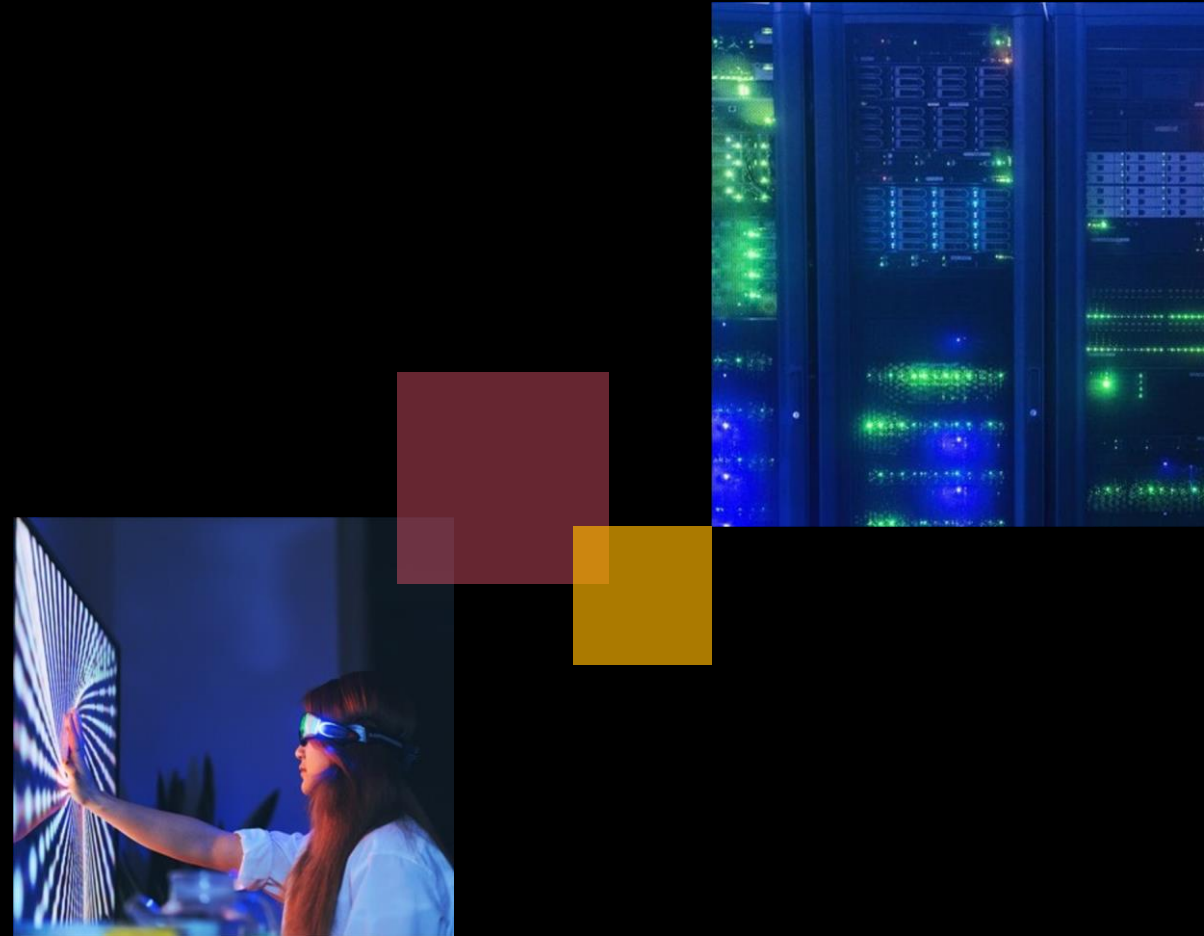




The Digital Personal Data Protection Act, 2023

Contents

1. Introduction
2. Key tenets of the DPDP Act 2023
3. Our perspective on the key tenets
4. Penalties for non-compliance
5. Way forward for organisations



Introduction

01

The Digital Personal Data Protection Act 2023

The Act applies to

01

within the Indian territory



to the processing of digital personal data within the territory of India, where the personal data is collected in a:

01 a) digital form



01 b) personal data collected is in non-digital form and digitised subsequently.

02

outside the Indian territory



to processing of digital personal data outside the territory of India, if such processing is in connection with:

02 a) any activity related to offering of goods or services to data principals within the territory of India.

The Act 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.

The Act is an attempt to bring a **harmonised data privacy** regime in India.



Digital personal data means personal data in digital form.



The Act 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 crore for data fiduciary** and the **Act does not impose criminal penalty** for non-compliance.



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







The Act 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 Act
2023

02

Key tenets of the DPDP Act 2023

Data lifecycle	 Data collection	 Data processing	 Data storage/transfer	 Transparency and accountability			
Data principal	Consent and consent withdrawals		Right to access information about personal data	Right to correction of personal data	Right to erasure	Right to grievance redressal and nominate	Duties of data principal
Data fiduciary	Notice	Grounds of processing personal data	Certain legitimate uses	Security safeguards	Data fiduciary accountable for data processor	Data privacy impact assessments	
	Verifiable parent/guardian consent	Additional obligations of significant data fiduciary	Data processor engagement	Data retention	Data protection officer	Independent data audits	
			Personal data breach notification	Processing of personal data outside India	Consent managers	Complying to government notifications	
Data Protection Board of India							
Penalty		Grievance redressal		Review and appeal		Dispute resolution	

Our perspective

on the key tenets

03

Data principal's rights and duties

Reference to the Act	Key highlights	Our perspective
Consent and consent withdrawal (Chapter II, Clause 6)	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Through consent, organisations acknowledge the rightful ownership of personal data processing. Therefore, organisations need to ensure that the process of withdrawing consent is as easy as it is to obtain one.
Consent and consent withdrawals	<p>infringement of the provisions of this act, 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.</p> <p>in the eighth schedule of the constitution.</p> <ul style="list-style-type: none">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.	<ul style="list-style-type: none">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 Act does not place a direct obligation on data processors.

Data principal's rights and duties

Reference to the Act	Key highlights	Our perspective
Rights and duties of data principal (Chapter III) Rights of data principal	<ul style="list-style-type: none">• Right to access information about personal data• Right to correction, completion, updation and erasure of personal data• Right of grievance redressal• Right to nominate	<ul style="list-style-type: none">• These rights echo the core theme of the Act 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 Act will foster trust, accountability and positive relationships with employees/customers.
Rights and duties of data principal (Chapter III) Duties of data principal	<p>Data principal shall perform the following duties while exercising the rights:</p> <p>any document, unique identifier, proof of identity or proof of address.</p> <ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.

Data fiduciary's obligations

Reference to the Act	Key highlights	Our perspective
Notice (Chapter II, Clause 5)	<ul style="list-style-type: none">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 Act. 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.	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">For lawful purpose after obtaining consent of the data principal or for certain legitimate uses. <p>These legitimate cases include:</p> <ol style="list-style-type: none">Voluntarily provided personal data by data principal.Data principal has not indicated 'does not consent' to use personal data.By the state and any of its instrumentalities for any function under any law for the time being in force in India.For matters concerning public interest, e.g., medical emergency, judicial use.For the purposes of employment or those related to safeguarding the employer from loss or liability.	<ul style="list-style-type: none">The Act 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

Reference to the Act	Key highlights	Our perspective
Consent manager (Chapter II, Clause 6) Consent managers	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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

Data fiduciary's obligations

Reference to the Act		Key highlights	Our perspective
Security safeguards and data processor obligation (Chapter II, Clause 8)		<ul style="list-style-type: none">A data fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of the Act.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 Act does not directly impose any obligation on data processors.	<ul style="list-style-type: none">Organisations need to have robust monitoring systems in place that should extend beyond technology to people and processes for defending their data against threats.
Security safeguards	Data fiduciary accountable for data processor		
Data retention (Chapter II, Clause 8)		<ul style="list-style-type: none">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.	<ul style="list-style-type: none">This is to ensure a balance between historical relevance, regulatory compliance and privacy concerns.This also makes sure that the information is easily accessible for legal purposes.Data processor processing on behalf of a data fiduciary must also delete such data on receiving the written instructions of the data fiduciary.
Data retention			
Data breach notification (Chapter II, Clause 8)		<ul style="list-style-type: none">Data fiduciary to take reasonable security safeguards to prevent personal data breach.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.	<ul style="list-style-type: none">The Act 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’.Data subjects will not be kept in the dark about the breach and this would bring in the required transparency.
Personal data breach notification			

Data fiduciary's obligations

Reference to the Act		Key highlights	Our perspective
Guardian consent and processing children’s personal data (Chapter II, Clause 9)		<ul style="list-style-type: none">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 targetted advertising directed at children.	<ul style="list-style-type: none">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’s data processing			
Additional obligations of significant data fiduciary (SDF) (Chapter II, Clause 9) Right to correction and erasure of personal data		<ul style="list-style-type: none">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. <p>Such an SDF shall:</p> <ul style="list-style-type: none">appoint a Data Protection Officerappoint an Independent Data Auditorundertake compliance measures including Data Protection Impact Assessment (DPIA).	<ul style="list-style-type: none">The Act 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.DPO should be able to perform their duties and tasks in an independent manner. They should directly report to the highest management level of the organization.As board’s primary functions include inquiring breaches, directing measures and imposing penalties hence Data Fiduciary must appropriately respond to board's inquiry request.
Additional obligations of significant data fiduciary	Data privacy impact assessments		
Independent data audits	Data protection officer		

Data fiduciary's obligations

Reference to the Act	Key highlights	Our perspective
Data processor engagement (Chapter II, Clause 8) Data processor engagement	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Data fiduciary must ensure that the data processors who are engaged with them have appropriate safeguards in place.Data fiduciary must consider carrying out a privacy risk assessment and closing out the identified gaps prior to onboarding a data processor.Data fiduciary, during the engagement with data processor, must implement appropriate monitoring mechanisms, e.g., third party audits.
Processing personal data outside India (Chapter IV, Clause 16) Processing of personal data outside India	<ul style="list-style-type: none">The Government by notification, can restrict the transfer of personal data by a data fiduciary for processing to a country or territory outside India.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 Act.	<ul style="list-style-type: none">Cross-border transfers are allowed unless restricted by the Government.If data is being moved to a country that gets restricted, immediate action should be taken to stop the data transfer.The listed exemption would help IT/ITes companies to continue their business as usual with minimal impact.The Act 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).

Penalties for non-

compliance

04

Proposed penalties for data privacy breach in the DPDP Act 2023

Major penalties

Other 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 a 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

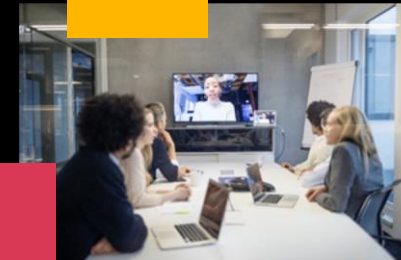
Non-compliance shall lead to a penalty of **INR 10,000**.

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 the observance of the additional obligations of a 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




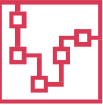
05

Step 1: Assess the current state and start building data privacy within the organisation





Key actions	Key activities to be performed
 Assess the current state and start building data privacy within the organisation.	<ul style="list-style-type: none">• Assess your current maturity with the DPDP Act's requirements and develop an action plan for compliance. The action plan can be bifurcated into short term and medium-term plans 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.
 Prepare an inventory of applications/data stores that houses personal data.	<ul style="list-style-type: none">• 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.).
 Identify the ecosystem of data processors which are currently being leveraged.	<ul style="list-style-type: none">• 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 their upcoming responsibilities and obligations with respect to personal data which they are handling on the data fiduciary's behalf.

Note: Organisations who will be classified as significant data fiduciary may have to take additional actions such as Independent Data Audits and DPIA to comply with the provisions of the Act.

Step 2: Take first-level measures to establish mechanisms

Key actions	Key activities to be performed
 Design draft versions of documents based on the requirements of the DPDP Act (policies, processes, notice, consent, contractual clauses).	<ul style="list-style-type: none">• Prepare approved versions of documents such as data privacy policy and supporting processes.• Update data privacy policies and processes• Prepare content around privacy notices and consent• 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.
 Design consent mechanisms based on application inventory gathered from earlier phases.	<ul style="list-style-type: none">• Determine the consent types which are based on the applications gathering personal data directly from data principals.• Design consent mechanisms to offer choices and options to data principals.• Implement mechanisms that require individuals to take clear, affirmative action to provide consent.• Determine tools that can be leveraged to facilitate the collection, management and documentation of consent.
 Design data principal's rights mechanisms to uphold the rights provided as per the provisions of the Act.	<ul style="list-style-type: none">• Establish processes to address various rights which have been provided to data principals.• Prepare procedures to determine how the request shall be accepted, validated and responded to, to the data principals.• Determine tools that can be leveraged to facilitate the data principal rights management
 Establish data breach notification and management mechanisms.	<ul style="list-style-type: none">• Establish processes for data privacy breach management, including notifications to stakeholders (data principals, data protection board).• Integrate these breach management mechanisms with existing incident management processes.

Step 3: Take next level measures to ensure data protection

Key actions	Key activities to be performed
 Define the data retention period for various categories of data.	<ul style="list-style-type: none">• 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.
 Evaluate, agree to and implement data privacy technologies that can be leveraged for data protection.	<ul style="list-style-type: none">• 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 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 process.
 Conduct communication and awareness programmes for various stakeholders.	<ul style="list-style-type: none">• 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 the notifications and amendments made by the Central Government.	<ul style="list-style-type: none">• 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.

Thank you

