The Digital Personal Data Protection Bill India 2023
Contents

1. Introduction
2. Key tenets of the DPDP Bill 2023
3. Our perspective on the key tenets
4. Penalties for non-compliance
5. Way forward for organisations
Introduction
# The Digital Personal Data Protection Bill 2023

## The Bill applies to

<table>
<thead>
<tr>
<th>01</th>
<th>within the Indian territory</th>
</tr>
</thead>
<tbody>
<tr>
<td>to the processing of digital personal data within the territory of India, where the personal data is collected in a:</td>
<td></td>
</tr>
<tr>
<td>01 a) digital form</td>
<td></td>
</tr>
<tr>
<td>01 b) personal data collected is in non-digital form and digitised subsequently.</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>outside the Indian territory</td>
</tr>
<tr>
<td>to processing of digital personal data outside the territory of India, if such processing is in connection with:</td>
<td></td>
</tr>
<tr>
<td>02 a) any activity related to offering of goods or services to data principals within the territory of India.</td>
<td></td>
</tr>
</tbody>
</table>

## The Bill doesn’t apply to

- personal data processed by an individual for any personal or domestic purpose; and
- personal data that is made or caused to be made publicly available by the data principal to whom such personal data relates
- person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Digital personal data means personal data in digital form.

The Bill introduces duties for data principals and imposes a penalty up to INR 10,000 for any breach of duty.

There are financial penalties up to INR 250 crores for data fiduciary and the Bill does not impose criminal penalty for non-compliance.

Significant Data Fiduciary (SDF) notified by the government will be accountable for additional obligations.

The Bill gives equal merit for protection to all digital personal data and does not define any data category as sensitive personal data/critical data.
Key tenets of the DPDP Bill 2023
### Key tenets of the DPDPB 2023

<table>
<thead>
<tr>
<th>Data lifecycle</th>
<th>Data collection</th>
<th>Data processing</th>
<th>Data storage/transfer</th>
<th>Transparency and accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data principal</strong></td>
<td>Consent and consent withdrawals</td>
<td>Right to access information about personal data</td>
<td>Right to correction of personal data</td>
<td>Right of grievance redressal and nominate</td>
</tr>
<tr>
<td><strong>Data fiduciary</strong></td>
<td>Notice</td>
<td>Grounds of processing personal data</td>
<td>Certain legitimate uses</td>
<td>Security safeguards</td>
</tr>
<tr>
<td></td>
<td>Verifiable parent/guardian consent</td>
<td>Additional obligations of significant data fiduciary</td>
<td>Data processor engagement</td>
<td>Data retention</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Personal data breach notification</td>
<td>Processing of personal data outside India</td>
</tr>
</tbody>
</table>

**Data Protection Board of India**

- **Penalty**
- **Grievance redressal**
- **Review and appeal**
- **Dispute resolution**
Our perspective on the key tenets
## Data principal’s rights and duties

### Reference to the Bill | Key highlights | Our perspective
--- | --- | ---
**Consent and consent withdrawal (Chapter II, Clause 6)**
- Consent given should be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and signify an agreement to the processing of personal data.
- Any part of consent referred to in this bill, which constitutes an infringement of the provisions of this bill, or the rules made thereunder or any other law, for the time being, in force shall be invalid to the extent of such an infringement.
- Request for consent to be presented in English or any language specified in the eighth schedule of the constitution.
- Data principal shall have the right to withdraw the consent at any time.
- Upon withdrawal of consent, the data fiduciary shall cease processing the personal data of data principal unless such processing is required.

- Through consent, organisations acknowledge the rightful ownership of personal data processing. Therefore, organisation need to ensure that the process of withdrawing consent is as easy as it is to obtain one.
- Upon the withdrawal of consent, organisations must ensure that appropriate actions are taken by processors that are processing the data on their behalf.
- Non-compliance by the processor will be considered non-compliance by the data fiduciary as the Bill does not place a direct obligation on data processors.
# Data principal’s rights and duties

<table>
<thead>
<tr>
<th>Reference to the Bill</th>
<th>Key highlights</th>
<th>Our perspective</th>
</tr>
</thead>
</table>
| **Rights and duties of data principal (Chapter III)** | • Right to access information about personal data  
  • Right to correction, completion, updation and erasure of personal data  
  • Right of grievance redressal  
  • Right to nominate | • These rights echo the core theme of the Bill as it empowers individuals to have control over their information and how it is collected, processed, and shared by organisations.  
  • Organisations need to establish processes and mechanisms to handle and respond to the right requests.  
  • The Bill will foster trust, accountability and positive relationships with employees/customers. |
| Rights of data principal | | |
| **Data principal shall perform the following duties while exercising the rights:** | • Not to suppress any material information while providing personal data for any document, unique identifier, proof of identity or proof of address.  
  • Not to register a false or frivolous grievance or complaint.  
  • Furnish only information which is verifiably authentic.  
  • Comply with the provisions of all applicable laws for the time being in force.  
  • Not to impersonate another person while providing her personal data for a specified purpose. | • The duties of data subjects involve responsible and informed behaviour when it comes to sharing, protecting and exercising control over their personal data.  
  • By embracing these duties, a data principal can have an active participation in shaping the privacy ecosystem where rights are balanced with responsibilities. |
| Duties of data principal | | |
## Reference to the Bill | Key highlights | Our perspective
---|---|---
**Notice**  
(Chapter II, Clause 5) | • The notice should contain details about personal data which is to be collected, the purpose of processing, rights of the data principal and the way in which the rights can be exercised.  
• A similar notice should also, as soon as ‘reasonably practicable’ be provided to the data principal when consent was obtained before the commencement of the Bill. The timeline of lookback period has not been provided.  
• The option to access the contents of the notice should be in English or any language specified in the Eighth Schedule to the Constitution. | • Organisations can utilise this opportunity to demonstrate transparency and help the data principal to make an informed decision about the processing of their personal data. This notice helps in educating the data principal on common scenarios they might encounter, rectify inaccuracies or withdraw consent. |
**Grounds of processing personal data**  
(Chapter II, Clause 4 and Clause 7) | • For lawful purpose after obtaining consent of the data principal or for certain legitimate uses.  
**These legitimate cases include:**  
1. Voluntarily provided personal data by data principal.  
2. Data principal has not indicated ‘does not consent’ to use personal data.  
3. By the state and any of its instrumentalities for any function under any law for the time being in force in India.  
4. For matters concerning public interest, e.g., medical emergency, judicial use.  
5. For the purposes of employment or those related to safeguarding the employer from loss or liability. | • The Bill mentions consent and certain legitimate use as primary grounds for processing personal data.  
• Organisations which collect voluminous personal data can leverage technology solutions for consent mechanisms.  
• Organisations need to create data privacy notices that categorically indicate to the data principal if they wish to restrict usage of their personal data else the data fiduciary may legitimately process such data where consent is not provided. |
## Data fiduciary’s obligations

<table>
<thead>
<tr>
<th>Reference to the Bill</th>
<th>Key highlights</th>
<th>Our perspective</th>
</tr>
</thead>
</table>
| Consent manager (Chapter II, Clause 6) | • The data principal may give, manage, review or withdraw consent through a consent manager.  
• The consent manager shall be accountable to the data principal and shall act on their behalf.  
• The consent manager shall be registered with the board.  
• Consent managers can also make complaints to the board on behalf of the data principal, and are subject to inquiry by the board in the event of breach of any of their registration conditions. | • Consent managers will act as a bridge between legitimate processing by organisation and upholding data principal rights.  
• Apart from organisations (data fiduciary) consent managers will keep record when consent was obtained, its purpose and circumstances.  
• Consent managers should facilitate periodic reviews and refreshing of consent wherever applicable. |
## Data fiduciary’s obligations

<table>
<thead>
<tr>
<th>Reference to the Bill</th>
<th>Key highlights</th>
<th>Our perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security safeguards</strong>&lt;br&gt;and data processor obligation&lt;br&gt;(Chapter II, Clause 8)</td>
<td>• A data fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of the Bill.&lt;br&gt; • A data fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by the data processor or on data fiduciary’s behalf by a data processor, by taking reasonable security safeguards to prevent personal data breach as the Bill does not directly impose any obligation on data processors.</td>
<td>• Organisations need to have robust monitoring systems in place that should extend beyond technology to people and processes for defending the data against threats.</td>
</tr>
<tr>
<td><strong>Data retention</strong>&lt;br&gt;(Chapter II, Clause 8)</td>
<td>• A data fiduciary shall, unless retention is necessary for compliance with any law, erase personal data upon the data principal withdrawing his/her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier.</td>
<td>• This is to ensure a balance between historical relevance, regulatory compliance and privacy concerns.&lt;br&gt; • This also makes sure that the information is easily accessible for legal purposes.&lt;br&gt; • Data processor processing on behalf of a data fiduciary must also delete such data on receiving the written instructions of data fiduciary.</td>
</tr>
<tr>
<td><strong>Data breach notification</strong>&lt;br&gt;(Chapter II, Clause 8)</td>
<td>• Data fiduciary to take reasonable security safeguards to prevent personal data breach.&lt;br&gt; • In the event of a personal data breach, the data fiduciary shall give the board and each affected data principal, intimation of such a breach in such form and manner as may be prescribed.</td>
<td>• The Bill does not specify any time period in which the data fiduciary and data subject needs to be informed, however, considering its significance we can infer reporting needs to be done ‘at the earliest’.&lt;br&gt; • Data subjects will not be kept in the dark about the breach and this would bring in the required transparency.</td>
</tr>
</tbody>
</table>
# Data fiduciary’s obligations

## Reference to the Bill | Key highlights | Our perspective
--- | --- | ---
Guardian consent and processing children’s personal data (Chapter II, Clause 9) | • Before processing any personal data of a child or a person with disability who has a lawful guardian, verifiable consent of the parent of such a child or the lawful guardian is required to be taken.  
• A data fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.  
• A data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children. | • Guardian/parental consent would help in creating more awareness, along with an additional layer of safeguarding to protect children from online risks.  
• Organisations must put in place measures to authenticate/verify the identity of a parent/guardian.  
• This would further help the cause of protecting children in the Indian digital space and ensure a standard practice and enhance the level of security. |

Guardian consent and children data processing

## Additional obligations of significant data fiduciary (SDF) (Chapter II, Clause 9)

### Right to correction and erasure of personal data

<table>
<thead>
<tr>
<th>Additional obligations of significant data fiduciary</th>
<th>Data privacy impact assessments</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent data audits</td>
<td>Data protection officer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Such an SDF shall:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• appoint a Data Protection Officer</td>
<td></td>
</tr>
<tr>
<td>• appoint an Independent Data Auditor</td>
<td></td>
</tr>
<tr>
<td>• undertake compliance measures including Data Protection Impact Assessment.</td>
<td></td>
</tr>
</tbody>
</table>

• The Central Government may notify any data fiduciary as an SDF based on the assessment of relevant factors such as the volume and sensitivity of personal data processed, risk to the rights of data principal and the potential impact on the integrity of India.

• The Bill introduces additional obligations of a significant data fiduciary as they process data which merits higher protection due to its sensitive nature.

• Unauthorised disclosure of such data would create significant risks to the fundamental rights and freedom of data principals.
# Data fiduciary’s obligations

<table>
<thead>
<tr>
<th>Reference to the Bill</th>
<th>Key highlights</th>
<th>Our perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data processor engagement</strong>&lt;br&gt;(Chapter II, Clause 8)</td>
<td>- A data fiduciary may engage, appoint, use or otherwise involve a data processor to process personal data on its behalf for any activity related to offering of goods or services to data principals only under a valid contract.</td>
<td>- Data fiduciary must ensure that the data processors who are engaged with them have appropriate safeguards in place.</td>
</tr>
<tr>
<td></td>
<td>- Data processor must ensure that the data processors who are engaged with them have appropriate safeguards in place.</td>
<td>- Data fiduciary must consider carrying out a privacy risk assessment and closing out the identified gaps prior to onboarding a data processor.</td>
</tr>
<tr>
<td></td>
<td>- Data processor must consider carrying out a privacy risk assessment and closing out the identified gaps prior to onboarding a data processor.</td>
<td>- Data fiduciary, during the engagement with data processor, must implement appropriate monitoring mechanisms, e.g., third party audits.</td>
</tr>
<tr>
<td></td>
<td>- Data processor must consider carrying out a privacy risk assessment and closing out the identified gaps prior to onboarding a data processor.</td>
<td>- Data processor must consider carrying out a privacy risk assessment and closing out the identified gaps prior to onboarding a data processor.</td>
</tr>
<tr>
<td><strong>Processing personal data outside India</strong>&lt;br&gt;(Chapter IV, Clause 16)</td>
<td>- Government by notification, can restrict the transfer of personal data by a data fiduciary for processing to a country or territory outside India.</td>
<td>- Cross-border transfers are allowed unless restricted by the government.</td>
</tr>
<tr>
<td></td>
<td>- Personal data of data principals not within the territory of India can be processed pursuant to any contract entered with such person outside the territory of India this is listed as an exemption in the Bill.</td>
<td>- If data is being moved to a country that gets restricted, immediate action should be taken to stop the data transfer.</td>
</tr>
<tr>
<td></td>
<td>- Personal data of data principals not within the territory of India can be processed pursuant to any contract entered with such person outside the territory of India this is listed as an exemption in the Bill.</td>
<td>- The listed exemption would help IT/ITeS companies to continue their business as usual with minimal impact.</td>
</tr>
<tr>
<td></td>
<td>- The Bill also clarifies that if any other existing Indian law provides for a higher degree of regulation with respect to transfer of personal data outside India, then such regulations will take precedence, e.g., requirement of storage of payment system data within the country as mandated by the Reserve Bank of India (RBI).</td>
<td>- The Bill also clarifies that if any other existing Indian law provides for a higher degree of regulation with respect to transfer of personal data outside India, then such regulations will take precedence, e.g., requirement of storage of payment system data within the country as mandated by the Reserve Bank of India (RBI).</td>
</tr>
</tbody>
</table>
Penalties for non-compliance
Proposed penalties for data privacy breach in the DPDP Bill 2023

**Major penalties**

01

The Data Protection Board has the power to issue penalties up to **INR 250 crore.**

02

Data fiduciaries are liable to pay a penalty up to **INR 250 crore** for breach in observing the obligation of Data fiduciary to take reasonable security safeguards to prevent personal data breach.

**Penalty on data principal**

**Breach in observance of the duties of data principal**

Non-compliance shall lead to a penalty of **INR 10,000.**

**Other penalties**

Breach in observing the obligation to give the board or affected data principal notice of a personal data breach.

Non-compliance in this case shall lead to a penalty of **INR 200 crore.**

Breach in observance of additional obligations of significant data fiduciary

Non-compliance shall lead to a penalty of **INR 150 crore.**

Breach in observance of additional obligations in relation to children

Non-compliance shall lead to a penalty of **INR 200 crore.**

Breach of any other provision of this Act or the rules made thereunder

Non-compliance shall lead to a penalty of **INR 50 crore.**
Way forward for organisations
Step 1: Assess the current state and start building data privacy within the organisation

**Key actions**

1. **Assess the current state and start building a data privacy organisation.**
   - Assess your current maturity with the DPDP Bill’s requirements and develop an action plan for compliance. The action plan can be bifurcated into short terms and medium-terms covering governance, technology, people and processes initiatives.
   - Initiate the implementation of an identified action plan.
   - Set up privacy organisation which might consist of a Data Protection Officer (DPO), representatives of various functions along with their roles and responsibilities.

2. **Prepare an inventory of applications/data stores that houses personal data.**
   - Identify key applications/databases which are used to store/process personal data.
   - Identify whether these applications are directly capturing personal data from data principals, or if these are downstream applications (this information will be used to apply data privacy controls such as privacy notice, consent, etc.).

3. **Identify the ecosystem of data processors which are currently being leveraged.**
   - Identify all third parties including service providers who are storing or processing personal data on behalf of an organisation. The data fiduciary will need to amend the third-party agreements/contracts with respect to their obligations and connect with data processors and communicate to them about their upcoming responsibilities and obligations with respect to personal data they are handling on the data fiduciary’s behalf.

**Key activities to be performed**

- Prepare an inventory of applications/data stores that houses personal data.
- Identify the ecosystem of data processors which are currently being leveraged.

Note: Organisations who will be classified as significant data fiduciary may have to take additional actions such as Independent Data Audits, DPIA to comply with the provisions of the Bill.
## Step 2: Take first-level measures to establish mechanisms

<table>
<thead>
<tr>
<th>Key actions</th>
<th>Key activities to be performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design draft versions of documents based on the requirements of the DPDP Bill (policies, processes, notice, consent, contractual clauses).</td>
<td>• Prepare approved versions of documents which can be released as soon as DPDP becomes a law, e.g., data privacy policy and supporting processes.</td>
</tr>
<tr>
<td>Design consent mechanisms based on application inventory gathered from earlier phases.</td>
<td>• Update data privacy policies and processes.</td>
</tr>
<tr>
<td>Design data principal's rights mechanisms to uphold the rights provided as per the provisions of the Bill.</td>
<td>• Prepare content around privacy notices and consent.</td>
</tr>
<tr>
<td>Establish data breach notification and management mechanisms.</td>
<td>• Define standard contractual clauses which are to be embedded in various agreements, such as data processing agreements with third parties, contractual vendors/service providers, etc.</td>
</tr>
<tr>
<td>• Determine the consent types which are based on the applications gathering personal data directly from data principals.</td>
<td>• Implement mechanisms that require individuals to take clear, affirmative action to provide consent.</td>
</tr>
<tr>
<td>• Design consent mechanisms to offer choices and options to data principals.</td>
<td>• Determine tools that can be leveraged to facilitate the collection, management and documentation of consent.</td>
</tr>
<tr>
<td>• Establish processes to address various rights which have been provided to data principals.</td>
<td>• Establish processes for data privacy breach management, including notifications to stakeholders (data principals, data protection board).</td>
</tr>
<tr>
<td>• Prepare procedures to determine how the request shall be accepted, validated and responded to the data principals.</td>
<td>• Integrate these breach management mechanisms with existing incident management processes.</td>
</tr>
</tbody>
</table>
Step 3: Take next level measures to ensure data protection

Key actions

- Define the data retention period for various categories of data.
- Evaluate, agree and implement data privacy technologies that can be leveraged for data protection.
- Conduct communication and awareness programmes for various stakeholders.
- Refer to the notifications and amendments made by the central government.

Key activities to be performed

- Categorise different types of data in relation to the retention period based on the inventory gathered.
- Assess business/operational/legal requirements for the category.
- Determine the minimum necessary retention period for each category based on these requirements.
- Determine the privacy technology solutions that can be leveraged to address specific privacy needs, e.g., automating data principal rights, conducting data protection impact assessments.
- Evaluate the measures provided by the privacy technology solutions.
- Assess the compatibility and scalability of privacy technology solutions with the existing IT infrastructure.
- Make an informed decision and begin the implementation.
- Develop communications and awareness plans.
- Design engaging communication and awareness material.
- Launch awareness programmes.
- Leverage multiple channels of communication.
- Provide training and awareness sessions to different stakeholders.
- Refer to recent notifications and amendments made by the central government and take appropriate action, e.g., notification from the government on countries or territories outside India where data transfers would be restricted.
Contact us

Sivarama Krishnan
Partner and Leader, Risk Consulting, PwC India, and Leader of APAC Cyber Security and Privacy, PwC
Email: sivarama.krishnan@pwc.com

Anirban Sengupta
Partner and Leader – Business Risk Consulting, PwC India
Email: anirban.sengupta@pwc.com

Sundareshwar Krishnamurthy
Partner and Leader – Cybersecurity, PwC India
Email: sundareshwar.krishnamurthy@pwc.com

Heena Vazirani
Partner, Business Risk Consulting, PwC India
Email: heena.vazirani@pwc.com
Thank you