PERSPECTIVE

# GDPR - An industry and geography agnostic regulation

## Abstract

As the deadline to comply with the General Data Protection Regulation (GDPR) draws near, many organizations are unaware of what this regulation means and how it will impact their operations, processes, and growth in the European Union (EU). This perspective provides an overview into the drivers and features of GDPR, outlines the cost of non-compliance and explains what organizations can do to ensure they are GDPR-ready before time runs out.

## Overview of GDPR

As the world embraces new technologies, it must also accept and prepare for complex challenges, most notably, personal data theft and cyber attacks. In 2016, the European Commission released a new regulation on data protection that overrode the existing national laws of the 28 EU member states and repealed Directive 95/46/EC. This new regulation supports what is known as the General Data Protection Regulation (GDPR) that aims to fortify data protection for EU residents whose data resides anywhere in the world.

There is a pressing need for organizations to assess their current environment and implement the revised data framework if they aim to be GDPR-compliant before 25th May 2018.

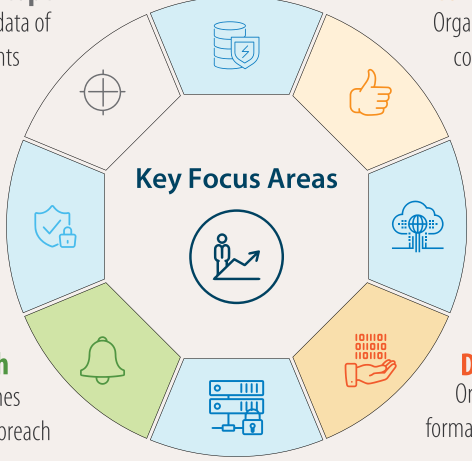
Directive 95/46/EC comprised a set of guidelines and rules for all EU nations that could be implemented and administered in different ways according to each member country. Alternatively, GDPR seeks to homogenize the protection of this fundamental right by leveraging a single supervisory authority and ensuring uniform implementation across all EU nations.

GDPR ensures that organizations that collect, process, transfer, store, and dispose personal data of EU residents do so in a manner that does not infringe upon the rights of these individuals. It also simplifies the regulatory environment of digital businesses – a critical imperative for growth.

It introduces several key changes that will impact organizations across the globe. For instance, any EU-based organization that processes personal data of EU citizens must comply with this regulation, even if the actual data processing is done outside the EU. The regulation also extends to organizations outside the EU that offer goods and services or process personal data of EU citizens by monitoring their behavior.

GDPR mandates customer consent for the lawful processing of personal data. This means that organizations must ensure that consent from data subjects is explicit, freely given, etc. Subjects can provide consent through a statement or a clear affirmative action and are free to withdraw their consent at will and at any time. When processing personal data of children, consent can only be given by the person who holds parental responsibility for the child.

## Key Focus Areas



### Data Protection Officer

Every member state needs to have an appointed supervisory authority who will interact with the DPO (Data protection officer) at Controller / Processor level

### Extended Territorial Scope

Non-EU organizations which process personal data of EU residents or provide services to EU residents will need to adhere to the new regulation

### Consent and Profiling

Organizations must inform data subjects of the existence and consequences of any profiling activities which they carry out and obtain explicit consent from data subjects

### Privacy Impact Assessment

Organizations processing the data will be required to conduct privacy impact assessments

### Erasure / Rectification of Data

Data subjects have the right to ask for rectification or right to be forgotten

### Notification of Breach

Organizations need to report data breaches within 72 hours of awareness of the breach

### Data Portability

Organizations should develop interoperable formats that enable data portability

### Privacy by Design

Data protection principles should be adopted into product / project design process

*Fig 1: Key focus areas of GDPR*

**Extended territorial scope –** GDPR must be followed by non-EU organizations that process personal data of EU residents.

**Data portability –** GDPR insists that data subjects have: 1) the right to receive any personal data that concerns them in a machine-readable format, and 2) the right to transmit this data to any other controller.

**Privacy impact assessment –** In cases when data processing can threaten the right / freedom of the data subject, GDPR instructs organizations to conduct privacy impact assessments.

**Notification of breach –** GDPR mandates that data controllers and processors must notify their local data protection authority about personal data breaches within 72 hours of awareness of the breach.

**Privacy by design –** According to GDPR, data controllers must integrate data protection and privacy controls for each project at the design phase.

**Consent and Profiling –** GDPR states that an organization must inform data subjects of the existence and consequences of any profiling activities carried out by them and obtain explicit consent from each data subject.

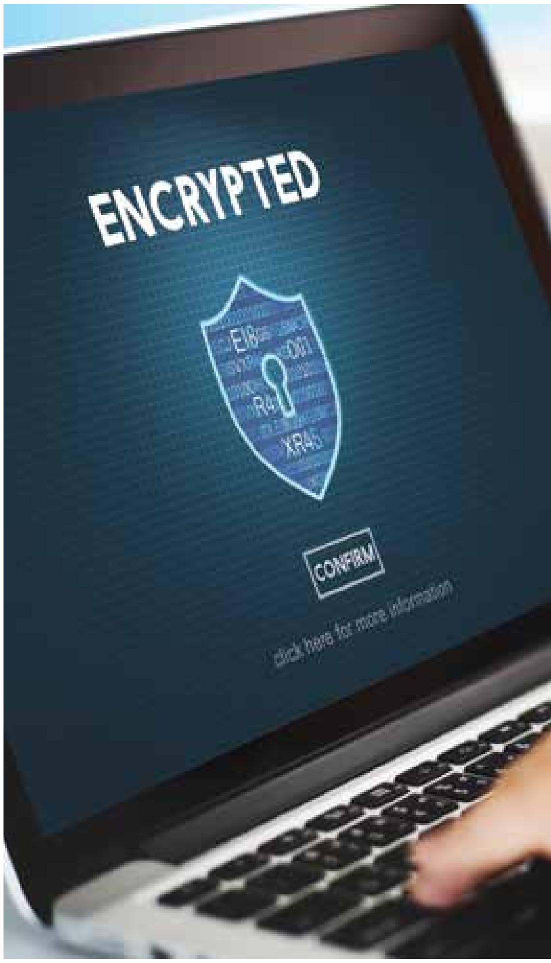
**Erasure / rectification of data –** GDPR ensures the data subject's right to rectify, erase, and restrict the processing of personal data.

**Data protection officer –** GDPR states that every member state must have an appointed data protection officer (DPO) to interact with all the stakeholders including controllers, processors, and the supervisory authority.

**IMPLICATIONS OF NON-COMPLIANCE**

In case of non-compliance with GDPR, two types of sanctions are applicable:

- For breaches of those stipulations that are gauged as most important for data protection, data regulators and DPOs can levy fines of up to €20 million or 4% of the organization's global annual turnover of the previous financial year, whichever is greater.
- For other violations, authorities may levy penalties of up to €10 million or 2% of the organization's global annual turnover, whichever is greater.



## Is GDPR relevant to your organization?

GDPR has an extended territorial scope. This means that while EU organizations are subject to GDPR, non-EU organizations that process personal data of EU residents,  or provide services to them are also subject to GDPR.

In the context of GDPR, personal data refers to any information attribute or a combination of information attributes that can directly or indirectly identify an individual. GDPR has further identified a special category of personal data or sensitive data which has more stringent regulations. Special category personal data includes data revealing religious beliefs and racial or ethnic origin, biometric data, or genetic data, to name a few.

**GDPR applies to the following categories:**

| | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Headquarters | Within Europe | Outside Europe | Outside Europe |
| Core Business | In Europe | In Europe | Not in Europe |
| Personal Data | Captures personal data of EU residents | Captures personal data of EU residents | Captures personal data of EU residents |

*Fig 2: Categories where GDPR is applicable*

## Industrial ramifications

For certain industries, personal customer data is a precious commodity. This data predominantly falls under categories 2 and 3 in the above table. For example, the financial services industry deals with highly sensitive and high-risk data containing financial records of individuals that can directly identify data subjects. The healthcare industry also keeps records of sensitive health-related personal data that can identify a data subject.

Owing to the sensitive nature of such data, a privacy breach has serious repercussions in terms of negative brand image, legal ramifications, and heavy penalties. Thus, the onus for data protection rests squarely on the DPO due to the high-risk nature of data and proliferation of data between various systems and processes.

## Technical ramifications

Most of the existing enterprise cloud applications and enterprise documents that are stored and shared across organizations are not GDPR-compliant. As GDPR takes effect, organizations can expect significant changes to budget allocations, and technological and infrastructural changes, as well as expenditure for security and storage software.

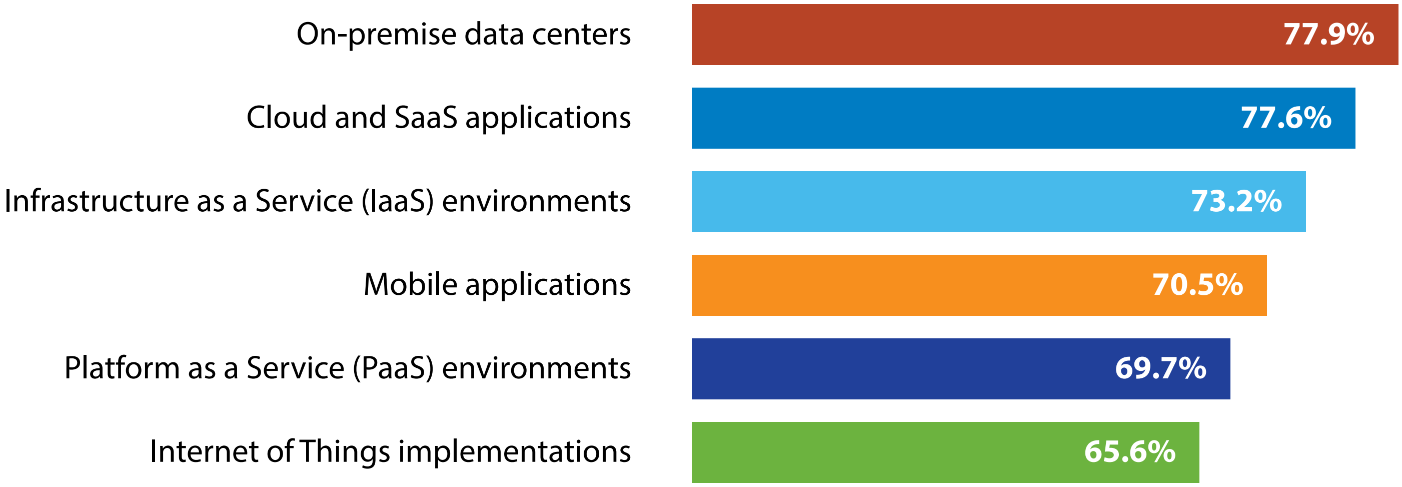


*Fig 3: Technology environments that will be regulated for sensitive data within the next 3 years*

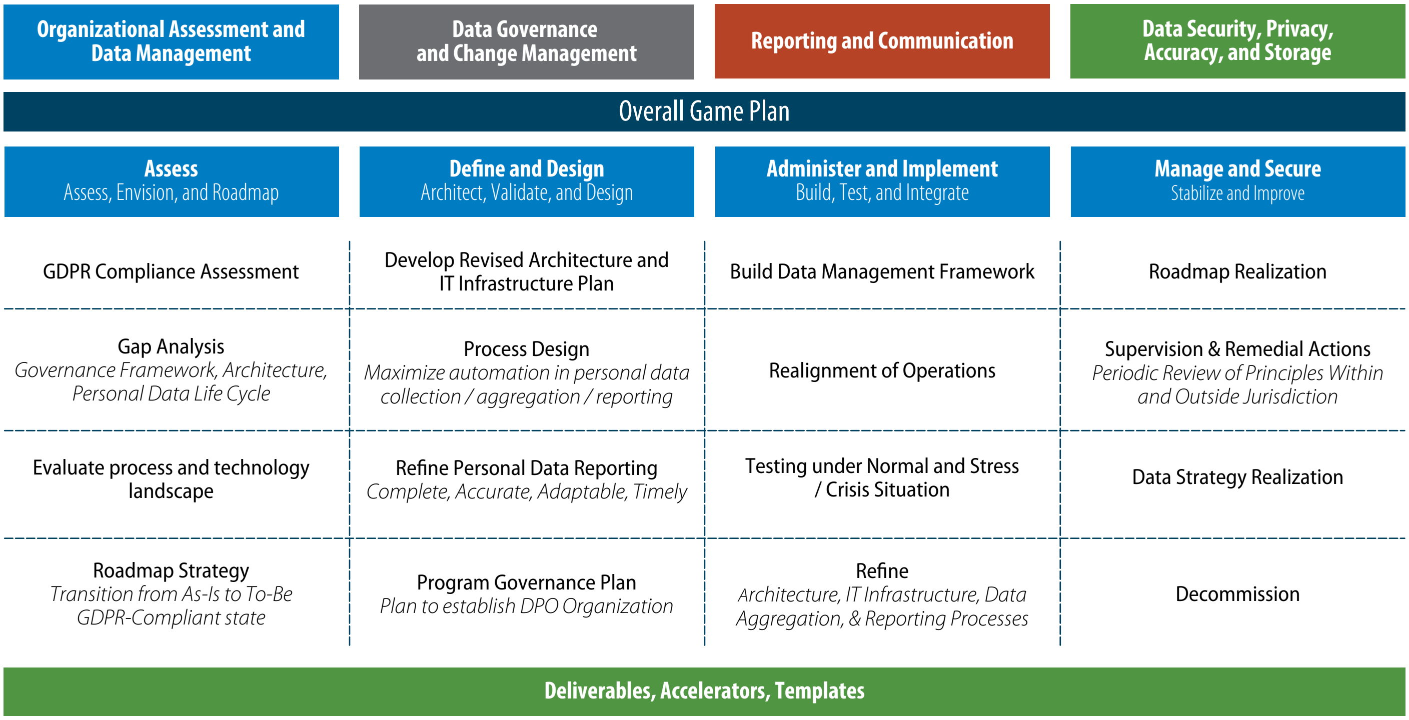
Reference: *http://www.ten-inc.com/presentations/intralinks2016.pdf*

## How can my organization prepare for GDPR?

Organizations can expect significant changes with the rollout of GDPR. Thus, it is paramount that they study the features of this new regulation and learn how to implement it while unlearning existing data regulations. This requires a dedicated as-is analysis to uncover the lacuna between the future-state and existing data models.

The Infosys Framework for GDPR (ADAM - Assess, Define and Design, Administer and Implement, Manage and Secure) is an end-to-end solution that helps organizations achieve GDPR-readiness in four phases:

- A: Assess – Here, Infosys identifies the gaps between GDPR requirements and the organization's current state and generates a road map. An organization-wide assessment is conducted that can be further drilled down to  an application-level assessment, if required.
- D: Define and Design – In this phase, policies for GDPR requirements are defined at the organizational / unit level and the future data architecture to support these policies is designed.
- A: Administer and Implement – Here, the processes and technology changes identified in the previous phase are implemented, tested, and integrated with the existing system.
- M: Manage and Secure– This phase focuses on providing support and enabling audits while the refined system is deployed across the organization.

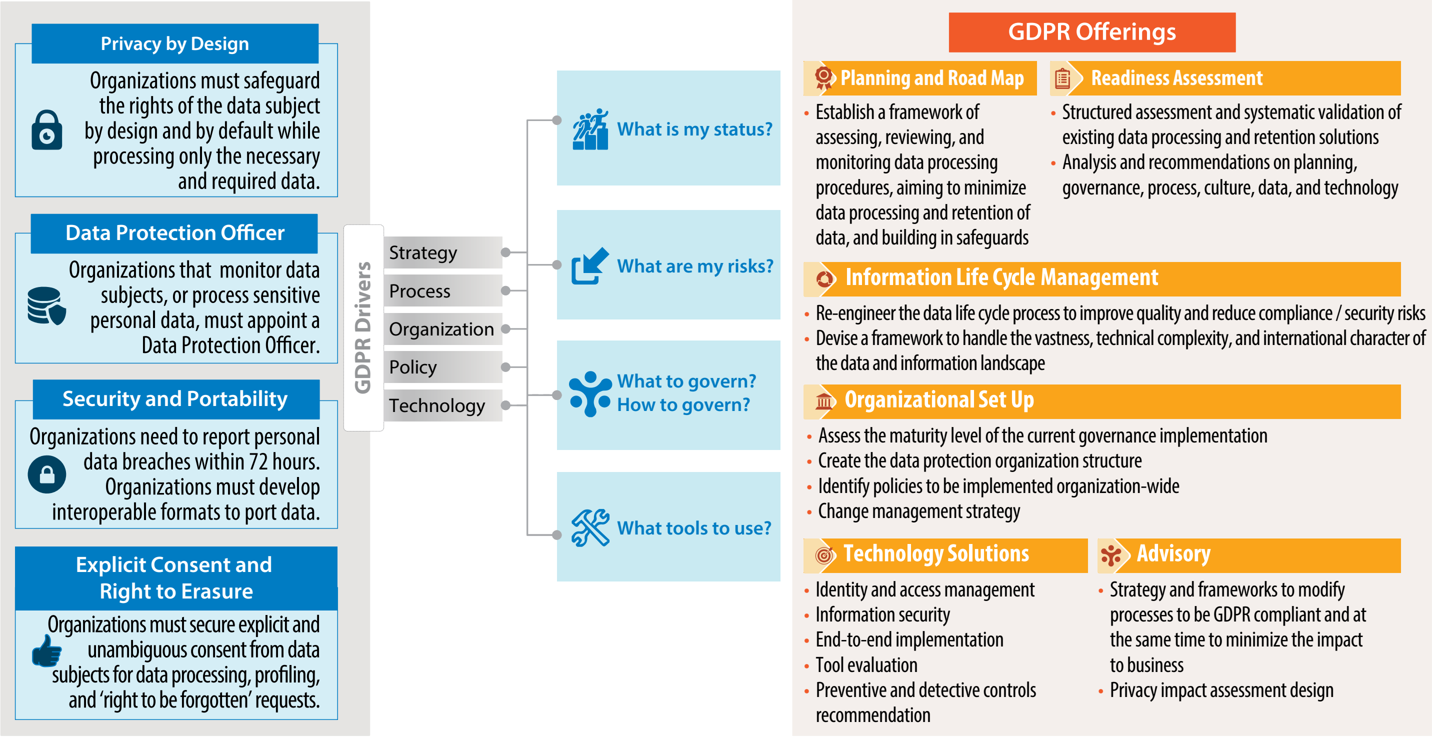


| Organizational Assessment and Data Management | Data Governance and Change Management | Reporting and Communication | Data Security, Privacy, Accuracy, and Storage |
|---|---|---|---|
| **Overall Game Plan** | | | |
| **Assess**<br>Assess, Envision, and Roadmap | **Define and Design**<br>Architect, Validate, and Design | **Administer and Implement**<br>Build, Test, and Integrate | **Manage and Secure**<br>Stabilize and Improve |
| GDPR Compliance Assessment | Develop Revised Architecture and IT Infrastructure Plan | Build Data Management Framework | Roadmap Realization |
| Gap Analysis<br>*Governance Framework, Architecture, Personal Data Life Cycle* | Process Design<br>*Maximize automation in personal data collection / aggregation / reporting* | Realignment of Operations | Supervision & Remedial Actions<br>*Periodic Review of Principles Within and Outside Jurisdiction* |
| Evaluate process and technology landscape | Refine Personal Data Reporting<br>*Complete, Accurate, Adaptable, Timely* | Testing under Normal and Stress / Crisis Situation | Data Strategy Realization |
| Roadmap Strategy<br>*Transition from As-Is to To-Be GDPR-Compliant state* | Program Governance Plan<br>*Plan to establish DPO Organization* | Refine<br>*Architecture, IT Infrastructure, Data Aggregation, & Reporting Processes* | Decommission |
| **Deliverables, Accelerators, Templates** | | | |

*Fig 4: Infosys Framework for GDPR*

Uploading ...
GUARD
DATA PROTE
PROTECT

# GDPR Offerings



**Privacy by Design**

Organizations must safeguard the rights of the data subject by design and by default while processing only the necessary and required data.

**Data Protection Officer**

Organizations that monitor data subjects, or process sensitive personal data, must appoint a Data Protection Officer.

**Security and Portability**

Organizations need to report personal data breaches within 72 hours. Organizations must develop interoperable formats to port data.

**Explicit Consent and Right to Erasure**

Organizations must secure explicit and unambiguous consent from data subjects for data processing, profiling, and 'right to be forgotten' requests.

**GDPR Drivers**

- Strategy
- Process
- Organization
- Policy
- Technology

What is my status?

What are my risks?

What to govern? How to govern?

What tools to use?

**GDPR Offerings**

**Planning and Road Map**

- Establish a framework of assessing, reviewing, and monitoring data processing procedures, aiming to minimize data processing and retention of data, and building in safeguards

**Readiness Assessment**

- Structured assessment and systematic validation of existing data processing and retention solutions
- Analysis and recommendations on planning, governance, process, culture, data, and technology

**Information Life Cycle Management**

- Re-engineer the data life cycle process to improve quality and reduce compliance / security risks
- Devise a framework to handle the vastness, technical complexity, and international character of the data and information landscape

**Organizational Set Up**

- Assess the maturity level of the current governance implementation
- Create the data protection organization structure
- Identify policies to be implemented organization-wide
- Change management strategy

**Technology Solutions**

- Identity and access management
- Information security
- End-to-end implementation
- Tool evaluation
- Preventive and detective controls recommendation

**Advisory**

- Strategy and frameworks to modify processes to be GDPR compliant and at the same time to minimize the impact to business
- Privacy impact assessment design

*Fig 5: GDPR offerings*

# Conclusion

The advent of General Data Protection Regulation (GDPR) is set to disrupt how organizations operate within their member states. As an upgrade to the previous Directive 95/46/EC, the GDPR upholds the rights of EU citizens to protect their personal data irrespective of the location of processing. Faced with pressure to comply with GDPR before the deadline lapses, organizations around the world are unaware of how to begin their transformation as personal data is captured even in core functional areas like HR & Recruitment, and Infrastructure security. The Infosys Framework for GDPR helps organizations achieve GDPR-readiness by assessing the current state, defining and designing the future state, administering and implementing the changes, and managing and securing the renewed compliance. It is important for organizations to identify the impact this regulation could bring in and take appropriate steps to handle the same. In order to grow their business in the EU and avoid stiff penalties, the time to act upon the new regulatory requirements, is now.

## About the Author

**Gaurav Bhandari**

*Senior Principal, Business Consulting,  Infosys*

Gaurav heads the Data & Analytics Consulting Practice in Infosys and has more than 14 years of experience in management and operational processes, statutory and management reporting, business intelligence, and KPI / balanced scorecard and enterprise performance management. Gaurav spearheads the Infosys GDPR service offering and has been instrumental in conceptualizing and crafting the Infosys GDPR solution framework and methodology.

He can be reached at gaurav_bhandari@Infosys.com.

*Connect with our experts at* gdprcompliance@infosys.com *to know more about GDPR, its impact on your business and how you can stay secure.*

For more information, contact askus@infosys.com

Stay Connected