Deloitte.

# EU General Data Protection Regulation (GDPR)

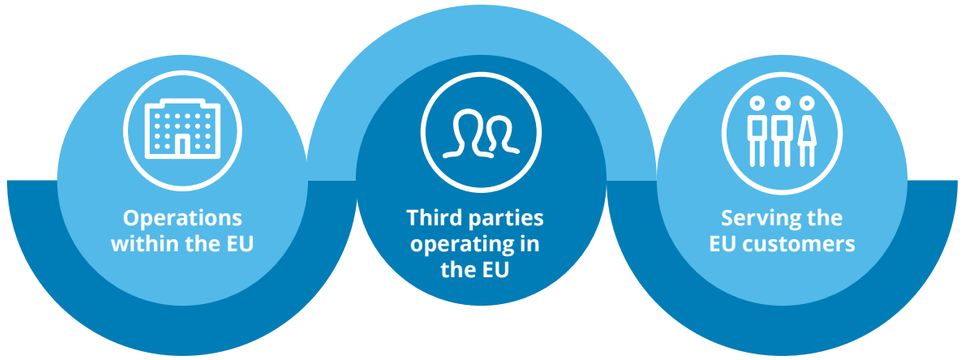
## Point of View for ERP and HRMS Operations

For private circulation only

Cyber Risk

# Preface

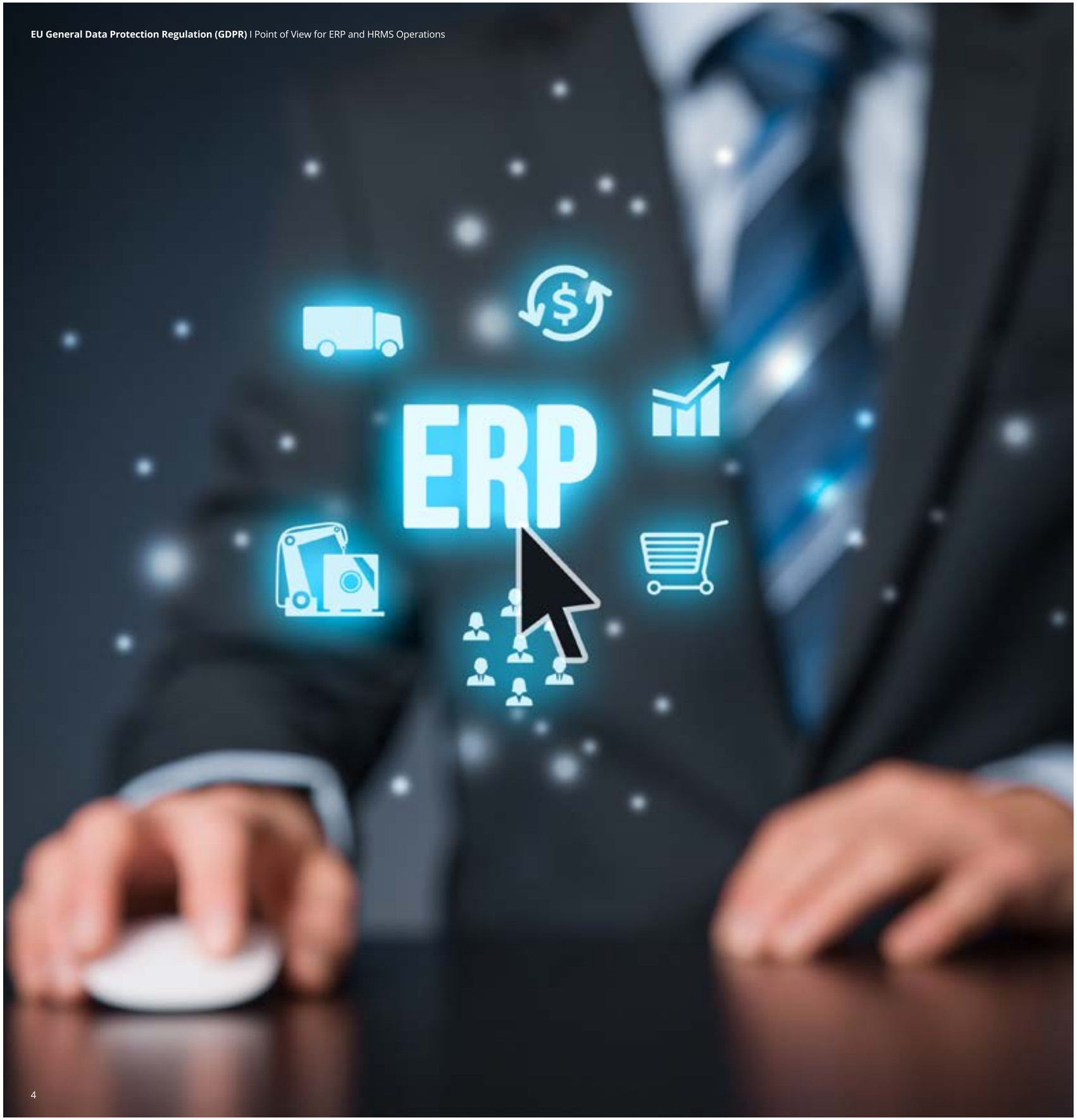
**Does the EU GDPR impact organisations in India?**
Yes! This new law will have a profound impact on the operational and control environment of the organisations, not only within EU but also within the organisations based outside the EU having:




This is a border less and sector neutral legislation. It goes beyond EU to 'organisations offering goods or services to customers in EU', 'organisations that monitor the (online) behavior of the EU customers' and during these services such organisations access/process/host/store "personal data" of EU customers.

With enforcement date approaching fast (25 May 2018), organisations are recommended to quickly assess GDPR's applicability and initiate readiness journey at the earliest.

Note: Map on this slide is only for the representation purposes.






**EU General Data Protection Regulation (GDPR)** I Point of View for ERP and HRMS Operations

# Content

# Understanding this new regulation

## How it applies to Indian organisations?

- The General Data Protection Regulation (GDPR) is a law or a regulation which was adopted by the European Commission on 27 April 2016.
- It is scheduled to go into enforcement effective 25 May 2018 and is expected to impact organisations across the globe that do business in Europe.
- A core feature of the GDPR is that as a regulation, rather than a directive, it does not require enabling legislation in each member state, something that historically led to inconsistencies.
- As per the Article 2 "Material Scope", this regulation applies to the processing of personal data wholly or partly by automated means.
- Applicability (as per the Article 3 "Territorial effect") of GDPR is linked to the processing of the "personal data"
  - In the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.
  - Of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services, to such data subjects in the EU; or the monitoring of their behaviour as long as their behaviour takes place within the EU.
  - By a controller not established in the EU, but in a place where member state law applies by virtue of public international law.

**Is it a 'must' to comply?**
Yes, if your organisation is subject to this regulation.

**Any impact of its non-compliance?**
Key impact – penalty of maximum 4% of annual worldwide turnover or €20 million (greater of the two)!!!




**EU General Data Protection Regulation (GDPR)** I Point of View for ERP and HRMS Operations

# How it evolved?

**1995**

In 1995, the European Union released the **European directive 95/46/CE** relative to personal data protection.

**2012**

The European Commission proposed to **reform** the current fragmented legal framework to deal with the new challenges for the protection of personal data and to make the EU member states fit for the digital age.

**2016**

On 4 May 2016, the **EU Regulation on Data Protection (GDPR)** has been published in the Official Journal of the European Union. The GDPR has entered into force on 24 May 2016 and will replace the former 1995 EU Data Protection Directive and create a harmonised data protection law across Europe.

**2018**

The GDPR will be enforced as of 25 **May 2018** directly across all 28 EU Member States after a two years implementation period.

**Now**

**Data Protection Directive 95/EC/46 + National Laws**

- First harmonisation, but fragmentation per country
- Transposed in natural laws
- Enforcement by national Data Protection Authorities (DPAs)
- Low penalties

**Future**

**General Data Protection Regulation (GRPR)**

- Full harmonisation
- Directly applicable
- Enforcement by national DPAs + Consistency Mechanism + European Data Protection Board (EDPB)
- High penalties





# What has changed?

What has changed from the former 1995 EU Data Protection Directive?

**General Data Protection Regulation**

| | |
|---|---|
| **Broader territorial scope** | Applies to players **not established in the EU** but whose activities consist of targeting data subjects in the EU. |
| **Enforcement** | Data Protection Authorities (DPA) will be entitled to impose **fines ranging between 2% to 4% of annual turnover or 10–20 million EUR, whichever is higher.** |
| **Accountability** | Explicit obligation to the controller as well as the processor to be able to **demonstrate their compliance to the GDPR.** |
| **Expanded definitions** | Personal data now **explicitly includes location data, IP addresses, online and technology identifiers.** |
| **Data Subject's rights** | **Reinforced rights:** Access, rectification, restriction, erasure, objection to processing, no automated processing, and profiling. |
| **Consent** | **Spelled out more clearly** and focus on ability of individuals to distinguish a consent. |
| **Data breach notification** | Report a personal data breach to the DPA within 72 hours. |
| **One-stop shop** | **Data Protection Authorities (DPA) of main establishment can act as lead DPA,** supervising processing activities throughout the EU. |
| **International data transfers** | **Binding Corporate Rules** ("BCR") as tools for data transfers outside the EU and EEA are now embedded in the law. |

# Understanding GDPR in numbers

**4%**
Potential fines as a percentage global turnover as it applies to cross border organisations which have access to EU data.

**7**
Core individual rights afforded under the GDPR.

**72**
Hours given to report a data breach.

**250m**
Cost of 4% fine for a typical FTSE 100 company.

**28,000**
Estimated number of new Mandatory Data Protection Officers required in Europe (IAPP study 2016).

**190+**
Countries potentially in scope of the regulation.

**80+**
New requirements in the GDPR.

**88** Pages
**11** Chapters
**99** Articles



**EU General Data Protection Regulation (GDPR)** I Point of View for ERP and HRMS Operations

# Key considerations for ERP environment

Organisations today use various ERP solutions while dealing with their business partners (e.g., employees, customers, vendors etc.) and many capture personal data of these data subjects. It is essential to understand which of these data subjects and personal information is covered under GDPR (as briefed in preceding section). ERP also emphasises on ease of user experience and have been aggressively pushing solutions like mobility, cloud, etc., which adds newer dimension to data access. Holistic view is required where ERP and non-ERP applications co-exist while performing the impact assessment.

- ERP solution facing retail customers e.g., IS Utilities, IS Retail or any other similar solution capturing information of retail customers which can be treated as sensitive information under GDPR.


- Analytical tools extracting data from ERP may replicate sensitive information for employees, and customers or a combination of multiple applications, such information may be sensitive under GDPR.

- Employee information can be captured using ERPs like SAP HR, SAP Success Factors, SAP ESS/MSS, etc.
- Creation of employees as vendors for advances, expenses in ERPs like SAP HR, SAP FICO, concur, etc.
- Organisations may also go for a hybrid approach where employee data is shared across ERP and other applications using interface/data exchange

- Covered persons under GDPR are individuals (may be employees, consultants, vendors, etc.) or customers in EU. Their personal data gets recorded in ERP applications such as (SAP MM module/SRM tools, e.g., Ariba, etc.)

- Customer information including client and contact details of key client contact person may become a sensitive information under GDPR.

ERP environment is accessed by various departments, functions within organisation and ERP support by vendors. While evaluating GDPR impact around ERP operations it is recommended to consider data residing in non productions instances like development, quality and test. Data exposed using interfaces and mobile application utilities will necessitate the need for tools to perform data masking, data archival and data encryption.

# Are you prepared?

## Respond

- Do you have a process to enable data subjects' rights such as request for access/ portability or erasure?
- Is there adequate processes in place to respond and notify data breaches?

## Assess

- What types of data do you collect, and where does the data originate?
- Are adequate controls in place for use, processing, storage, transfer and destruction?
- Are Privacy Impact Assessments conducted as required?
- Are internal and independent reviews conducted on a periodic basis?

## Governance

- Are roles and responsibilities defined?
- Has an assessment of the organizations' risk exposure from EU GDPR been conducted?
- Do you have oversight of the data lifecycle from the point of origin to destruction?
- Is there a process for identifying and responding to local regulatory requirements in addition to GDPR?

## Monitor

- Are compliance metrics identified and measured?
- Are processes, systems, and networks monitored to identify data access, use, change and breaches?

## Protect

- Do you have a process to perform a risk analysis or new or changing business processes?
- Is Privacy by Design and Privacy by Default incorporated within the processes?
- Will you able to erase data when requested?
- Are technological safeguards in place to protect sensitive data?





# How can we help?

## Our service offerings*

Deloitte has a dedicated team of specialists with a deep expertise in privacy data protection programs across large scale and complex organizations, embedding change and offering a full spectrum of **GDPR related services:**

- GDPR readiness assessment
- Change programme design and delivery
- Third party management
- GDPR compliance roadmap
- Incident Management Framework
- GDPR program monitoring and roll-out strategy
- Global privacy compliance assessment
- Data discovery, mapping, and inventories
- Governance and compliance review
- GDPR technology impact assessment
- Privacy-by-design advice and application
- Privacy risk and compliance training
- Privacy programme development
- Data leakage protection
- Privacy strategy and roadmap development
- Privacy impact assessment and health check

*Deloitte Touche Tohmatsu India LLP offers advisory services on aspects related to Governance, People, Technology and Processes to help address the requirements under GDPR. Kindly note that Deloitte Touche Tohmatsu India LLP does not provide any legal advice, including any legal advice relating to privacy or data protection laws.

# Key contacts

## National

**Rohit Mahajan**
Partner & National Leader – Risk Advisory
rmahajan@deloitte.com

**Shree Parthasarathy**
Partner – Risk Advisory
National Leader – Cyber Risk Services
sparthasarathy@deloitte.com

## Regional

**A.K. Viswanathan**
Partner – Risk Advisory
Cyber Risk Services
Mumbai

**Priti Ray**
Partner – Risk Advisory
Cyber Risk Services
Mumbai & Kolkata

**Abhijit Katkar**
Partner – Risk Advisory
Cyber Risk Services
Mumbai

**Maninder Bharadwaj**
Partner – Risk Advisory
Cyber Risk Services
Bangalore

**Ramu Narsapuram**
Partner – Risk Advisory
Cyber Risk Services
Hyderabad

**Ashish Sharma**
Partner – Risk Advisory
Cyber Risk Services
Pune

**Ravi Veeraraghavan**
Partner – Risk Advisory
Chennai

**Gaurav Shukla**
Partner – Risk Advisory
Cyber Risk Services
Bangalore & Hyderabad

**Gautam Kapoor**
Partner – Risk Advisory
Cyber Risk Services
Gurgaon

**Praveen Sasidharan**
Partner – Risk Advisory
Bangalore & Chennai

**Munjal Kamdar**
Partner – Risk Advisory
Cyber Risk Services
Mumbai

## National Privacy Centre of Excellence

**Vishal Jain**
Partner – Risk Advisory
Cyber Risk Services
National Privacy Lead
Mumbai
jainvishal@deloitte.com

**Manish Sehgal**
Director – Risk Advisory
National Solution Director for Privacy
Gurgaon
masehgal@deloitte.com

Deloitte.