



IBM's Journey to GDPR Readiness



GDPR

EU General Data Protection Regulation

IBM's Journey to GDPR Readiness

“At IBM, we have a deep rooted understanding that privacy is foundational to trust. We are approaching the GDPR in the same spirit, both internally and with respect to our client offerings. IBM’s legal and data privacy teams have been reviewing and assessing the new [EU General Data Protection Regulation](#) since its early draft stages, and as IBM’s Chief Privacy Officer, I recently published a statement that outlines [IBM's commitment to GDPR readiness](#).

Teams across IBM are adapting our internal processes and commercial offerings to prepare for when the GDPR comes into effect on May 25, 2018. These same experienced professionals are available to support you at each stage of your own GDPR readiness journey. And what better customer reference for IBM’s capabilities on GDPR, than IBM itself?”

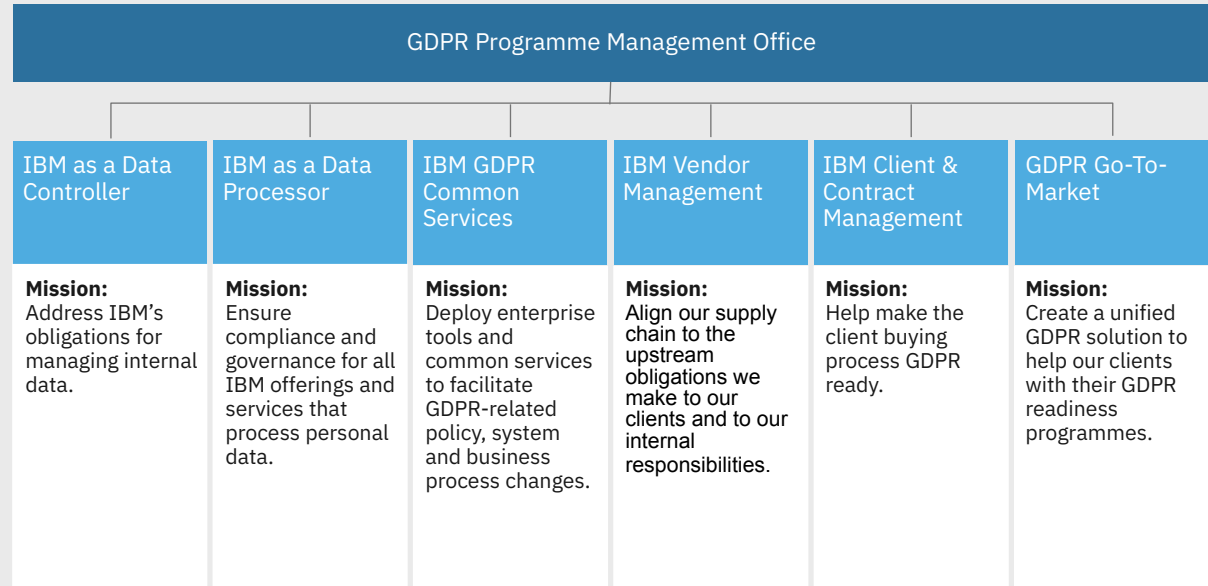
- Cristina Cabella
IBM Chief Privacy Officer
ibm.com/privacy
ibm.com/gdpr



Our GDPR Readiness Programme

IBM has established a global readiness programme tasked with identifying the key impacts of the GDPR across IBM's business and preparing IBM's internal processes and commercial offerings for compliance with the GDPR.

The programme is organised into several work streams, staffed with IBM's top data privacy and security professionals. Focal points in each Business Unit are responsible for implementing the GDPR-related policy, system and business process changes mandated by the various key work streams.

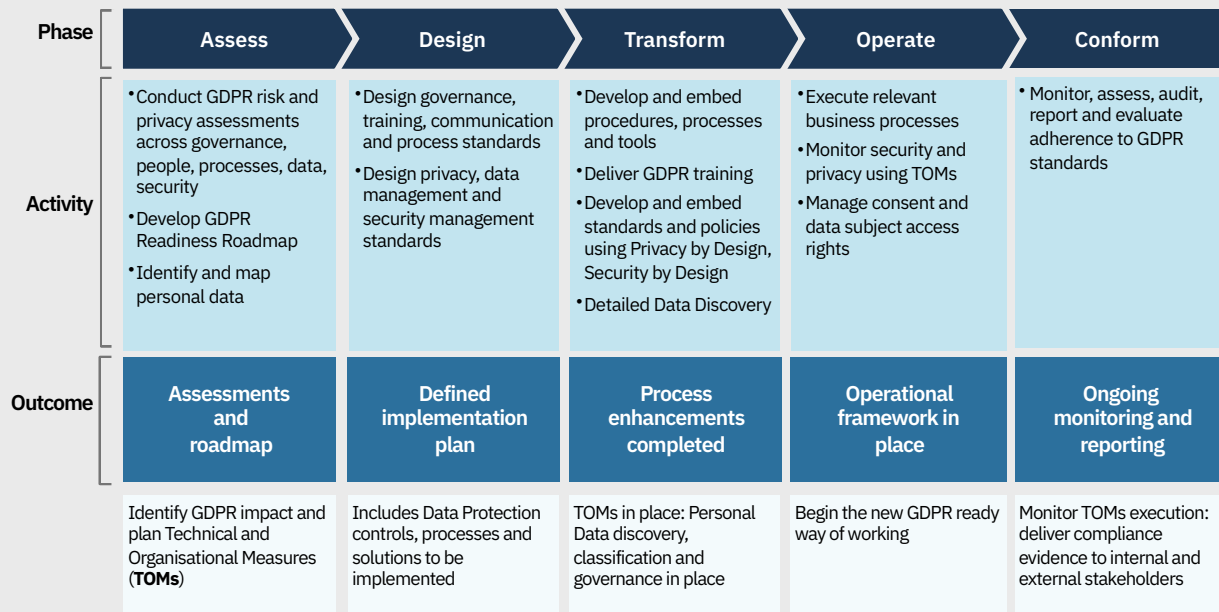


The IBM GDPR Framework

Our internal GDPR readiness activities are aligned with a global framework derived from lessons learned on our many security and privacy client engagements.

This framework takes a holistic approach that spans people, processes and technology. It translates GDPR obligations into the concrete actions and outcomes that are needed to progress towards GDPR readiness.

This close interlock helps to ensure that the best practices, solutions and services that IBM uses internally are the same as those we offer our clients.



Visit ibm.com/gdpr and download our white paper [IBM pathways for GDPR readiness](#) for more details on the IBM GDPR Framework and guidance on addressing your own organisation's GDPR readiness challenges.

Assess

IBM is conducting global privacy assessments on both our internal systems and our client offerings, and is incorporating Technical and Organisational Measures into new and existing contracts to cover the GDPR's requirements.

IBM's long standing services in data privacy and security bring dedicated and multi-disciplinary expertise to address the challenges of legal and regulatory compliance, project management and operational risk controls across more than 70 jurisdictions.

One key challenge for us was to standardise our taxonomy of data across all IBM Business Units. This is being achieved with the help of our advanced cognitive analytics solutions.

With clients and for ourselves, these assessment outputs include PIA (Privacy Impact Assessments), gap analysis, data mapping and compliance handbooks.

Projects for Fortune
750 Companies

60+ countries

100 years of collective
experience



IBM's long-standing Data Privacy Consulting Service was extended with the acquisition of Promontory Financial Group in 2016.

Promontory's team blends experience as former regulators, in-house compliance managers, and global privacy consultants and is providing IBM with unique perspectives and expertise on GDPR readiness, data-mapping, and compliance strategies.

Visit www.promontory.com for more details on Promontory's expertise and services.

Design

IBM has deployed a number of corporate wide common services to accelerate and assist in programme execution across all of our business units. These include Programme Governance, Risk Management, Data Subject Rights Management and Processor/Controller Governance solutions.

We have developed range of internal communication and training initiatives to ensure employees are made aware of and enabled on GDPR duties, obligations, and proper data use. Additional self-service materials include approved content libraries, Q&A forums and knowledge base resources.

IBM's GDPR solution provides clients with the same capabilities that we have developed internally to help accelerate their own journey towards GDPR readiness.

The image shows a screenshot of a web application interface for a GDPR glossary. The top section is titled "personal data" and includes the text "A term from the GDPR Regulation". Below this, there are sections for "PARENT CATEGORY" (GDPR Glossary), "REFERENCING CATEGORIES (3)" (three instances of GDPR Glossary > CHAF), and "STATUS" (Standard). A "General Information" section is partially visible. A navigation bar at the bottom includes "Glossary", "Information Assets" (highlighted with a green box), "Labels", "Queries", "Collections", and "Data Integration". Below the navigation bar, a search bar contains "BI". The main content area is divided into "Browse Hierarchies" and "Manage".

personal data
A term from the GDPR Regulation

PARENT CATEGORY: [GDPR Glossary](#)

REFERENCING CATEGORIES (3):
GDPR Glossary > CHAF
GDPR Glossary > CHAF
GDPR Glossary > CHAF

STATUS: Standard

» General Information

» Associated Terms (3)

IS A TYPE OF (3): [Article 01 Subject-matter and](#)

Navigation: Glossary | **Information Assets** | Labels | Queries | Collections | Data Integration

Search: BI

Browse Hierarchies

- GDPR Data Processing
- Implemented Data Resources
- Logical Data Models
- StoredIQ Document Services
- Physical Data Models
- XML Schema Definitions
- Data Classes
- Master Data Models
- Applications
- Stored Procedure Definitions
- Business Intelligence

Manage

- Create Extension Mapping Document...
- Create Data Class...
- Import Extension Mapping Documents...
- Import Extended Data Sources...
- Import Asset Values...
- Monitor Lineage Tasks

Sticky Notes:

- LEGAL CONTROLLER IDENTITY
- LEGAL PROCESSOR IDENTITY
- DPO OF LEGAL ENTITY
- LEGAL ENTITY REGISTER.
- CONTACT DETAILS OF EACH
- GDPR
- RISK ASSESSMENT FOR OPA SUBJECTS
- RISK MODELS
- RISK MODEL RESULTS
- THRESHOLD MATRIX
- DSAR
- DSAR PROCESS
- AUDIT OF SECURITY PROFILES
- CONDUITANCE AUDIT LOGGING

Transform

We are transforming all our business units globally to ensure consistent adoption of GDPR capabilities across IBM.

GDPR Common Services are being implemented in three main phases.

Phase 1: Data & Risk Classification High Level Assessment

Regulatory Response
Dashboard

Privacy Risk Assessments

Data Maps

Data Sources Discovery

Data Catalogues

Phase 2: Detailed Assessment & Priority Data Remediation

Detailed Data Discovery

Initial Record of Processing

Priority Data Remediation

Cognitive Analytics
Solutions

Phase 3: Operationalise GDPR Capabilities

Contract Management
Customer Portal

Vendor Repository &
Workflow

Compliance Validation

Consent Management

Data Subject Access
Requests

Incident Response


Data Remediation

Operate

Key GDPR capabilities will be fully operational before the GDPR comes into effect in May 2018. At this point, IBM's new GDPR way of working should become standard operating practice for interactions with our clients and their data.

Features and services integrated directly into our offerings will help protect privacy and meet our GDPR-related obligations, such as the ability for data subjects to manage their consent preferences (“privacy by design”) and submit data subject access requests (DSARs).

Incident Management and meeting the 72-hour breach reporting window is a key operational challenge for all organisations. IBM will use our Computer Security Incident Response Team (CSIRT) to address this challenge.



Compliance Monitoring

Known databases	Unconfigured databases
24	21

General Data Protection Regulation (GDPR)

- Scanning for sensitive data
Last scan: 2017-05-28 10:31:02
Matches found: 698
- Monitoring enabled
Traffic last captured: 2017-06-01 09:17:07
- Sensitive objects
- Applications (Client IP)
- Privileged users

Updated: 2017-05-24 18:22:20 [View details](#)

Payment Card Industry

- Scanning for sensitive data
Last scan: None
Matches found: None
- Monitoring enabled
Traffic last captured: None
- Sensitive objects
- Applications
- Privileged users

Updated: 2017-05-24 18:22:20 [View details](#)

Category	CC	C	IC
Organization Level	Company Confidential	Confidential	Internally Controlled
Ma Marketing and Sales	Actuary Data Company Confidential 1 16	Personal Affiliation Confidential 0 61	
RP Redstreak PNW		Personal Affiliation Confidential 0 61	Pseudonymization Metadata Internally Controlled 0 63
RD RW Divestiture	Actuary Data Company Confidential 0 1	Personal Social Confidential 0 31	Pseudonymization Metadata Internally Controlled 0 8

Conform

IBM draws on its extensive governance, consulting and practice knowledge with a wide range of global privacy and security regulations to help ensure compliance of our business operations worldwide.

This includes monitoring of Technical and Organisational Measures, security and privacy assessments, auditing and evaluating ongoing conformance to the GDPR and the provision of evidence of compliance to both internal and external stakeholders. IBM makes these same services available to clients.

General Data Protection Regulation (GDPR)
Updated: 2017-06-01 19:17:00

Summary Databases **Policies** Reports

Policies associated with this compliance type: 2

Discovery scenario: Quick Start GDPR scenario

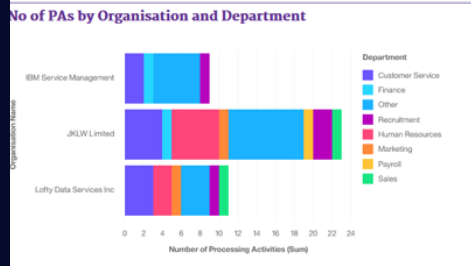
Security policy: Quick Start GDPR [Reset to default](#)

- Failed Login - GDPR Personal Data - Log Violation
- Failed Login - GDPR Personal Data - Alert if repeated
- SQL Error - GDPR Personal Data - Log
- SQL Error - GDPR Personal Data - Alert on Risk Indicative errors
- Select Commands, non App User, GDPR Personal Data Sensitive Objects - Log Full Details
- DDL Commands, GDPR Personal Data Sensitive Objects - Log Full Details
- DML Commands, GDPR Personal Data Sensitive Objects - Log Full Details
- Delete Commands, GDPR Personal Data Sensitive Objects - Log Full Details
- Update/Modify Commands, GDPR Personal Data Sensitive Objects - Log Full Details
- GDPR Personal Data Unauthorized User - Log Full Details
- GDPR Personal Data Admin User - Log Full Details
- GDPR Personal Data Authorized User - Log Full Details
- GDPR Personal Data Unauthorized User, GDPR Personal Data Sensitive Objects - Log Violation
- GDPR Personal Data Admin User, GDPR Personal Data Sensitive Objects - Log Violation
- GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects - Log Violation
- Grant Commands, GDPR Personal Sensitive Data Objects - Log INFO
- REVOKE Commands, GDPR Personal Data Sensitive Objects - Log INFO
- DDL Commands, GDPR Personal Data Sensitive Objects - Log INFO
- DML Commands, GDPR Personal Data Sensitive Objects - Log INFO
- Unauthorized Clients access to Personal Data Sensitive Objects - Alert
- Unauthorized Users access to Personal Data Sensitive Objects - Alert
- Credit Card Numbers, Unauthorized Users - Log Violation
- Unauthorized Users, Phone Numbers - Log Violation

[Go to discover sensitive data](#) [Go to policy builder](#)

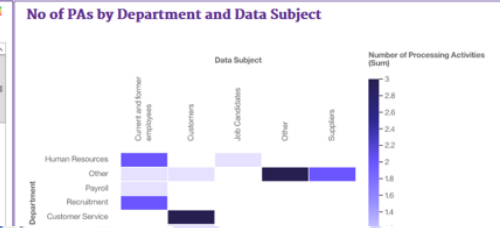


By Organisation By Controller By Processor By Data Subject **By Department** By Location PA Details



No of PAs by Department and Organisation Role

Number of Processing Activities		Customer Service	Finance	Human Res
IBM Service Management	Data Process Operator	2	1	(no value)
	Data Processor	1	1	(no value)
	Data Storage Operator	1	1	(no value)
	Joint Controller	1	(no value)	(no value)
	Recipient Organisation	1	(no value)	(no value)
	Summary	6	3	(no value)
	Data Controller	4	1	(no value)



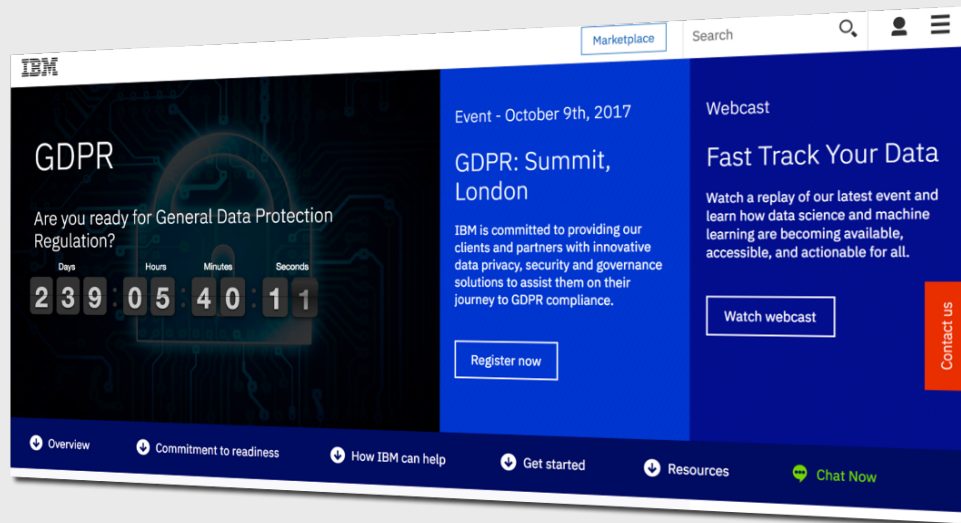
Are you ready?

The work that IBM is doing internally to prepare for the GDPR reinforces the controls already in place that limit access to our clients' personal data and will ensure that we continue to handle our clients' most valuable assets in a compliant manner at all times.

The GDPR represents a unique opportunity to help strengthen your own privacy compliance posture and preserve the trust of your customers, while reducing your exposure to risk, and creating real competitive advantage.

[Connect with our GDPR professionals](#) or join us for one of our regular online or in-person briefings to learn more about how IBM is preparing for the GDPR and how we can support you on your own journey to GDPR readiness.

Visit ibm.com/gdpr for more details.



The screenshot shows the IBM website for the GDPR Summit in London. The main heading is "GDPR" with the sub-heading "Are you ready for General Data Protection Regulation?". A digital clock displays the time as 239:05:40:11, with labels for Days, Hours, Minutes, and Seconds. To the right, it says "Event - October 9th, 2017" and "GDPR: Summit, London". Below this is a "Register now" button. Further right is a "Webcast" section titled "Fast Track Your Data" with a "Watch webcast" button. The footer contains navigation links: Overview, Commitment to readiness, How IBM can help, Get started, Resources, and Chat Now. A "Contact us" button is visible on the right side.



© Copyright IBM Corporation 2017

IBM Corporation
New Orchard Road
Armonk, NY 10504

October 2017

IBM, the IBM logo, and ibm.com 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 NONINFRINGEMENT. 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.