THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Summary of Provisions and Implementation Approach

PREPARED BY

Risk · Pro

Table of Contents

1 INTRODUCTION

After a long wait, India's Digital Personal Data Protection Act is passed. The bill received presidential assent on August 11th 2023 for it to become the law.

This is a concise and simply written document, accompanied by practical examples/illustrations. It's a welcome departure from the prescriptive approaches to personal data protection legislations till now.

This report provides summary of provisions and suggested implementation approach.

2 PROVISIONS SIMPLIFIED

2.1 Chapter I: PRELIMINARY

2.1.1 Applicability of the Act

- The Act applies to processing of "digital" personal data which includes
  - the data collected online, or
  - the data collected offline but digitized subsequently within the Indian territory.
- The Act also applies to processing of personal data outside India goods and services are offered to Data Principals within the territory of India.
- **Act does not apply to:**
  - The processing of any personal data by individuals for personal or domestic purpose and personal data made available publicly by Data Principal or any other individual.

2.1.2 Key definitions

Term	Definition
Automated	Any digital process that can run automatically in response to commands or in another way for the purpose of processing data.
Board	Data Protection Board of India established by the Central Government under section 18.
Child	Individual who has not completed the age of eighteen years.
Consent Manager	A person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform.
Data	A representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation, or processing by human beings or by automated means.
Data Fiduciary	Any person who alone or jointly with other persons determines the purpose and means of processing of personal data.
Data Principal	Individual to whom the personal data relates and where such individual is: • a child, includes the parents or lawful guardian of such a child;

Term	Definition
	• a person with disability, includes her lawful guardian, acting on her behalf.
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary.
Data Protection Officer	Individual appointed by the Significant Data Fiduciary
Digital Personal Data	Personal data in digital form
Personal data	Any data about an individual who is identifiable by or in relation to such data.
Person	Person includes— (i) an individual; (ii) a Hindu undivided family; (iii) a company; (iv) a firm; (v) an association of persons or a body of individuals, whether incorporated or not; (vi)the State; and (vii) every artificial juristic person, not falling within any of the preceding sub-clauses.
Personal data breach	Any unauthorised processing of personal data or an unintentional acquisition, sharing, use, alteration, destruction, or loss of access to personal data that jeopardies its integrity, confidentiality, or availability.
Processing	**Processing** in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment, or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
Significant Data Fiduciary	Any Data Fiduciary or class of Data Fiduciaries may be notified by the Central Government under section 10.

2.1.3 Implementation Approach

- Understanding the definitions and applicability.
- Systematic identification of data processed by each product, business process, website, internal department, source & purpose of the data, and flow of the data would be the key to building a robust data inventory. This could be the basis for further implementation.
- There could also be certain services that are not fully digitized – the data is collected through paper-based forms and later keyed into the systems – Organizations must also identify such processes and data.

2.1.4 Chapter II: OBLIGATIONS OF DATA FIDUCIARY

2.1.5 Summary of Provisions

Obligations of Data Fiduciary primarily include:

- Establishing grounds for processing of personal data. .
- Serving Privacy Notice before or at the time of taking the consent. Privacy Notice should also be served to those individuals whose data is being processed on basis of consent but a notice was not served in past.
- Providing Data Principals option to access the notice and the request to consent in English or any language specified in the Eighth Schedule to the Constitution.
- Ensuring that the Consent is free, specific, informed, unconditional and unambiguous with a clear affirmative action.
- Establishing an effective mechanism to redress the grievances of Data Principals.
- Ensuring availability of contract with the data processor.
- Ensuring completeness, accuracy and consistency of personal data.
- Liability to protect the data either processed by Data Fiduciary or by Data processor would be upon Data Fiduciary.
- In case of data breach, Data Fiduciary would be required to serve Breach Notification to the Board and the affected Data Principal.
- Ensuring erasure of the data once the consent is withdrawn.
- Obtaining verifiable consent from parent/lawful guardian before processing any personal data of a child or a person with disability.
- **Additional obligations of Significant Data Fiduciary:**
    - Data Protection Officer shall be appointed who shall be based in India.
    - Data Protection Officer shall be the point of contact for the grievance redressal mechanism.
    - Independent data auditor shall be appointed.
    - Periodic Data Protection Impact Assessment and Periodic Audit shall be performed.

2.1.6 Implementation Approach

- Identify a Data protection officer (if applicable) / team for managing data privacy obligations and upskilling this team.
- Conduct organization-wide data privacy awareness program.
- Establish a robust governance framework with policies and procedures to align with expectation of this Act, periodic audits, and reviews by the management.
- Review current Privacy Notices and Consent against the requirements of the Act. Evaluate Consent Management Platforms.
- Identify lawful basis for each processing; Document legitimate interest assessment where the data is processed based on legitimate interest.
- Establish effective mechanism for grievance redressal and data subject request management

- Implement appropriate technical and organisational measures based on the risk/data protection impact assessment.
- Review data under retention. Data should be erased when the purpose of collection of data is fulfilled.
- Additional precautionary measures should be taken while processing the data of children.
- Data should not be transferred to a territory outside India if transfer of data to such country is restricted by Government of India.

2.1.7 Chapter III: RIGHTS AND DUTIES OF DATA PRINCIPAL

2.1.8 Summary of Provisions

2.1.8.1 Rights of the Data Principal

- The rights of the Data Principal include the following:
  - Right to access information about personal data
  - Right to correction and erasure of personal data
  - Right of grievance redressal
  - Right to nominate
    - The data principal has the right to nominate any other individual, who in the event of death / inability (unsoundness of mind or infirmity of body) of the data principal, could exercise the rights guaranteed under the Act.

2.1.8.2 Duties of the Data Principal

- Duties of the Data Principal include the following:
  - Compliance with all the applicable laws of India while performing the Rights mentioned in the Act.
  - Providing authentic information while exercising the right to correction or erasure.
  - Data Principals are prohibited from the following:
    - impersonating another individual while providing the personal data for any specified purposes.
    - Hiding/omitting any personal information while providing personal data for any document, unique identifier, proof of identity or proof of address issued by the State.
    - Registering a false grievance or complaint with a Data Fiduciary or the Board

2.1.9 Implementation Approach

- Inform the data principals of their rights under the Act, through the Privacy Notice.
- Document a Data Principal Rights Policy and Supporting Documents.
- Establish system and process for grievance redressal and effectively management of Data principals requests.

2.2 Chapter IV: SPECIAL PROVISIONS

2.2.1 Summary of Provisions

- **These sections provide guidance about Processing of personal data outside India**
  - The Central Government of India may issue a notification about the countries to which data transfer is prohibited. The Act instructs against transfer of personal data to any country outside the territory of India as notified by the Central Government.
  - Any law (currently in force) in India is applicable which provides for a higher degree of protection for the transfer of personal data by a Data Fiduciary outside India in relation to any personal data.
- **Exemptions**

  Few of the provisions of the Act do not apply if:
  - the processing is necessary by any court or tribunal or any other body in India for enforcing any legal right or claim;
  - processing in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India;
  - personal data of Data Principals not within the territory of India is processed by any person based in India in accordance with a contract with any person outside the territory of India.
  - the processing is necessary for company mergers/acquisitions approved by a court or tribunal or other authority competent to do so by any law for the time being in force;
  - the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution;

  The provisions of this Act do not apply where:
  - processing is in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or preventing incitement to any cognizable offence relating to any of these;
  - processing is necessary for research, archiving, or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal
- **Few of the provisions (section 5, sub-sections (3) and (7) of section 8, and sections 10 and 11) of the Act do not apply to Data Fiduciaries or class of Data Fiduciaries, including startups on the basis of the volume and nature of personal data processed by them. The Central Government will notify such Data Fiduciaries.**

2.2.2 Implementation Approach

- Document a Cross-Border Transfer Policy and procedures once the Central Government issues a notification.
- Agreements with third parties about data transfers.

2.3 Chapter V: DATA PROTECTION BOARD OF INDIA

2.3.1 Summary of Provisions

- The Act proposes the establishment of the Data Protection Board of India, which would perform the functions as notified by the Central Government of India.
- The Board will be an independent body, functioning as a digital office by adopting the techno-legal measures as may be prescribed

  This provision is more about how the Data Protection Board will function and will not apply to individual organizations.

2.4 Chapter VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD

2.4.1 Summary of Provisions

- **Primary responsibilities of the board include:**
    - Investigation and inquiry of personal data breaches, as well as imposing urgent remedial and mitigating measures for breach containment.
    - Acknowledging violations of the Act on the receipt of a complaint filed by a data principal against a data fiduciary/consent manager, and to impose penalties.
    - Acknowledging and initiate inquiries on the violations by an intermediary, as per references made by the Central Government.
    - Taking appropriate action against any consent manager on being intimated of any breach of registration condition, and impose penalties.
    - Imposing penalties against the appropriate party as per Schedule of the Act.

2.4.2 Implementation Approach

- This provision is more about power and functions of the board as well as the procedure to be followed by the board. As such, it will not apply to individual organizations. However, the organizations must implement the procedures to communicate and cooperate with the board per the section ‘Obligations of Data Fiduciary’.

2.5 Chapter VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION

2.5.1 Summary of Provisions

- Data Principal aggrieved by an order or direction made by the Data Protection Board may want to appeal before the Appellate Tribunal. This section provides guidance about the process followed by The Appellate Tribunal
- This section also refers to the Alternate Dispute Resolution – process to resolve complaints raised by the Data Principal through mediation.

This provision lists the process to be followed for various dispute resolution mechanisms. The organizations should be aware of such provisions and execute them in case of dispute.

2.6 Chapter VIII: Penalties and Adjudication

2.6.1 Summary of Provisions

- The Act speaks about hefty penalties for failure to take reasonable security safeguards to prevent data breaches as well as non-fulfilment of certain obligations. The section refers to the Schedule in the Act –

#	Breach of Provision (Violation) of Act	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (*5*) of section 8 (General Obligations of Data Fiduciary): *A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.*	Upto two hundred and fifty crore rupees
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach. under sub-section (*6*) of section 8 (General Obligations of Data Fiduciary): *In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.*	Upto two hundred crores rupees
3	Breach in observance of additional obligations in relation to children under section 9: *The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent ofsuch child or the lawful guardian, as the case may be, in such manner as may be prescribed*	Upto two hundred crores rupees
4	Breach in observance of additional obligations of Significant Data Fiduciary under section 10 (Obligations for significant data fiduciary)	Upto one hundred and fifty crore rupees
5	The breach in observance of the duties under section 15 (Duties of the Data Principal) This will be applicable to the data principal (individual) breaching the duties. This point will not be applicable at the organization level.	Upto ten thousand rupees
6	Breach of any term of voluntary undertaking accepted by the Board under section 32.	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were. instituted.
7	Breach of any other provision of this Act or the rules made thereunder.	Upto fifty crore rupees

2.6.2 Implementation Approach

- The challenge for the organizations is to identify risks and obligations related to the data in scope and accordingly implement the safeguards. Identifying a Data protection officer, training the data protection team, and detailed data protection impact and risk assessment would help.

2.7 Chapter IX: MISCELLANEOUS

2.7.1 Summary of Provisions

- This chapter talks about power of central government to issue the directions. It will not apply to the organizations.

3 CONCLUSION

While we await for clarifications and further guidance on enforcement; it's time for the organizations to re-think their approach to personal data processing based on the obligations mandated by the law and the risks involved.

With our expertise in risk management and compliance services, Riskpro can be your Compliance Partner as you embark on this journey. To know more contact us at *info@riskpro.in*