAGE GDPR PROGRAM:** • Manage GDPR data governance practices such as information lifecycle governance • Manage GDPR enterprise conformance programs such as data use, consent activities, data subject requests **RUN SERVICES:** • Monitor personal data access • Govern roles and identities • Develop GDPR metrics and reporting schemas	**DEMONSTRATE:** • Record personal data access audit trail including data subject rights to access, modify, delete, transfer data • Run data processor or controller governance including providing processor guidance, track data processing activities, provide audit trail, prepare for data subject access requests • Document and manage compliance program: ongoing monitoring, assessment, evaluation and reporting of GDPR activities **RESPOND:** • Respond to and manage breaches
	PREPARE: • Assess security current state, identify gaps, benchmark maturity, establish conformance roadmaps • Identify vulnerabilities, supporting Security by Design **DISCOVER:** • Discover and classify personal data assets and affected systems to design security controls	**ROADMAP:** • Create security remediation and implementation plan **SECURITY BY DESIGN:** • Create security reference architecture • Design Technical and Organizational Measures (TOMs) appropriate to risk (such as encryption, pseudonimization, access control, monitoring)	**PROTECT:** • Implement privacy-enhancing controls (for example, encryption, tokenization, dynamic masking) • Implement security controls; mitigate access risks and security vulnerabilities	**MANAGE SECURITY PROGRAM:** • Manage and implement security program practices such as risk assessment, roles and responsibilities, program effectiveness **RUN SERVICES:** • Monitor security operations and intelligence: monitor, detect, respond to and mitigate threats • Govern data incident response and forensics practices	**DEMONSTRATE:** • Demonstrate technical and organizational measures to ensure security appropriate to processing risk • Document security program: ongoing monitoring, assessment, evaluation and reporting of security controls and activities **RESPOND:** • Respond to and manage breaches

Learn how to design your GDPR plan.

IBM Security

Three points on the GDPR readiness journey

Every organization must face GDPR requirements regarding both security and privacy from its own unique position—but many organizations find themselves at one of three points on the GDPR readiness journey:

"I've heard of GDPR, but I'm not sure how it will impact my organization or where I should start."

IBM can provide a starting point for those organizations that are just beginning the GDPR journey with a GDPR readiness assessment and a roadmap for moving forward.

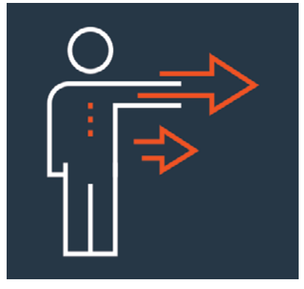
"I've started on my GDPR readiness plans, but I'm having a hard time getting to the next stage."

IBM offers a comprehensive set of data discovery and data mapping tools to help you pinpoint where your personal data is located, track its movement across business processes, and help find, identify and mitigate data layer security and access risks.

"I've developed my GDPR readiness and response plans, but I need help implementing them."

If you're ready to run your GDPR program, IBM can help you develop and execute TOMs (Technical and Organizational Measures), develop or enhance new processes and procedures, manage risks, automate security operations, design processor audits, and help identify and respond to data breaches.

See for yourself how the IBM Security GDPR framework can help your organization prepare for and meet GDPR requirements for both privacy and security. You can begin by exploring the assessment phase if you're just starting out, or choose the area that best reflects whatever your current needs may be.



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

Help prepare for GDPR with IBM Security solutions

GDPR is a game-changer to organizations worldwide. At minimum, the regulation demands:

- **Data protection accountability.** Companies must demonstrate that considerable security measures are in place to protect users' private data. The ante is upped for companies delving in high-risk areas.
- **Data subjects' right to access, rectification, erasure and portability.** Organizations need to validate the individual's identity, swiftly produce personal data it processes, and correct, erase or transfer data on request.
- **Data breach notification.** A personal data breach "leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" must be reported within 72 hours of discovery.[1]

To help with your GDPR readiness, IBM recommends:

- Assess your current data privacy stature with GDPR readiness assessment from IBM.
- Know your users and what they can access. That's IBM Security Identity Governance and Intelligence.
- Know where your critical data is and who's touching it. That's IBM Security Guardium®.
- Find, identify and mitigate data layer security and access risks with IBM Data Risk Manager and Critical data protection program from IBM (CDPP).
- Know how to use this information for a view of attacks. That's IBM QRadar® Security Intelligence Platform.
- Know how you've been breached and how to mitigate risk. That's IBM Resilient® Incident Response Platform.
- Leverage prebuilt and ready-to-deploy tools for GDPR readiness. That's IBM Security Guardium GDPR Accelerator.

"As the dusty corners of our online identities are opened to the physical world, we must hold those we trust... more accountable."

—Ponemon Institute[2]

Assess your progress now with the interactive Personalized Guide to GDPR Readiness.

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

2 "2016 Cost of Data Breach Study: Global Analysis," Benchmark research sponsored by IBM, *Ponemon Institute,* June 2016.

IBM Security

IBM

Control user access points and automatically uncover potential compliance risks

IBM Security Identity Governance and Intelligence

IBM Security Identity Governance and Intelligence delivers a single foundation to help organizations understand and control user access and risks. It connects compliance auditors, IT staff, and business perspectives for a clear picture of identities and their access.

- Control access and help ensure user access audit readiness
- Centralize and automate tasks for administering user identities, credentials, accounts and access permissions
- Facilitate communication between auditors and IT staff and determine segregation-of-duties violations

IBM Data Risk Manager

To be ready for GDPR, organizations must be able to find, identify and mitigate data layer security and access risks. IBM Data Risk Manager provides a business-consumable data risk control center, helping to uncover, analyze and visualize data-related business risks so they can take action to protect their business.

IBM Security Guardium

IBM Security Guardium offers automated analysis to quickly uncover internal and external risks to data. It supports the entire data protection journey with the same infrastructure and approach. With Guardium, companies can:

- Discover and classify sensitive data and automatically uncover potential compliance risks
- Know who is accessing data, spot anomalies and stop data loss with data activity monitoring
- Scan and analyze audited data to detect symptoms that a database attack is underway—from the inside or outside
- Safeguard against liability with audit capabilities for data at rest and in motion
- Locate GDPR-governed personal data and better understand the scope of GDPR with Guardium GDPR Accelerator.

60% of all attacks

in 2015 were caused by insiders—up from 55% in 2014.[1]

1 "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *IBM X-Force Research: 2016 Cyber Security Intelligence Index,* April 2016.

IBM Security

Identify high-risk scenarios before they mature. Act rapidly when they do.

IBM QRadar Security Intelligence Platform

The QRadar platform's IBM Sense Analytics™ Engine detects advanced threats, while providing ease of use and low total cost of ownership.[1] The platform enables companies to:

- Collect and analyze identity data and vulnerabilities, as well as log events, network traffic flows and network packets through a single architecture
- Achieve automatic incident response and regulatory readiness with data collection, correlation and reporting
- Identify potential high-risk threats, attacks and security breaches via real-time correlation using Sense Analytics
- Prioritize incidents requiring urgent attention among billions of daily data points received

IBM Resilient Incident Response Platform

As a leading incident response platform (IRP), Resilient helps organizations thrive in the face of cyber attacks or business crisis, and empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. Resilient arms organizations to take actions required under GDPR-related breach-notification guidelines and incorporates them into organizations' incident response plans. This prescriptive guidance speeds response and provides a record of action. Resilient offers:

- GDPR Preparatory Guide: An interactive tool that prescribes step-by-step how to prepare for GDPR.
- GDPR Simulation: This simulator within the Resilient IRP is where organizations rehearse the actions they will have to take in the future in the event of a GDPR breach.
- GDPR-Enhanced Privacy Module: Resilient clients will have access to a database of GDPR-related guidelines and regulations embedded in their IRP.

600 million

records were leaked worldwide in 2015, according to public breach disclosures.[2]

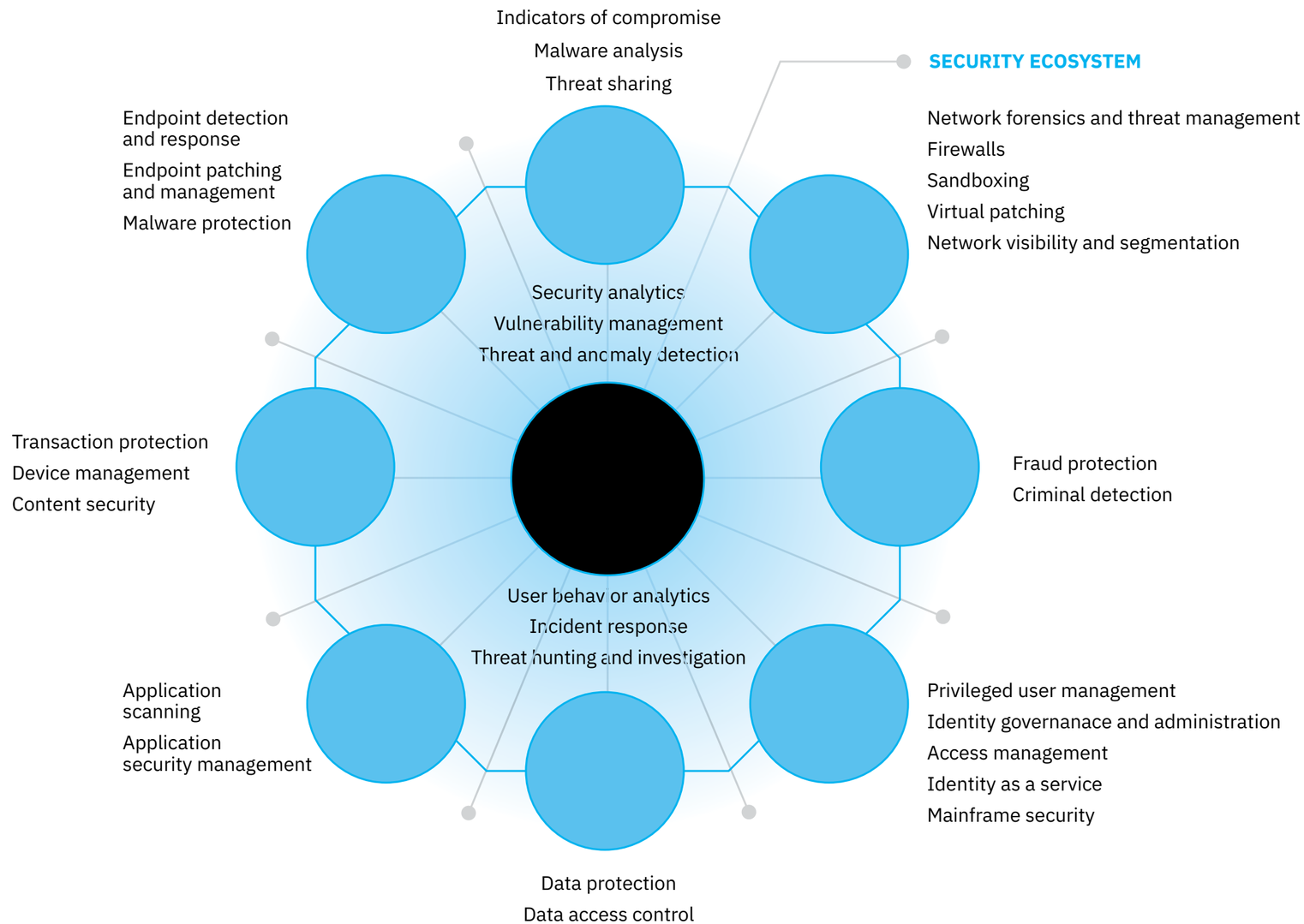
1 "QRadar Study on Sense Analytics," *Ponemon Institute,* February 2017.

2 "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.,* February 2016.

IBM Security

An integrated and intelligent 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.



Learn more about the IBM security immune system.

IBM Security IBM

Leverage global IBM experience in privacy consulting services

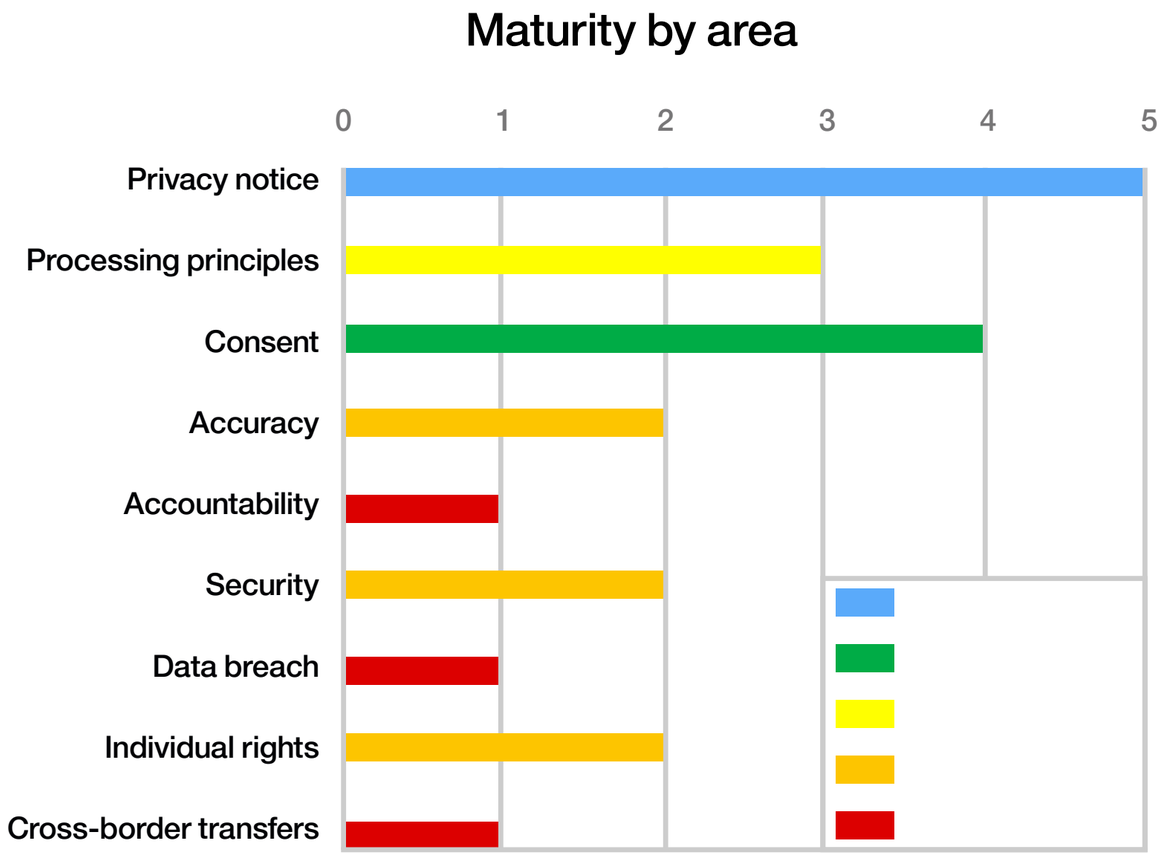
IBM Privacy Consulting Practice

IBM Privacy Consulting Practice helps organizations rapidly create and deploy comprehensive privacy policies, standards, guidelines and operating procedures designed to align with best practices and help better manage their regulatory obligations. IBM provides a holistic approach with the Total Privacy Management Framework for building a bridge between line-of-business, legal, IT and management structures. It enables clients to have a more efficient privacy program to help better prepare for local and global regulatory requirements.

IBM GDPR Assessment

As a foundational offering for an organization's GDPR activities, IBM Data Privacy Consulting Services can help identify areas of the business that will be impacted by GDPR requirements and obligations. Through a customized end-to-end GDPR Readiness Assessment, IBM can evaluate the organization's current practices against the new GDPR requirements with a focus on process development, best practices and organizational need. As part of the service, IBM provides a GDPR maturity model and gap/remediation plan to assist in developing and implementing a roadmap toward readiness. GDPR Readiness Assessment can also help you select IBM services and products to help you prepare for GDPR.

Learn more about the GDPR readiness assessment from IBM.



A maturity model and gap/remediation plan assists with developing and implementing a GDPR readiness roadmap.

Case study: Italian insurance company ensured appropriate user access

With enormous stores of data, one of Europe's largest insurance, banking and investment management companies faced a dilemma. It had an identity management solution for provisioning and de-provisioning in place, but the custom-built tool for access and recertification wasn't keeping pace. It lacked scalability for new applications and users, and few employees understood how to use it.

Charged with privacy and internal audit requirements—and compliance to the Italian 196 Privacy Law on data—the company sought a solution with a strong access and identity certification process.

After researching potential remedies, the company deployed an integrated IBM Security Identity Governance and Intelligence solution for its 75,000 users. This solution worked with existing SAP and non-SAP applications and the mainframe to meet the company's requirements—providing significant time, cost, compliance and security benefits.

By connecting compliance, business and IT points of view, and simplifying processes for certifying user access and roles, IBM Security Identity Governance and Intelligence was able to help with audit readiness. Post deployment review done by IBM revealed that IBM Security Identity Governance and Intelligence helped reduce the client's policy violations and risk vulnerability. It helps this company prepare for Italy's 196 Privacy Law and the 262 Law (equivalent to the US Sarbanes-Oxley Act) on corporate governance. Importantly, the IBM solution helps prepare companies for GDPR by providing visibility and user access control across the full user lifecycle.

Insurance company benefits with IBM:

- *Enhanced process controls for risk reduction and access compliance*
- *Improved ability to meet mandated privacy requirements*

Read the IBM white paper to learn how identity governance can help ensure appropriate user access.

IBM Security IBM

Case study: Bank locks down employee access to customer data

When a regional bank failed an audit due to lax controls over its customers' sensitive information, it knew it needed stronger capabilities for limiting access and preventing data breaches. It needed to control—and put an end to—practices by which IT administrators shared access to customer applications, and each line of business used its own spreadsheets to track information. Inability to properly control access had even resulted in one instance where an ex-employee accessed and extracted customer data.

To store login credentials and govern administrators' access to sensitive data, the bank deployed IBM Security Privileged Identity Manager. Under this system, when an administrator needs data access, an agent built into the solution checks out credentials and automatically logs the approved user in to the application without ever disclosing the password. After the session, the password is changed.

The bank also deployed Guardium to monitor in real time privileged users' activities accessing data—and to validate that access using a shared ID is within the scope of users' defined privileges. If a violation of data access policy is detected, Guardium sends alerts to IBM QRadar SIEM, which integrates security and event data for cross-enterprise anomaly detection, incident forensics, incident response and vulnerability management.

Bank benefits with IBM:

- *Streamlined control and tracking of shared ID access*
- *Reduced operational costs*
- *Help preventing damaging data breaches*
- *Simplified audits with consolidated audit records*

Learn more about IBM Security Privileged Identity Manager and Guardium on the web.

IBM Security IBM

Why IBM?

IBM helps organizations protect their business-critical data and mainframe infrastructures—and the people who use them—from threats and breaches. The layered, integrated IBM approach to security solutions addresses mainframe-specific concerns as well as overarching security issues such as identity and access management, security intelligence and data security across the enterprise.

The broad IBM portfolio of security solutions provides a comprehensive view of all network user activity—including potentially abnormal behavior—as well as potential system vulnerabilities, identifying threats and alerting administrators so they can take necessary action to help prevent or remediate damage.

Deploying IBM Security solutions now gives companies a start on the path to GDPR readiness when it goes into effect in 2018. IBM Security solutions also enable a best-practice approach that builds a solid foundation for the organization's overarching security needs, helping protect both customer and enterprise data from theft, fraud or compromise.

For more information

To learn more about how IBM Security solutions can help you prepare for GDPR as well as meet your overall enterprise security needs, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

Watch the IBM video about protecting the digital world from cyber attacks.

IBM Security

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

© Copyright IBM Corporation 2017

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2017

IBM, the IBM logo, ibm.com, Guardium, QRadar, Sense Analytics, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml
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.

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. Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.

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.

WGW03247-USEN-05

IBM Security

IBM