EU General Data Protection Regulation (GDPR)
A Point of View for Global In-house Centres (GICs) in India
For private circulation only
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.
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 "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)!!!

How it evolved?

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

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.

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.

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

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

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

Now

Future
What has changed?

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

- **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
Impact of GDPR on Global In-house Centres (GICs)

**GICs in India**

**IT GICs**
- ADM – Application Development & Maintenance,
- SI – System Integration,
- IMS – Infrastructure Management Services,
- Others include IT Consulting

**Business Process Outsourcing**
- F&A – Finance Accounting,
- HR – Human Resources,
- P&L – Procurement & Logistics,
- S&M – Sales & Marketing,
- TS – Technical Support,
- KBS – Knowledge Based Services

**Product Development**
- Software Product Development
- Embedded Systems
- Engineering Services
- Research and Development

**GDPR Impact**

<table>
<thead>
<tr>
<th>Actionable by GICs?</th>
<th>Broader territorial scope</th>
<th>Enforcement</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Applies to any organisation handling EU citizens data</td>
<td>Non-compliance results in fines</td>
<td>Demonstrate Compliance Responsible for Compliance by third parties Privacy by design/default Training and awareness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Expanded definitions</th>
<th>Data Subject’s rights</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Classification Data Management Data Security</td>
<td>Privacy by design/default Data Lifecycle Management Data Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unambiguous consent required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incident Management Process Crisis Management Report to DPA within 72 hours Report to Data Subject as soon as possible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>One-stop shop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One Data Protection Authority (DPA) to act as lead DPA for reporting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>International data transfers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Third Party Management Contract Management Vendor Review</td>
</tr>
</tbody>
</table>

* Representative action/impact areas and may vary with organisations.
Are you prepared?

**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?

**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?

**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 impact assessment and health check
- Privacy strategy and roadmap development

*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**

Amry Junaideen  
President - Risk Advisory  
amjunaideen@deloitte.com

Shree Parthasarathy  
Leader - Cyber Risk  
sparthasarathy@deloitte.com

**Regional**

**Mumbai**

A.K. Viswanathan  
Partner - Risk Advisory  
akviswanathan@deloitte.com

Abhijit Katkar  
Partner - Risk Advisory  
akatkar@deloitte.com

Vishal Jain  
Partner - Risk Advisory  
jainvishal@deloitte.com

Priti Ray  
Partner - Risk Advisory  
pritiray@deloitte.com

Munjal Kamdar  
Partner - Risk Advisory  
mkamdar@deloitte.com

**Bengaluru**

Maninder Bharadwaj  
Partner - Risk Advisory  
manbharadwaj@deloitte.com

Gaurav Shukla  
Partner - Risk Advisory  
shuklagaurav@deloitte.com

Praveen Sasidharan  
Partner - Risk Advisory  
psasidharan@deloitte.com

**Delhi**

Gautam Kapoor  
Partner - Risk Advisory  
gkapoor@deloitte.com

**Hyderabad**

Ramu Narsapuram  
Partner - Risk Advisory  
ramun@deloitte.com

**Pune**

Ashish Sharma  
Partner - Risk Advisory  
sashish@deloitte.com