The Digital Personal Data Protection Act, 2023

Advent of Privacy Era in India

The better the question. The better the answer. The better the world works.
Salient features of the Act (Contd.)

Significant Data Fiduciary
Significant Data Fiduciary will be determined based on an assessment which include:

- The volume and sensitivity of personal data processed
- Risk to electoral democracy
- Risk to the rights of data principal
- Security of the state
- Potential impact on the sovereignty and integrity of India
- Public order

Obligations of the Significant Data Fiduciary

- Appoint a Data Protection Officer (DPO) based in India
- Appoint an Independent Data Auditor for evaluating compliance
- Conduct Data Protection Impact Assessment (DPIA) & periodic audits

Data Principal Rights

- Right to information: Data Principals have the right to seek information on how their data is processed, available in clear and understandable way.
- Right to correction and erasure: Individuals have the right to correct inaccurate / incomplete data and erase data that is no longer required for processing.
- Right to nomination: Individuals can nominate any other individual to exercise these rights in the event of death or incapacity.
- Right to grievance redressal*: Individuals have the right to readily available means of registering a grievance with a Data Fiduciary.

*Timeline to respond to grievances raised by Data Principals shall be notified by the Central Government.
Salient features of the Act (Contd.)

Personal Data Breach

- A Data Fiduciary is required to protect personal data, including any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent Personal Data Breach.
- In the event of a Personal Data Breach, the Data Fiduciary needs to notify the Board and each affected Data Principal of such breach.

Penalties

- **Up to INR10,000**
  - Breach in observance of duty of Data Principal
- **Up to INR200 Crore**
  - Breach in observance of additional obligation in relation to children
- **Up to INR200 Crore**
  - Breach in not giving notice of Personal Data Breach
- **Up to INR250 Crore**
  - Noncompliance of the provisions by Data Fiduciaries

The Data Protection Board

The Central Government may, by notification shall appoint and establish, an independent board to be called the Data Protection Board of India (Board).
- This Board should consist of a chairperson and other members, who should be appointed by the Central Government.
- The Board is entrusted with the task of enforcement, including determining non-compliances, imposing penalties, issuing directions and mediation (to resolve dispute between parties) to ensure compliance with the law.
- The Board is enshrined with powers of a civil court and appeals against its decisions lie to Telecom Disputes Settlement and Appellate Tribunal.

Amendments to Prevailing Laws

Existing IT Act, 2000 and Right to Information Act 2005 are amended as following:

- Article 43(A) (Compensation for failure to protect data) of IT Act 2000 is omitted
- Section 8 (1)(j) RTI Act 2005 is amended to exempt the personal information which allows disclosure for public interest
Salient features of the Act (Contd.)

Key Highlights

- When the consent for processing Personal Data was provided before the commencement of this Act, Data Fiduciary needs to provide detailed privacy notice describing the Personal Data collected and the purpose as soon as practicable after the enactment of this Act.
- Certain provisions* of the Act will not be applicable for the processing of Personal Data in India of a Data Principal not based in India pursuant to a contract signed with a person outside India.
- The Central Government may upon ensuring if the processing is verifiably safe, notify the age above which a Data Fiduciary shall be exempt from applicability of children’s personal data obligations.
- The Data Principal shall exhaust the opportunity of redressing her grievance with Data Fiduciary before approaching the Data Protection Board of India.

Exemptions

The DPDP Act exempts Data Fiduciary from certain obligations (except for being responsible for its data processor and taking reasonable security safeguards) under specified circumstances including:

- Processing for enforcing any legal right or claim.
- Processing for performance of any judicial or quasi-judicial functions by any Indian court/tribunal or other body.
- Processing in the interest of prevention, detection, investigation or prosecution of any offence of any law.
- Processing of Data Principals outside the territory of India pursuant to any contract entered into with any person outside the territory of India by any person based in India.
- Processing necessary for a merger / amalgamation or similar arrangement as approved by a court or other authority competent.

Ambiguities

Below mentioned are the ambiguities in the Act:

- **Children’s Data**
  The definition of detrimental effect on well-being of a child as a result of processing their Personal Data has not been specified.

- **Breach Notification**
  Absence of defined timeline for notifying a Personal Data breach to the Data Protection Board and the affected Data Principal(s).

- **Publicly available data**
  The Act exempts any Personal Data that is made available publicly, but it does not clarify if the information is made available to public can be used for processing or can be for view-only purposes.

- **Data Principal Request timeline**
  The Act has not specified a timeframe for Data Fiduciaries to respond to any Data Principal requests.
The Digital Personal Data Protection Act, 2023

GDPR lays down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules. The Act has not identified any transfer mechanisms for transferring Personal Data.

Both Controllers and Processors are under the obligation to appoint a DPO in specific circumstance. Only the Significant Data Fiduciary shall have to appoint DPO as a point of contact for the Data Protection Board.

GDPR does not explicitly specify to provide notice to regional languages. Significant Data Fiduciaries are obligated to conduct periodic Data Protection Impact Assessment (DPIA).

GDPR does not include right to nominate however provides for the right to portability. Organizations have 30 days to respond to a Data Subject request. The Act comprises of an additional right to nominate while omits the right to portability and timeline to respond to the Data Principal requests has not been specified.

Breaches should be notified to the Supervisory Authority within 72 hours and possibly to the affected Data Subjects. The Act does not specify a timeframe for Personal Data breach notification.

Minors under age 16 need parental consent. Members states of Europe can lower this age to 13 for their regions. Children under the age of 18 need consent from parents/guardian.

Penalties under GDPR extend to 20 million euros, or 4% of the firm’s worldwide annual revenue from the preceding financial year, whichever amount is higher. Penalties under the DPDP Act extend up to INR250 crore.

GDPR applies to processing of Personal Data wholly or partly by automated means and to Personal Data which form or will form a part of a filing system. The DPDP Act will apply to digitized personal data and non-digitized personal data which is subsequently digitized.

The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA). DPDPA Act requires the Data Fiduciaries to provide notice in 22 Indian languages in addition to English.

Below mentioned are the key differences between DPDPB 2023 and the General Data Protection Regulation (GDPR):

<table>
<thead>
<tr>
<th>General Data Protection Regulation (GDPR)</th>
<th>Digital Personal Data Protection (DPDP) Act, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR applies to processing of Personal Data wholly or partly by automated means and to Personal Data which form or will form a part of a filing system.</td>
<td>The DPDP Act will apply to digitized personal data and non-digitized personal data which is subsequently digitized.</td>
</tr>
<tr>
<td>Penalties under GDPR extend to 20 million euros, or 4% of the firm’s worldwide annual revenue from the preceding financial year, whichever amount is higher.</td>
<td>Penalties under the DPDP Act extend up to INR250 crore.</td>
</tr>
<tr>
<td>Minors under age 16 need parental consent. Members states of Europe can lower this age to 13 for their regions.</td>
<td>Children under the age of 18 need consent from parents/guardian.</td>
</tr>
<tr>
<td>Breaches should be notified to the Supervisory Authority within 72 hours and possibly to the affected Data Subjects.</td>
<td>The Act does not specify a timeframe for Personal Data breach notification.</td>
</tr>
<tr>
<td>GDPR does not include right to nominate however provides for the right to portability. Organizations have 30 days to respond to a Data Subject request.</td>
<td>The Act comprises of an additional right to nominate while omits the right to portability and timeline to respond to the Data Principal requests has not been specified.</td>
</tr>
<tr>
<td>GDPR lays down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules.</td>
<td>The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA).</td>
</tr>
<tr>
<td>Both Controllers and Processors are under the obligation to appoint a DPO in specific circumstance.</td>
<td>Only the Significant Data Fiduciary shall have to appoint DPO as a point of contact for the Data Protection Board.</td>
</tr>
<tr>
<td>Data Controller and Data Processor are required to maintain the records of processing activities (ROPA).</td>
<td>The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA).</td>
</tr>
<tr>
<td>GDPR does not explicitly specify to provide notice to regional languages.</td>
<td>DPDPA Act requires the Data Fiduciaries to provide notice in 22 Indian languages in addition to English.</td>
</tr>
<tr>
<td>Data Protection Impact Assessment (DPIA) is to be conducted by Data Controllers for all the high-risk processing activities.</td>
<td>Significant Data Fiduciaries are obligated to conduct periodic Data Protection Impact Assessment (DPIA).</td>
</tr>
</tbody>
</table>
What’s Now, Next and Beyond

Journey to Compliance

As organizations embark on the journey toward compliance with DPDP Act 2023, there are multiple facets and requirements as per the Act and could be phased in 3 - 24 months for an effective and sustainable Data Privacy and Protection Program.

**Now**
3 - 6 months

- Undertake a Data Privacy Assessment to understand the current posture toward privacy and the requirements
- Develop Data Privacy framework to strengthen your organizations Data Privacy Program
- Establish the Data Privacy Organization to drive the program
- Data Discovery, Classification, and Mapping exercise to identify the Personal Data touch points, and structured and unstructured data across the environment and classify them.
- Develop an inventory of assets processing personal information and also the entire list of suppliers / 3rd parties leveraged for various purposes / delivering the services

**Next**
6 - 12 months

- Develop/update relevant policies and underlying procedures to outlay the intent and consistent approach toward privacy and protection
- Conduct Data Privacy Impact Assessments (DPIAs) for the high-risk in-scope business functions/ applications to identify the potential risk exposure
- Establish mechanisms for:
  - Consent management
  - Data Principal rights
  - Breach notification

**Beyond**
12 - 24 months

- Implement Privacy Enabling Technologies (PETs) to reduce manual tasks, and manage your data governance activities in an automated manner
- Undertake external certifications to demonstrate compliance toward the Privacy Information Management System
- Technical safeguards
- Training and awareness
- Periodic audits
- Establish and drive cyber culture in the enterprise
- Strong cyber governance mechanism sponsored by the Board
- Continuous monitoring of the notifications and amendments by the Data Protection Board / Central Government

*Note: Conducting DPIAs is a mandatory requirement for a Significant Data Fiduciary*
How EY can help?

Journey to Compliance

Our broad transformation approach considers the key facets of the Act across organization’s data management lifecycle

- **Data Privacy Assessment**: Assess the current Data Privacy posture, working practices and documentation against the requirement of DPDB
- **Data Discovery and Mapping**: Identify the Personal Data touch points and conduct data discovery and mapping activities
- **Third-Party Risk Management**: Identify the third party ecosystem, ensure organizational and technical security measures are implemented through inclusion of the same within valid contracts
- **Technical Safeguards**: Identify the critical business processes/assets/applications which processes large volume of Personal Data and implement technical security measures
- **Privacy Risk Assessment**: Perform Data Protection Impact Assessment (DPIA) for the high risk in-scope business functions/applications to identify the potential risk exposure*
- **Privacy Enhancing Technologies**: Reduce manual tasks with integrated workflow through Privacy Enhancing Technologies and manage your data governance activities in an automated manner
- **Internal Audit Assistance**: Independent Data Privacy audits to identify the gaps and risks on a periodic basis

* Potential risk exposure refers to the extent to which personal data is affected and the severity of the impact.
Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 9th Floor, Golf View Corporate Tower B, Sector 42, Golf Course Road, Gurugram, Haryana - 122 002.

© 2023 Ernst & Young LLP. Published in India. All Rights Reserved.

EYIN2308-011
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RS2