Point of View

Mind the Gap:

GDPR Ahead

Author

Rakesh Sancheti

Vice President and Business Head - Analytics, Europe and Nordic

The regulatory environment has become increasingly complex, with new regulations being introduced across the world. Lately, there has been renewed focus in strengthening regulations around data, reporting, and cyber security. One of the most significant regulations affecting all the organizations in possession of European citizens' personal data, is the EU General Data Protection Regulation (GDPR) coming into effect on May 25, 2018.

The GDPR, which was adopted in May 2016, imposes a radical, much tougher data protection regulatory framework across the EU, over the processing of personal data. It covers every processing operation that can be carried out on personal data, irrespective of whether it is undertaken by automated or non-automated means, or whether done actively or passively. It defines the increased rights of EU citizens (Data Subjects), around the privacy and protection of their personal data.

The regulation also specifies the increased responsibility for any organisation or individual (Data Controller) that is responsible for storage and processing of EU citizens' personal data, while hiring or surveying them, buying selling, or marketing a service / product, etc. Data controllers have to stick to the purpose for which the data has been acquired, minimize the amount of data held, keep it accurate, secure and confidential at all times. They then must delete or destroy it when the purpose for which the data was obtained or created has been fulfilled, or if the consent to use it has been withdrawn. Failure to comply with this regulation can result in fines of up to 4% of the global revenue.

LTIMindtree

The fundamental cornerstones of GDPR regulation

Assess Personal Data

- Classify organisational data
- Identify compliant data

Protect Personally Identifiable Information

- Protect data in use, in transit, and at rest
- Ensure Privacy by Design which will involve rethinking the way PII, PHI, ePHI, and PCI data is handled
- Address the requirements of the GDPR compliance in a methodical and modular fashion

Appoint a Data Protection Officer

- Appoint a Data Protection Officer (DPO) at both Data Controller and Data Processor levels

Enable the Data Subject rights

- Erase the data once the purpose is complete and cease its dissemination
- Develop interoperable formats that enable Data Portability

Notify breaches within 72 hours

- Carry out Data Protection Impact assessments
- Formulate measures to address any high risks that have been identified

GDPR Implementation: How Confident are the Organizations?

According to a recent global survey, a staggering 90% of the organizations believe that the GDPR will impact the way they collect, use, and process personal data. Only 46% of the organizations are confident to be ready by the go-live date; and most importantly, 88% of the organizations accepted that the GDPR has exposed holes in their IT architecture, and hence, they consider this as an opportunity to overcome their technological challenges, thus contributing towards their IT transformation programs.

Our conversations with European and Nordic customers have highlighted the challenges they are facing, to rightly fulfil the complex regulatory demands of the GDPR, and in parallel, manage the data deluge and technology disruption. They are looking out for help in driving efficient risk management across the value chain of their business landscape, and continue to move upwards in the technology maturity continuum.

Route to the GDPR: The Key to Success

To implement GDPR successfully, organizations need to follow a three step systematic approach that begins with a maturity assessment and finding the gaps, followed by any application and architecture related changes to bridge those gaps. In the later stage, it includes continuous execution of automated processes, to ensure continued improvement and prevention of breaches.

Find the Gap: in order to protect data, the organizations first need to know where it is, and determine its risk profile. It's easier said than done. Most organizations struggle to gain visibility into their data assets, and thus have to invest in data discovery and classification related initiatives. The first step toward the GDPR compliance is to conduct a Privacy Impact Assessment to understand the data landscape, and how data flows inside and outside the organization. This will enable to better assess information risk profile, classify data, and identify lineage. Additionally, this exercise will locate the gaps in an organization's processes, systems, oversight mechanisms, and skills. Once this has been done, the next step is to evaluate the current risk mitigation strategies. This includes, for example, reviewing the implementation of security controls. Firms must also use the gap analysis phase to estimate the approximate budget required to successfully implement the GDPR program.

Bridge the Gap: Once the assessment has been completed, organizations must define data governance best practices, policies, data stewardship and establish a Data Governance Office. The current information architecture should also be looked at, with focus on bridging gaps around managing data subject consent, access & rights, Privacy by Design & Privacy by Default, and data pseudonymization & anonymization. Additionally, it is necessary to have insight into the physical location of data and where it is processed, including cross-border transfers.

Therefore, organizations must assess master data residency, data storage management (backup and recovery policies), and the use of cloud Infrastructure as a Service (IaaS) & Platform as a Service (PaaS). In addition, organizations must deploy security controls compliant with the GDPR. For example, when encrypting data, privacy and security teams must pay attention to how the encryption keys are being managed.

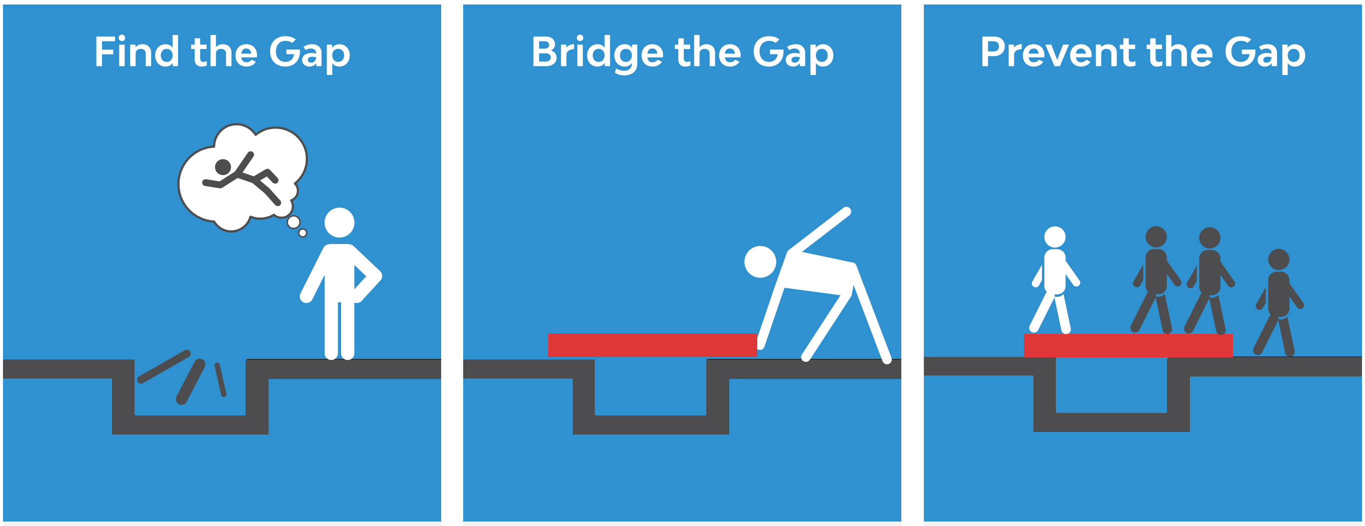
Prevent the Gap: GDPR is not a one-time regulation. It is a continuous process which requires defining a continuous feedback loop for ongoing compliance and improvement. Metrics that track the achievements of data privacy and security programs, along with self-service BI reports and real-time dashboards for KPI tracking need to be in place.

With the deadline to become GDPR-compliant approaching fast, organizations need to act now. They need to know which IT applications and business processes possess personal data; why they have it; how they are using it; who is accessing it; how they are protecting it; if they have the right technology infrastructure to be able to demonstrate end-to-end data lineage to an external regulator, etc.

To conclude, treating GDPR as merely a compliance is the first sign of non-compliance. The task at hand is surely overwhelming, but can be managed if we treat this as an embedded and holistic set of interventions across the applications and systems landscape.

This has been demonstrated below:

3 Step Route to GDPR



Find the Gap

GDPR Readiness Assessment

- Data Management Maturity
- Personal Data Inventory
- Data Breach Risk Assessment & Exposure

Bridge the Gap

Data Governance Policy

(Re) architect Data Landscape

- Workflows & controls
- Data Masking
- Dissemination & Standards
- MDM
- Metadata hub

Data Security Enablement

Performance & Data Protection Rules Testing

Prevent the Gap

Intelligent Breach Assistance

- Prevent security breaches
- Advanced analytics

GDPR Insight

- Data Breach Monitoring
- Real time Dashboards
- Self-service BI portal
- Data Subject Rights - queue / status
- Metrics & Threshold monitoring

About the Author

Rakesh Sancheti

Rakesh Sancheti is Area Vice President at LTIMindtree, and Business Head for Analytics & Information Management Practice for Europe and Nordic. He is a Data analytics practitioner with 11+ years of hands on experience in helping customers co-create Data-driven enterprise, by leveraging Data analytics as fuel in their digital transformation journey. He is well-versed in defining Data strategy, Information architecture and Business use cases for Big data analytics across industry value chain, to deliver meaningful business insights, and better business outcomes at speed and scale. He has worked with global clients to deliver projects across Data to Insight value chain - Data Integration, Data Management, Business Intelligence, Big Data, Data Science and Machine Learning.