

Handbook on The Digital Personal Data Protection Act, 2023

Compiled and Edited By:



MOHIT KHANDELWAL & ASSOCIATES, JAIPUR
(ADVOCATES & CONSULTANTS)

IN ASSOCIATION WITH



**RAJASTHAN HIGH COURT BAR ASSOCIATION,
JAIPUR**

Rajeev Sogarwal
(President)

Deepesh Sharma
(General Secretary)

and other office bearers

Disclaimer

Please Note

- This handbook is intended solely for educational and informational purposes and does not constitute legal advice.
- Readers should refer to the Digital Personal Data Protection Act, 2023, applicable Rules, notifications, and professional legal advisers for guidance on specific legal or compliance matters.

Table of Contents

I.	Introduction	1
II.	Evolution of India's Data Protection Framework	1
III.	Understanding the DPDP Act, 2023	2
IV.	Fundamental Principles of the DPDP Act, 2023	4
V.	Important Definitions under the DPDP Act, 2023	6
VI.	International Perspective - GDPR	9
VII.	Applicability and Scope of the DPDP Act, 2023	11
VIII.	Rights and Duties of Data Principals	13
IX.	Data Fiduciaries	16
X.	Significant Data Fiduciaries	19
XI.	Cross-Border Transfer of Personal Data	22
XII.	Exemptions under the DPDP Act	22
XIII.	Legitimate Uses	23
XIV.	Consent Manager	25
XV.	Children's Personal Data	28
XVI.	Personal Data Breach and Penalties	30
XVII.	Data Protection Board of India	33
XVIII.	DPDP Act, 2023 - Compliance Checklist	37
XIX.	From the Editor's Desk	40

Introduction

In today's digital world, huge quantity of personal data is being rapidly collected, stored, transferred and processed, underscoring the need to develop a robust data protection mechanism digitally. The Digital Personal Data Protection Act, 2023 ("DPDP Act") introduces India's first dedicated framework, aiming to balance individual privacy rights with legitimate lawful exemptions.

This handbook provides a concise and practical overview of the DPDP Act, 2023 and the DPDP Rules, 2025, outlining the key concepts, stakeholder responsibilities, compliance requirements, and regulatory framework in a simple and reader-friendly manner. It is intended to serve as a quick reference for students, legal professionals, business organisations and anyone seeking to understand India's data protection regime.

Concepts

Plain-language explanations of the Act's stakeholders, principles and terminology.

Compliance

Rule-by-rule operational detail drawn from the DPDP Rules, 2025.

Practical Guidance

Checklists, roadmaps and worked examples for real-world application.

Evolution of India's Data Protection Framework

The systemic evolution of Data Protection laws and regulations in India was the need of the hour amid the rapid growth of Digital Economy, coupled with the dire need of safeguarding the Right to Privacy of citizens given the evolving paradigm shift in the global landscape concerning use of Data. A comprehensive legal framework was required to deal with the widespread use of digital technologies, e-commerce, social media, cloud computing, and artificial intelligence.

The Hon'ble Supreme Court in *Justice K.S. Puttaswamy (Retd.) versus Union of India, 2017 10 SCC 1*, recognised the Right to Privacy as a fundamental right under Article 21 of the Constitution of India. In pursuance of this, the Justice B.N. Srikrishna Committee was constituted aimed at examining the issues pertaining to data protection. The Committee submitted its report along with the Personal Data Protection Bill, 2018, which served as the first comprehensive proposal for regulating personal data in India. Thereafter, the Personal Data Protection Bill, 2019 was introduced which underwent extensive parliamentary scrutiny and stakeholder consultations. In 2022, the Government withdrew the Bill and came up with a simplified Digital Personal Data Protection Bill, 2022 for public consultation.

Accordingly, the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 were introduced dealing with the vital legal aspects of Data protection while also ensuring that the requisite regulatory and procedural framework is established to ensure compliance and ground level improvements.

Key Milestones in the Evolution of India's Data Protection Framework

Year	Milestone
24.08.2017	<i>Justice K.S. Puttaswamy (Retd.)</i> versus Union of India - Right to Privacy recognised as a fundamental right under Article 21 of the Constitution of India.
27.07.2018	Justice B.N. Srikrishna Committee Report and the Personal Data Protection Bill, 2018 introduced.
11.12.2019	Personal Data Protection Bill, 2019 introduced in Parliament for scrutiny and consultation.
03.08.2022	Personal Data Protection Bill, 2019 withdrawn.
18.11.2022	Digital Personal Data Protection Bill, 2022 released for public consultation
11.08.2023	Digital Personal Data Protection Act, 2023 (Act. No. 22 of 2023) receives Presidential assent.
13.11.2025	Digital Personal Data Protection Rules, 2025 notified with the Gazette Notification No. G.S.R.846(E)

The DPDP Act is a significant step towards building a privacy-centric and trusted digital ecosystem in India. It reflects the country's commitment to safeguarding personal data while promoting innovation, digital governance, and economic growth in an increasingly data-driven world.

Understanding the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDP Act") is India's first comprehensive legislation governing the processing of digital personal data. Enacted to address the growing concerns surrounding privacy in an increasingly digital world, the Act establishes a legal framework that balances an individual's right to protect personal data with the need for organisations to process such data for lawful purposes.

Building upon the constitutional foundation established by the Supreme Court in 2017, the DPDP Act seeks to foster a trusted digital ecosystem by prescribing clear rights for individuals / data principals and corresponding obligations for organisations that retain/process and handle digital personal data.

The Key Stakeholders

The DPDP Act operates through four principal categories of stakeholders:

Data Principal

The individuals to whom the personal data relates.

Data Fiduciary

The person (natural or juristic) that determines the purpose and means of processing personal data.

<p>Data Processor</p> <p>The person (natural or juristic) that processes personal data on behalf of a Data Fiduciary.</p>	<p>Consent Manager</p> <p>A person registered with the Data Protection Board who enables Data Principals to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform.</p>
<p>Significant Data Fiduciaries (SDF)</p> <p>A Data Fiduciary notified as such by the Central Government under Section 10, based on specified factors and subject to additional compliance obligations.</p>	<p>Data Protection Board of India</p> <p>The statutory body responsible for inquiring into breaches, exercising powers and performing functions assigned under the DPDP Act, including imposing monetary penalties and issuing directions.</p>
<p>Authorised Person</p> <p>A person or entity authorised under the applicable provisions of the DPDP Rules to make or receive specified requests or access information for the purposes prescribed under the Rules.</p>	<p>Data Protection Officer (DPO)</p> <p>A person appointed by a Significant Data Fiduciary under Section 10 of the DPDP Act. The DPO acts as the point of contact for Data Principals and the Data Protection Board, and is responsible for facilitating compliance with the Act and addressing relevant grievances and communications</p>
<p>Person</p> <p>Any reference to “Person” means and includes an individual, Hindu Undivided Family, company, firm, association of persons or body of individuals, State and every artificial juridical person.</p>	

Remember

- The DPDP Act applies only to digital personal data.
- A Data Fiduciary is primarily responsible for complying with the Act, even when processing is outsourced to a Data Processor.

The Act adopts a consent-centric framework, requiring Data Fiduciaries to obtain valid consent before collecting and processing personal data, unless such processing falls within one of the recognised legitimate uses prescribed under the Act. It also grants Data Principals statutory rights, including the right to access information, seek correction or erasure of personal data, avail grievance redressal, and nominate another individual to exercise their rights in specified circumstances.

To ensure responsible processing, the DPDP Act imposes several obligations on Data Fiduciaries, including providing transparent privacy notices, implementing reasonable security safeguards, establishing grievance redressal mechanisms, notifying personal data breaches where required, and erasing personal data once the purpose of processing has been fulfilled, unless its retention is required by law. Certain entities may also be notified as Significant Data Fiduciaries, making them subject to enhanced compliance obligations based on the nature, volume and sensitivity of the personal data and the scale of processing activities.

The DPDP Act promotes a culture of privacy governance, accountability, and responsible data management. It encourages organisations to integrate privacy into their business processes, adopt robust security measures, and build consumer trust through transparent data practices. The Act provides for a techno-legal and automated regulator mechanism to ensure protection of rights of the Data Principal.

Key Highlights

Aspect	Overview
Objective	Protect digital personal data while enabling lawful processing.
Applies To	Processing of digital personal data within and, in certain cases, outside India.
Key Stakeholders	Data Principals, Data Fiduciaries, Data Processors and Consent Managers.
Foundation	Consent-based processing with specified legitimate uses.
Focus Areas	Privacy, transparency, accountability, security, and responsible data governance.
Outcome	A trusted, secure, and privacy-centric digital ecosystem.

Fundamental Principles of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 is built upon a set of foundational principles that promote responsible and transparent processing of personal data. Although the Act does not expressly list these as “principles,” they are reflected throughout its provisions and form the basis of an effective privacy compliance framework.

The Eight Foundational Principles of the DPDP Act, 2023

1. Lawful Processing Personal data must be processed only for a lawful purpose, based on consent or a recognised legitimate use.	2. Purpose Limitation Personal data should be collected only for a specific, lawful, and clearly communicated purpose.
3. Data Minimisation Collect only such personal data as is necessary to achieve the stated purpose of processing.	4. Accuracy of Personal Data Reasonable efforts should ensure personal data used for decisions or disclosures is accurate and up to date.
5. Transparency Individuals should be informed, through a clear privacy notice, of how their data is processed.	6. Security Safeguards Implement reasonable technical and organisational measures to protect personal data.
7. Storage Limitation Personal data should not be retained indefinitely beyond the purpose of processing.	8. Accountability The Data Fiduciary remains responsible for compliance, even where processing is outsourced.

1. Lawful Processing

Personal data must be processed only for a lawful purpose. Such processing should either be based on the consent of the Data Principal or fall within one of the legitimate uses recognised under the Act.

Example

- A bank may process a customer's personal data for opening and operating a bank account after obtaining the customer's consent.

2. Purpose Limitation

Personal data should be collected only for a specific, lawful, and clearly communicated purpose and should not be used for unrelated purposes without a valid legal basis.

Example

- If an e-commerce platform collects a customer's address for product delivery, it should not use the same information for unrelated marketing activities without appropriate consent.

3. Data Minimisation

A Data Fiduciary should collect only such personal data as is necessary to achieve the stated purpose of processing. Excessive or unnecessary collection increases privacy risks and should be avoided.

Example

- A food delivery application generally requires a delivery address and contact number but does not ordinarily require a user's marital status or educational qualifications.

4. Accuracy of Personal Data

Reasonable efforts should be made to ensure that personal data used for making decisions affecting individuals or disclosed to other entities is accurate, complete, and up to date.

Example

- Financial institutions should periodically update customer contact details to ensure accurate communication and regulatory compliance.

5. Transparency

Individuals should be informed, through a clear and accessible privacy notice, about the personal data being collected, the purpose of processing, their rights under the Act, and the manner in which they may exercise those rights.

Example

- Before collecting personal data, an online platform should provide a privacy notice explaining how the information will be used.

6. Security Safeguards

Data Fiduciaries are required to implement reasonable technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, loss, or misuse.

Example

- Encryption, access controls, multi-factor authentication, regular security audits, and employee awareness programmes are common security measures.

7. Storage Limitation

Personal data should not be retained indefinitely. Once the purpose for processing has been fulfilled, the data should be erased, unless its retention is required under applicable law.

Example

- Recruitment records of unsuccessful candidates should be deleted after the applicable retention period unless there is a legal requirement to preserve them.

8. Accountability

The Data Fiduciary remains responsible for compliance with the DPDP Act, even where processing is carried out through a Data Processor. Organisations should establish internal governance mechanisms, maintain appropriate policies, and periodically review their privacy practices.

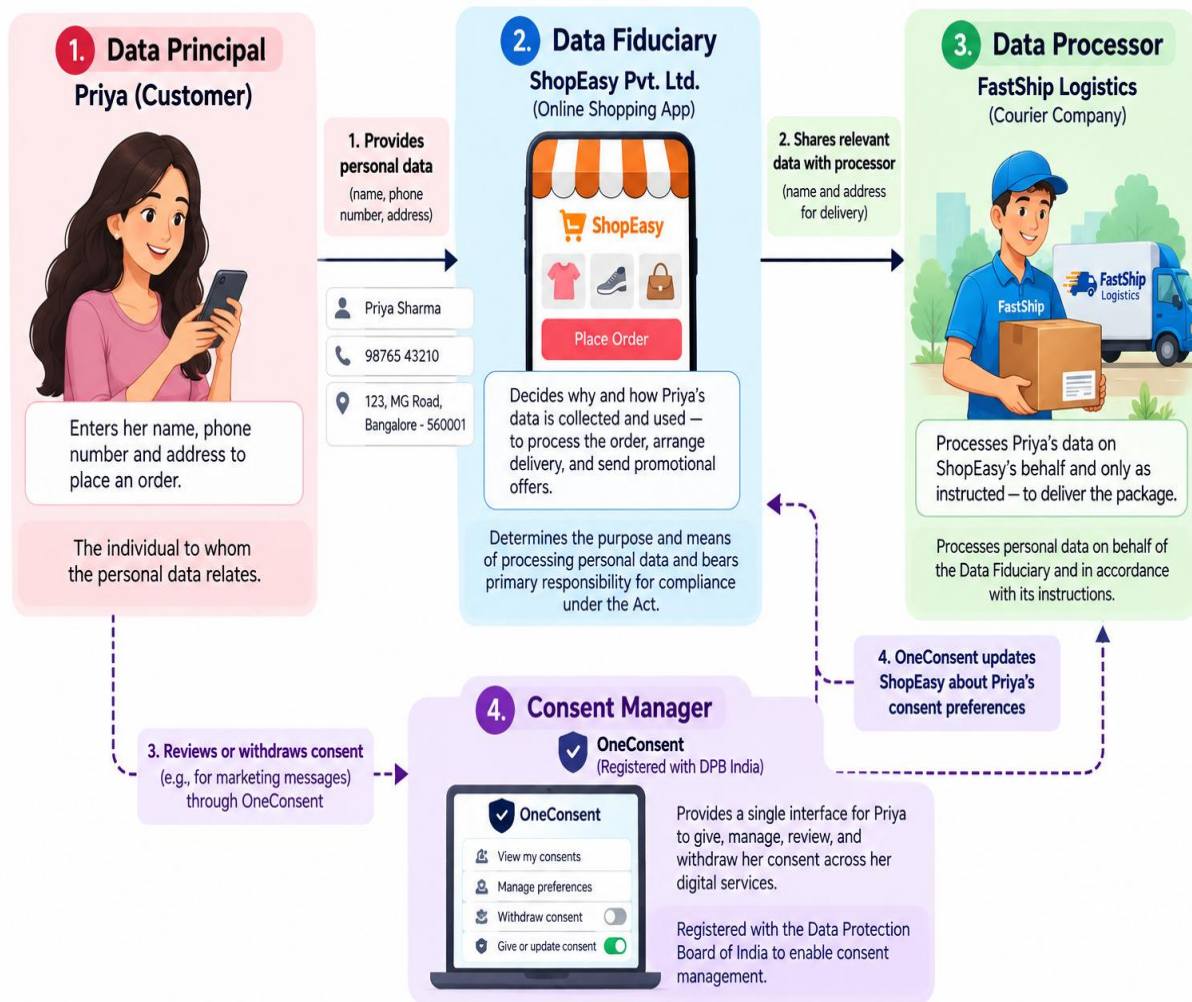
Important Definitions under the DPDP Act, 2023

Understanding the key terminology used in the Digital Personal Data Protection Act, 2023 ("DPDP Act") is essential for interpreting its provisions and determining the obligations of organisations processing personal data. The following are some of the most important definitions under the Act.

Term	Meaning
Personal Data [Section 2(t)]	Any data about an individual who is identifiable by or in relation to such data. Examples include name, mobile number, email address, Aadhaar number, PAN, photographs, IP address, and biometric information, etc.

Term	Meaning
Data [section 2(d)]	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;
Digital Personal Data [Section 2(n)]	Personal data collected in digital form or collected physically and subsequently digitised. The DPDP Act applies only to digital personal data.
Data Principal [Section 2(j)]	The individual to whom the personal data relates. In the case of a child, includes the parents or lawful guardian and in case of a person with disability, it includes the lawful guardian acting on behalf of such person with disability.
Data Fiduciary [Section 2(i)]	Any person (natural or juristic – defined u/s 2(s)) that determines the purpose and means of processing personal data. It bears the primary responsibility for compliance under the Act.
Data Processor [Section 2(k)]	A person that processes personal data on behalf of a Data Fiduciary and acts in accordance with its instructions.
Consent Manager [Section 2(g)]	A person registered with the Data Protection Board of India who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform.
Processing [Section 2(x)]	An automated operation or set of operations performed on digital personal data, including operations such as collection, storage, use, sharing, disclosure, retrieval, recording, adaptation, alteration, erasure or destruction.
Consent [Section 6(1)]	A free, specific, informed, unconditional, and unambiguous indication of the Data Principal's agreement to the processing of personal data through a clear affirmative action.
Personal Data Breach [Section 2(u)]	Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data.
Significant Data Fiduciary [Section 2(z); 10]	A Data Fiduciary notified by the Central Government based on factors such as the volume and sensitivity of personal data processed, risk to the rights of Data Principals, and other prescribed considerations.

PRACTICAL EXAMPLE TO UNDERSTAND THE ROLE OF STAKEHOLDER



International Perspective - GDPR

GDPR i.e., the General Data Protection Regulation is one of the most stringent and comprehensive data protection and data security law in the world. Passed by the European Union in 2018, the GDPR has emerged as the most influential data protection model, with extraterritorial application and provisions for imposing exemplary penalties against those who violate its privacy and security standards, with penalties extending to tens of millions of euros. Courts in European Union have delivered several landmark judgments on the GDPR and Data Protection laws. Such landmark rulings sets global benchmarks, heavily shape the global privacy standards and jurisprudence, directly influencing the data protection framework and compliance standards all over the world. Prior to the enactment of GDPR, the European Union issued the Data Protection Directives in the year 1995 which remained in force till the enactment of GDPR.

GDPR v/s DPDP Act

- Unlike DPDP Act, GDPR also covers personal data stored in physical form.
- DPDP Act is more consent centric as the consent of the Data Principal is required for any change in use. However, GDPR is more information centric, thus, frequent consent of user is not required for the specific 6 purposes.
- GDPR has extra-territorial applicability in even the data is used for monitoring behaviour of residents of EU. However, no such clear provision is present in the DPDP Act.

Few Benchmark Rulings on EU Data Protection Laws

1. Google Spain versus AEDP (C-131/12) – Decided on 13.03.2014

In summary, the Google Spain vs AEDP judgment established the "right to be forgotten" as a fundamental concept of EU data protection legislation and clarified search engine operators legal obligations with regard to personal data. It gave people the power to request that links to personal information be removed from search engine results provided certain requirements are met. It continues to shape discussions and policies on privacy, freedom of expression, and online information retrieval.

2. Digital Rights Ireland vs Ireland (C-293/12)- Decided on 08.04.2014

In the present case, validity of various provisions of Data Retention Directives in Ireland and Austria were challenged on the ground of breach of privacy. As per Data Retention Directives, telephone communication service providers were required to retain traffic and location of the users for a specified time frame with the object to use the same for prevention of crime, criminal investigation and to safeguard the security of the State. The challenge travelled to the ECJ and pursuant thereto ECJ vide this ruling quashed the Data Retention Directives as they were found to be in breach of "Right to Privacy" of the users. It was held that though the object of Data Protection Directives was a general interest, however, the directives were not proportionate to the objects sought to be achieved and stood in breach of Charter of Fundamental Rights.

3. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14) – Decided on 01.10.2015

This landmark judgment dealt with "territorial application" of EU data-protection law and answered the crucial question of "whether a company established in one Member State could be subject to the data-

protection laws of another Member State where it carried out real and effective activities through stable arrangements”. The case revolves around a Slovakian company “Weltimmo” which ran advertisements related to Hungarian properties on its websites. When the company started charging fee for running such advertisements on its websites the advertisers requested the deletion of their personal data. However, Weltimmo failed to comply with the said requests and even forwarded their personal data to debt recovering agencies. Thereafter, on being fined by the Hungarian Data Protection Authorities, Weltimmo contested such penalties on ground that it was a company established in Slovakia and thus, it was not to be made a subject to Hungarian laws. The CJEU upheld the imposition of such penalties and laid down that a company even if established elsewhere, if it carries out real and effective activity in relation to subjects of a particular jurisdiction, the company will be deemed to be “established” in and be subject to the laws application to that particular jurisdiction.

4. Smaranda Bara v. CNAS (C-201/14) (ANAF case) – Decided on 01.10.2015

In this landmark judgment, the CJEU held that where personal data is subject to transfer and processing between public administrative bodies, the data subject must be informed in advance. The CJEU further held that a public administrative body must notify data subjects that their data will be transferred to another public administrative body in order for the processing to be a “fair processing of personal data”. Further, a controller of data must further inform the data subjects regarding the purpose of further processing of the said data and any other information as may be necessary to ensure fair processing of personal data.

5. Schrems vs Data Protection commissioner (C-362/15) – Decided on 06.10.2015

The European Court of Justice was called upon to decide the legality of the agreement which permitted transfer of data of a Facebook user in Ireland to United States. The CJEU in its judgment struck down the agreement and held that the data of a citizen cannot be transferred to any other country unless that country provides for equal protection of personal data akin to that of European Laws. The court opined that the US safe harbour scheme enabled interference by US public authority which intends to undermine the fundamental rights of the citizens in respect to their private life.

6. Brillen Rottler GmbH & Co. KG versus TC (C-526/24) – Decided on 19.03.2026

This landmark judgment materially dealt with the right of data subjects, under Article 15 of the GDPR, to request access to information regarding the use and transfer of the personal data collected from the data subjects. The data subjects have a further right to claim compensation where such use/transfer has been made in contravention to the other provisions of the GDPR.

In the present case, the CJEU observed that many data subject engaged in a practice of “GDPR hopping” whereby soon after data collection, these data subjects exercised their “Right to Access” under Article 15 of GDPR with the sole intention to claim compensation and further damages where such request was denied by the organisation.

Through this ruling, the CJEU recognised that the business organisations, in exceptional circumstances, can even reject an initial request for access where there is sufficiently strong evidence that such request is being made solely with the intention to pursue compensation, thereby striking a balance between the right of data subjects to monitor use and control of their personal data and the abuse of rights of the organisations holding/processing such data.

Applicability and Scope of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (“DPDP Act”) defines the circumstances in which its provisions apply and identifies the categories of processing that fall outside its scope. Understanding the applicability of the Act is the first step towards determining whether an organisation is required to comply with its obligations.

Where Does the DPDP Act Apply?

The DPDP Act applies to the processing of digital personal data, namely:

- Personal data collected in digital form; and
- Personal data collected in physical form and subsequently digitised.

The Act governs the entire lifecycle of digital personal data, including its collection, storage, use, sharing, disclosure, and deletion.

Territorial Applicability

The Act has both domestic and extra-territorial application.

Processing Activity	Applicability
Processing of digital personal data within India	✓ Covered
Processing outside India in connection with offering goods or services to individuals in India	✓ Covered
Processing of personal data solely in physical form (not digitised)	✗ Not Covered

Exclusions from the Act (Section 3)

The DPDP Act does not apply to:

- Personal data processed by an individual for personal or domestic purposes.
- Personal data that has been made publicly available by the Data Principal or by another person under a legal obligation to make such data publicly available.

Illustrative Examples

Scenario	Covered under the DPDP Act?
A customer registers on an e-commerce website	✓ Yes
A hospital stores patient records in electronic form	✓ Yes
An employer maintains employee information in HR software	✓ Yes

Scenario	Covered under the DPDP Act?
A handwritten visitor register that is never digitised	X No
A foreign company offering online services to users in India	✓ Yes

Phased Commencement of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 observes a phased commencement:

Provision	Commencement	Time Period
Section 1(2), Section 2, Sections 18–26, Section 35, Sections 38–43, and Sections 44(1) and 44(3)	13 November 2025	In force from publication.
Section 6(9) and Section 27(1)(d)	13 November 2026	These provisions are set to come into force one year after publication of the commencement notification.
Sections 3–5; Sections 6(1)–6(8) and 6(10); Sections 7–10; Sections 11–17; Section 27 except Section 27(1)(d); Sections 28–34; Sections 36–37; and Section 44(2)	13 May 2027	These substantive provisions come into force eighteen months after publication of the commencement notification

Rights and Duties of Data Principals

The DPDP Act recognises that individuals, referred to as Data Principals, should have meaningful control over their personal data. Alongside granting important rights, the Act also places certain responsibilities on Data Principals to ensure that the digital ecosystem functions fairly and responsibly.

Rights of a Data Principal

Right	What it Means
Consent of Data Principal (Section 4 and 5)	Subject to the exceptions prescribed under the Act, Personal data of Data Principal can only be used after obtaining the informed consent of the Data Principal.
Right to Withdraw Consent (Section 6)	Where processing is based on consent, a Data Principal may withdraw consent at any time. Upon withdrawal, the Data Fiduciary must cease processing unless such processing is otherwise permitted under the Act or required by law.
Right to Access Information (Section 11)	A Data Principal may seek information regarding the personal data being processed, the processing activities undertaken, and the identities of Data Fiduciaries or Data Processors with whom such data has been shared.
Right to Data Trail Information (Section 11)	A Data Principal may seek information about how their personal data is being processed, including relevant processing activities and the entities involved in processing. The “data trail” is a practical transparency concept arising from the right to access information and is not separately named as a statutory right under the Act.
Right to Information on Data Sharing (Section 11)	A Data Principal may seek information regarding the Data Fiduciaries or Data Processors with whom their personal data has been shared, as provided under the Act.
Right to Correction, Completion and Erasure (Section 12)	A Data Principal may request correction of inaccurate or misleading personal data, completion of incomplete data, or erasure of personal data no longer required, subject to legal requirements.
Right to Grievance Redressal (Section 13)	Every Data Principal has the right to raise grievances before the Data Fiduciary or the Consent Manager in case of failure to perform their respective obligations under the Act. Thereafter, the Data Principal may approach the Data Protection Board.
Right to Nominate (Section 14)	A Data Principal may nominate another individual to exercise their rights under the Act in the event of death or incapacity of the Data Principal to exercise such rights.

Example

- If an online retailer continues to retain a customer's personal data even after the customer closes the account, the customer may request erasure of such personal data, unless retention is required under the law.

Consent under the DPDP Act

Consent forms the primary legal basis for processing personal data. To be valid, consent must be:

The Five Elements of Valid Consent under the DPDP Act

Free Given without coercion or undue influence.	Specific Tied to a specific purpose of processing.	Informed Given after receiving a clear privacy notice.
Unconditional Not conditioned on unrelated consents.	Unambiguous Indicated through a clear affirmative action.	

Before seeking consent, the Data Fiduciary must provide a clear and understandable notice specifying:

- The personal data proposed to be processed;
- The purpose of processing;
- The manner in which the Data Principal may exercise their rights; and
- The procedure for making a grievance.

A Data Principal also has the right to withdraw consent at any time. Upon withdrawal, the Data Fiduciary must cease processing the personal data unless such processing is otherwise permitted under the Act or required by law.

Rule 14 — Making Data Principal Rights Operational

The Act grants rights to Data Principals. Rule 14 focuses on how those rights are to be made accessible in its true sense.

Requirement	Rule 14 Position
Published means of making a request	The Data Fiduciary and, where applicable, the Consent Manager must prominently publish on its website or app or both, the means through which a Data Principal may make a request to exercise rights under the Act.
Identifiers	The organisation may specify particulars such as a username or other identifier required to identify the Data Principal under its terms of service.

Requirement	Rule 14 Position
Making the request	A Data Principal may request exercise of rights from the Data Fiduciary to whom consent was previously given, using the published means and required particulars.
Grievance redressal	The Data Fiduciary and Consent Manager must publish a reasonable period for responding to grievances, not exceeding 90 days, and must implement appropriate technical and organisational measures to make the system effective.
Nomination	A Data Principal may nominate one or more individuals, in accordance with the terms of service and applicable law, using the means and particulars required by the Data Fiduciary.

The Rules therefore expect organisations to make rights and grievance mechanisms visible and usable. A privacy notice that merely states that rights exist, without explaining how the Data Principal can exercise them, should be reviewed against the operational requirements of Rule 14.

Duties of a Data Principal (Section 15)

While the Act protects individual privacy, it also expects Data Principals to exercise their rights responsibly.

Duty	Description
Provide Authentic Information	Furnish accurate and verifiably authentic personal information while exercising rights under the Act.
Avoid Impersonation	Refrain from impersonating another person while providing personal data or exercising rights.
Do Not Suppress Material Information	Avoid knowingly suppressing material information or submitting false documents while interacting with a Data Fiduciary.
Avoid Frivolous Complaints	Do not file false, malicious, or frivolous grievances or complaints under the Act.
Comply with Applicable Laws	Exercise rights responsibly and in accordance with the DPDP Act and other applicable laws.

Rights and Duties of a Data Principal, Side by Side

Rights	Duties
Access information about processing	Provide authentic information
Correction, completion and erasure	Avoid impersonation
Grievance redressal	Do not suppress material information
Nominate another person	Avoid frivolous complaints; comply with the law

Data Fiduciary

A Data Fiduciary is a person who determines the purpose and means of processing personal data and plays a key role in safeguarding personal information. The DPDP Act places primary responsibility on the Data Fiduciary for managing and protecting the personal data, requiring it to process personal data in a fair, transparent, and secure manner.

Thus, the primary responsibility of the Data Fiduciary is to responsibly handle the personal data and act in the best interest of the Data Principal.

Functions of a Data Fiduciary

A Data Fiduciary may:

- Process personal data after obtaining valid consent from the Data Principal in respect thereof.
- Process personal data for legitimate uses recognised under the DPDP Act without obtaining consent, where permitted by law.
- Engage Data Processors to process personal data on its behalf, while primarily remaining accountable and responsible for the compliance of the provisions contained under the DPDP Act as well as the DPDP Rules.
- Retain personal data where its retention is required under any applicable law or for compliance with legal obligations.

Obligations of a Data Fiduciary

Obligation	Description
Lawful Processing (Section 4)	Process personal data collected from Data Principal only for lawful purposes and in accordance with the Act.
Notice and Consent (Sections 5 and 6)	Provide a clear notice to, and obtain valid consent from the Data Principal, unless processing is based on a recognised legitimate use.
Purpose Limitation	Use personal data only for the purpose for which it was collected and consent has been obtained in respect thereof, or as otherwise permitted by law.
Primary Accountability (Section 8 (1))	Data Fiduciary remains responsible for personal data handling in accordance with the Act even when such data is being processed by a Data Processor
Accuracy of Data (Section 8 (3))	Ensure personal data is accurate, complete, and consistent where such personal data is likely to be used to make decisions affecting such Data Principal or where the same is to be disclosed to another Data Fiduciary.
Security Safeguards (Section 8 (4) and (5))	Implement reasonable technical and organisational security measures to protect personal data from misuse or security breach.
Data Breach Notification (Section 8 (6))	Notify the Data Protection Board of India and affected Data Principals in the event of a personal data breach, as prescribed.

Obligation	Description
Erasure of Data (Section 8 (7) and Section 8 (8))	Delete personal data once the purpose of processing has been fulfilled, unless retention is required by law.
Grievance Redressal (Section 8 (10))	Establish an effective mechanism to address grievances and complaints raised by Data Principals.
Responsibility in case of processing of personal data related to a child (Section 9)	Obtain verifiable parental consent before processing a child's personal data or data of a person with disability having a lawful guardian. Not to undertake processing of data which is detrimental to the well-being of a child and comply with restrictions relating to tracking, behavioural monitoring and targeted advertising, subject to statutory provisions/exemptions.
Responsibility for Data Processors	Remain accountable for compliance of Act and Rules even where processing is outsourced to a Data Processor.

Rule 6: Reasonable Security Safeguards

Section 8 of the Act requires a Data Fiduciary to take reasonable security safeguards to prevent personal data breach. Rule 6 of the DPDP Rules prescribes the minimum-security safeguards to be implemented by a Data Fiduciary, including appropriate technical and organisational measures such as encryption, masking or tokenisation, access controls, logging and monitoring, and measures to ensure continuity of processing. These safeguards are required to be implemented in respect of processing undertaken by the Data Fiduciary and, where processing is carried out on its behalf by a Data Processor, through appropriate contractual and other measures to ensure that the prescribed safeguards are maintained.

Safeguard	What the Rule Requires
Protection of data	Appropriate security measures, including encryption, obfuscation, masking or the use of virtual tokens mapped to the personal data.
Access control	Appropriate measures to control access to the computer resources used by the Data Fiduciary or Data Processor, wherever applicable.
Logs, monitoring and review	Visibility into access to personal data through appropriate logs, monitoring and review so that unauthorised access can be detected, investigated and remediated.
Continuity and backups	Reasonable measures for continued processing where confidentiality, integrity or availability is compromised because of destruction or loss of access, including data backups.
Retention of logs and data	For detection, investigation, remediation and continued processing after a compromise, specified logs and personal data must be retained for one year, unless applicable law requires otherwise.

Safeguard	What the Rule Requires
Processor contracts	Contracts with Data Processors should contain appropriate provisions requiring reasonable security safeguards.
Technical and organisational measures	Appropriate measures must be maintained to ensure effective observance of the security safeguards.

The Rule does not prescribe a single or uniform technical architecture to be adopted by every organisation. Instead, the prescribed safeguards are required to be implemented through appropriate technical and organisational measures, having regard to the nature of the systems, processing activities, personal data involved and the risks associated with such processing.

✦ **Compliance Evidence to be Maintained**

The Organisation should maintain documentary evidence demonstrating implementation and periodic review of its security safeguards including - Security policies, access-control records, audit/logging arrangements, backup and continuity procedures, Data Processor contractual safeguards, incident records and records evidencing periodic review of technical and organisational measures.

Rule 9 — Contact Information

Every Data Fiduciary must prominently publish on its website or app, the business contact information of its Data Protection Officer, where applicable, or another person who can answer questions of a Data Principal about the processing of personal data.

The same contact information must also be mentioned in every response to a communication from a Data Principal concerning the exercise of rights under the Act.

Key Takeaway

- The DPDP Act places accountability of the Data Fiduciary at the heart of data governance. While Data Fiduciaries are empowered to process personal data for legitimate business and legal purposes, they are equally responsible for ensuring transparency, protecting personal data, respecting the rights of Data Principals, and maintaining effective privacy governance.

Notice Requirement under the DPDP Rules, 2025

Section 5 of the Act requires a Data Fiduciary to give notice to the Data Principal before or at the time of requesting consent from the Data Principal. Rule 3 of the DPDP Rules makes this requirement more specific by setting out the contents of such Notice and how the same should be presented.

Requisites of Notice requesting Consent	What it Means in Practice
Standalone and understandable	The notice must be presented and be understandable independently of any other information made available by the Data Fiduciary.
Clear and plain language	The notice should give a fair account of the details necessary for the Data Principal to provide specific and informed consent.
Itemised description of personal data	The categories of personal data proposed to be processed should be identified individually rather than described only through a broad or generic expression.
Specified purpose or purposes	The notice must state the purpose or purposes for processing.
Goods, services or uses	The notice must specifically describe the goods or services to be provided, or the uses to be enabled by processing.
Withdrawal of consent	The notice must provide a particular communication link for accessing the website/app or other means through which consent can be withdrawn, with ease comparable to giving consent.
Exercise of rights	The notice must provide the means through which the Data Principal may exercise rights under the Act.
Complaint to the Board	The notice must provide the means through which the Data Principal may make a complaint to the Data Protection Board.

Thus, the notice sent in compliance of this Act should allow a Data Principal to answer three questions without having to search through several documents, viz., What personal data is being processed? Why is it being processed? What can I do if I want to withdraw consent, exercise my rights or make a complaint?

Organisations processing personal data should review each juncture at which personal data is collected—including websites, mobile applications, customer onboarding, employee portals, forms and consent interfaces—and ensure that the notice presented at that very juncture corresponds to the processing activity.

✦ Practical Implication

A general privacy policy may not, by itself, satisfy the structure contemplated by Rule 3 if the information necessary for specific and informed consent is not independently and clearly presented.

Significant Data Fiduciaries (SDFs)

The Digital Personal Data Protection Act, 2023 (“DPDP Act”) recognises that certain Data Fiduciaries process personal data on a scale or in a manner that may pose a higher risk to the rights of Data Principals. Such Data Fiduciaries may be notified by the Central Government as Significant Data Fiduciaries (SDFs) and are subject to enhanced compliance obligations under the Indian data protection framework.

Unlike ordinary Data Fiduciaries, a Data Fiduciary does not automatically become an SDF merely because of its scale of business. Such designation is made by the Central Government after considering the following factors as prescribed under the Act.

Factors Considered in Classifying a Significant Data Fiduciary:

Volume of Data Scale of personal data processed by the organisation.	Sensitivity of Data Nature and sensitivity of the personal data processed.
Risk to Data Principals Potential impact on the rights of Data Principals .	Sovereignty & Public Order Risk to electoral democracy or public order.
Security of the State	Public Order

Additional Obligations for Significant Data Fiduciaries (SDFs)

Certain Data Fiduciaries may be designated by the Central Government as Significant Data Fiduciaries based upon factors such as the volume and sensitivity of personal data processed, the risk posed to Data Principals, and the impact of processing and handling the personal data on national interests.

The additional obligations of a Significant Data Fiduciary as given under Section 10 of the Act are as follows:

Requirement	Purpose
Appointment of a Data Protection Officer (DPO) [Section 10(2)(a)]	The DPO must represent the SDF under the Act, be based in India, be responsible to the Board of Directors or similar governing body, and serve as the point of contact for the grievance redressal mechanism.
Appointment of an Independent Data Auditor [Section 10(2)(b)]	The independent data auditor must carry out a data audit and evaluate the SDF's compliance with the Act.
Periodic Data Protection Impact Assessment (DPIA) [Section 10(2)(c)(i)]	To describe the rights of Data Principals and the purpose of processing, and to assess and manage risks to the rights of Data Principals, along with other prescribed matters.
Periodic Audit [Section 10(2)(c)(ii)]	To periodically evaluate the SDF's compliance with the Act and the Rules.
Other Prescribed Measures [Section 10(2)(c)(iii)]	To undertake such other measures, consistent with the Act, as may be prescribed.

Rule 13: Additional Obligations of Significant Data Fiduciaries

Section 10 of the Act identifies additional obligations for Significant Data Fiduciaries. Rule 13 of the DPDP Rules provides further operational detail and creates a recurring assessment and audit cycle.

Requirement	What Rule 13 Requires
Annual DPIA	An SDF must undertake a Data Protection Impact Assessment once in every 12-month period from the date it is notified as an SDF or included in a notified class.
Annual audit	An audit must be undertaken to ensure effective observance of the Act and the Rules.
Reporting to the Board	The person carrying out the DPIA and audit must furnish the Board with a report containing significant observations.
Algorithmic / technical due diligence	The SDF must exercise due diligence to verify that technical measures, including algorithmic software adopted by it for hosting, display, uploading, modification, uploading, transmission, publishing, storage, updating or sharing of personal data used for specified data operations, are not likely to pose a risk to the rights of Data Principals.
Conditional localisation	Where the Central Government specifies personal data on the recommendation of the committee constituted for this purpose, the SDF must ensure that the specified personal data and traffic data relating to its flow are not transferred outside India.

⚠ The Localisation Requirement is Conditional

Rule 13 does not itself declare that all personal data processed by every SDF must remain in India. The restriction applies where the Central Government specifies the relevant personal data through the mechanism provided in the Rule.

SDF calendar: maintain a 12-month DPIA and audit cycle, document algorithmic due diligence, preserve evidence of governance and review, map international transfers and monitor Central Government specifications affecting localisation.

Cross-Border Transfer of Personal Data and Exemptions under the Act

The DPDP Act permits the transfer of digital personal data outside India by Data Fiduciary for the purpose of processing the same. However, the Central Government may, by notification, restrict the transfer of personal data to specified countries or territories outside India.

Rule 15 — Transfer of Personal Data Outside India

The Act permits transfer of digital personal data outside India, subject to restrictions that may be imposed by the Central Government. Rule 15 further provides that personal data processed by a Data Fiduciary under the Act may be transferred outside India subject to any requirements the Central Government may specify, by general or special order, concerning making that personal data available to a foreign State or to a person or entity under the control of, or an agency of, such a State.

i Not a General Prohibition

Rule 15 should not be read as a general prohibition on international transfers. It merely requires that the that organisations must monitor and comply with any requirements or restrictions subsequently specified by the Central Government.

Exemptions under the DPDP Act (Section 17)

While the DPDP Act establishes a comprehensive framework for processing digital personal data, it also recognises that certain activities require exemption from the stringent provisions under the Act. Accordingly, Section 17 empowers the Central Government to exempt certain processing activities undertaken in respect of personal data, subject to prescribed conditions.

These exemptions include: -

- Where processing necessary for enforcing legal rights or claims;
- **Enforcement of legal rights or claims:** Specified provisions of the Act do not apply where processing of personal data is necessary for enforcing a legal right or claim.
- **Judicial, quasi-judicial, regulatory and supervisory functions:** Processing by a court, tribunal or other body in India entrusted by law with judicial, quasi-judicial, regulatory or supervisory functions is exempt to the extent necessary for performing those functions.
- **Prevention, detection, investigation or prosecution of offences:** Specified provisions do not apply where personal data is processed for the prevention, detection, investigation or prosecution of an offence or contravention of Indian law.
- **Processing relating to persons outside India:** Specified provisions do not apply where personal data of Data Principals who are not within India is processed pursuant to a contract entered into with a person outside India by a person based in India.

- **Corporate restructuring and transactions:** Exemptions apply to processing necessary for certain schemes of compromise or arrangement, mergers, amalgamations, demergers, reconstruction, transfer of undertakings or division of companies, where approved by the competent court, tribunal or authority.
- **Loan default assessment:** Processing for ascertaining the financial information, assets and liabilities of a person who has defaulted on a loan or advance from a financial institution is exempt, subject to applicable laws governing disclosure of information or data.
- **Certain State instrumentalities:** The Central Government may notify specified State instrumentalities to which the Act will not apply, where processing is undertaken in specified interests such as the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or prevention of incitement to specified cognizable offences.
- **Research, archiving and statistical purposes:** Processing necessary for research, archiving or statistical purposes may be exempt where the statutory conditions are satisfied, including that the personal data is not used to make a decision specific to a Data Principal and the prescribed standards are followed.
- **Exemptions for specified Data Fiduciaries, including startups:** The Central Government may, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or classes of Data Fiduciaries, including startups, to whom specified provisions relating to notice, certain obligations of Data Fiduciaries, Significant Data Fiduciaries and Data Principal rights will not apply.
- **Processing by the State or its instrumentalities:** Certain obligations relating to data retention and erasure, and certain Data Principal rights, may not apply to processing by the State or its instrumentalities in the circumstances specified under Section 17(4).
- **Power to grant further exemptions:** The Central Government may, before the expiry of five years from the commencement of the Act, notify that specified provisions of the Act will not apply to a Data Fiduciary or class of Data Fiduciaries for a specified period.

Rule 16 — Research, Archiving and Statistical Processing

⚠ The Exemption is Conditional

Research, archiving or statistical processing is not automatically exempt from the DPDP Act merely because it is undertaken for research or statistical purposes. The exemption under Section 17(2)(b), read with Rule 16, is subject to compliance with the standards specified in the Second Schedule.

Legitimate Uses (Sections 7)

The DPDP Act recognises that certain processing activities are necessary for public interest, legal compliance, or the efficient functioning of organisations. In such cases, personal data may be processed without obtaining consent, provided the processing falls within the legitimate uses specified under the Act.

Some important legitimate uses include:

Legitimate Use	Illustration
Performance of State Functions	Processing personal data for providing government benefits, subsidies, licences, certificates, or other services authorised by law.
Compliance with Judgments or Legal Obligations	Processing required to comply with court orders, statutory duties, or regulatory requirements.
Medical Emergencies	Processing personal data to protect the life or health of an individual during a medical emergency.
Disasters and Public Safety	Processing necessary during disasters, epidemics, public health emergencies, or other situations affecting public safety.
Employment Purposes	Processing personal data for recruitment, attendance, payroll, statutory compliance, protection of employer property, or other employment-related purposes, as permitted by the Act.

Consent-Based Processing Compared with Legitimate-Use Processing

Basis	Key Feature
Consent-Based Processing	Requires a free, specific, informed, unconditional and unambiguous affirmative action by the Data Principal; may be withdrawn at any time.
Legitimate-Use Processing	Permitted without consent for specified purposes such as State functions, legal compliance, medical emergencies, disasters, and employment.

Consent Managers

The Act recognises a Consent Manager as a person registered with the Data Protection Board who enables Data Principals to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform. Rule 4 and the First Schedule prescribe the conditions for registration and the obligations applicable to a registered Consent Manager.

Requirements for registration as a Consent Manager

A person seeking registration as a Consent Manager must satisfy the following conditions:

- The applicant must be a company incorporated in India.
- It must have sufficient technical, operational and financial capacity to fulfil its obligations as a Consent Manager.
- Its financial condition and the general character of its management must be sound.
- Its net worth must be at least ₹2 crore.
- The likely volume of business, capital structure and earning prospects must be adequate.
- Its directors, key managerial personnel and senior management must have a general reputation and record of fairness and integrity.
- Its constitutional documents must contain provisions requiring compliance with specified conflict-of-interest and transparency obligations, and amendments to those provisions require prior approval of the Board.
- Its proposed operations must be in the interests of Data Principals.
- Independent certification is required regarding the interoperability of its platform with data protection standards and assurance frameworks published by the Board and the technical and organisational measures supporting compliance.

Core obligations of a Consent Manager

- Enable Data Principals to give consent to a Data Fiduciary onboarded on the platform, either directly or through another onboarded Data Fiduciary that maintains the personal data.
- Ensure that when personal data is made available or shared through the Consent Manager, its contents are not readable by the Consent Manager.
- Maintain records of consents given, denied or withdrawn; notices preceding or accompanying consent requests; and sharing of personal data with a transferee Data Fiduciary.
- Give the Data Principal access to those records and, upon request and subject to its terms of service, provide the information in machine-readable form.
- Retain the consent records for at least seven years, or longer period where agreed upon between the Data Principal and Consent Manager or required by law.
- Maintain a website or app, or both, as the primary means of access to its services.
- Not subcontract or assign the performance of its obligations under the Act and Rules.

- Take reasonable security safeguards to prevent personal data breaches.
- Act in a fiduciary capacity in relation to the Data Principal.
- Avoid conflicts of interest with Data Fiduciaries and maintain measures to address the conflicts arising from directors, key managerial personnel and senior management.
- Publish specified information concerning its promoters, directors, key managerial personnel, senior management and certain significant shareholding interests, together with other information that the Board may direct.
- Maintain effective audit mechanisms covering technical and organisational controls, registration conditions and compliance with the Act and Rules, and report audit outcomes to the Board periodically or when directed.
- Obtain prior approval of the Board before transferring control of the Consent Manager by sale, merger or otherwise, subject to the conditions specified by the Board.

The Board may examine an application, register or reject it with reasons, require information, and direct corrective measures where it finds non-adherence. After giving the Consent Manager an opportunity of being heard, the Board may suspend or cancel registration where necessary in the interests of Data Principals.

Rule 5 and Second Schedule: Processing by the State for Benefits and Services

Section 7(b) of the Act recognises processing of personal data for the provision or issue of a subsidy, benefit, service, certificate, licence or permit by the State or its instrumentalities. Rule 5 requires such processing to comply with the standards set out in the Second Schedule.

For this purpose, the Rules cover benefits, services, certificates, licences and permits provided or issued under law, under a government policy or instruction issued in exercise of executive power, or using public funds.

The Second Schedule Standards

- Processing must be carried out lawfully.
- Processing must be limited to the uses specified under Section 7(b) and Section 17(2)(b) of the Act.
- Only the personal data necessary for those uses should be processed.
- Reasonable efforts should be made to ensure the completeness, accuracy and consistency of the personal data.
- Personal data should be retained only for as long as required for the relevant use or to comply with applicable law.
- Reasonable security safeguards must be implemented to prevent a personal data breach, including where processing is undertaken by a Data Processor.
- Where processing is under Section 7(b), the Data Principal must be given an intimation, business contact information for questions regarding the processing, and a link or other means through which rights under the Act may be exercised.

- The processing must also remain consistent with any other standards applicable under government policy or law.
- The person who determines the purpose and means of processing remains accountable for effective observance of these standards.

** Illustration**

An online shopping platform requires a customer's consent to use their email address for sending promotional offers. However, the same platform may process customer information to comply with a statutory tax obligation or a lawful direction issued by a court without obtaining fresh consent.

Children's Personal Data

The DPDP Act prescribes additional safeguards for the processing of personal data relating to children and persons with disabilities who have a lawful guardian. A Data Fiduciary must obtain verifiable consent from the parent or lawful guardian before processing such personal data.

To protect children from harmful data practices, the Act generally prohibits:

- Processing that is likely to cause any detrimental effect on the well-being of a child;
- Tracking or behavioural monitoring of children; and
- Targeted advertising directed at children.

The Central Government may notify certain classes of Data Fiduciaries or specified purposes that are exempt from some of these requirements, subject to the prescribed conditions.

Rule 10 - Verifiable Consent of a Parent

Section 9 requires the verifiable consent of a parent before processing a child's personal data. Rule 10 sets out the verification process. The Data Fiduciary must adopt appropriate technical and organisational measures to obtain verifiable parental consent and must exercise due diligence to establish that the person identifying themselves as the parent who is an identifiable adult if required in connection with any law for the time being in force in India.

The verification may be based on:

- Reliable identity and age details already available with the Data Fiduciary; or
- Identity and age details voluntarily provided by the individual, including through a virtual token mapped to such details and issued by an authorised entity.

The Rule's illustrations show that the same basic approach applies whether the parent is already a registered user of the platform or an unregistered user. Where reliable identity and age information is already available, the Data Fiduciary may use that information; otherwise, the relevant identity and age information, including the virtual-token, may be used.

Rule 11 - Lawful Guardian of a Person with Disability

Where consent is being obtained from a person identifying themselves as the lawful guardian of a person with disability, the Data Fiduciary must exercise due diligence to verify that the guardian has been appointed by

- a) a court of law;
- b) a designated authority; or
- c) a local level committee under the applicable guardianship law.

The Rule links the meaning of “law applicable to guardianship” to the relevant legal framework, including the Rights of Persons with Disabilities Act, 2016 and, for specified conditions, the National Trust Act, 1999 alongwith the rules made under these laws.

Rule 12 - Exemptions from Certain Child-Data Obligations

Rule 12 provides that the requirements under Sections 9(1) and 9(3) of the Act do not apply in specified circumstances. These are not general exemptions, rather they are confined to the classes of Data Fiduciaries and purposes identified in the Fourth Schedule and are subject to the conditions specified therein.

Fourth Schedule - Part A: Specified Data Fiduciaries

Class	Condition / Permitted Processing
Clinical establishment, mental health establishment or healthcare professional	Processing restricted to provision of health services to the child, to the extent necessary for protection of the child's health.
Allied healthcare professional	Processing restricted to supporting implementation of a recommended healthcare treatment or referral plan, to the extent necessary for protection of the child's health.
Educational institution	Tracking and behavioural monitoring only for educational activities or in the interests of safety of children enrolled with the institution.
Person responsible for children in a crèche or child day-care centre	Tracking and behavioural monitoring only in the interests of the safety of children in their care.
Transport provider engaged by educational institution, crèche or child-care centre	Location tracking during travel to and from the institution, restricted to the interests of child safety.

Fourth Schedule - Part B: Specified Purposes

- Exercise of a power, performance of a function or discharge of duties in the interests of a child under applicable Indian law, to the extent necessary.
- Provision or issue of a subsidy, benefit, service, certificate, licence or permit in the interests of a child under Section 7(b), to the extent necessary.
- Creation of a user account for communication by email, limited to what is necessary for that purpose.
- Determination of a child's real-time location where necessary for the child's safety, protection or security.
- Preventing information, services or advertisements likely to cause a detrimental effect on a child's well-being from being accessible to the child, to the extent necessary.
- Confirmation that a Data Principal is not a child and observance of the due diligence requirements under Rule 10, to the extent necessary.

⚠ Important

The Fourth Schedule does not create a general relaxation from the protections applicable to children’s personal data. Each exemption is tied to a defined class and carries a specific purpose and is subject to the particular conditions and limitations applicable to it.

Personal Data Breach and Penalties

The Digital Personal Data Protection Act, 2023 (“DPDP Act”) places significant emphasis on protecting personal data from unauthorised access, disclosure, loss, or misuse. To ensure accountability, the Act requires Data Fiduciaries to adopt appropriate security measures and prescribes substantial financial penalties for non-compliance.

What is a Personal Data Breach? (Section 2 (u))

A Personal Data Breach refers to any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of personal data that compromises its confidentiality, integrity, or availability.

Examples:

- Unauthorised access to a customer database by hackers.
- Accidental disclosure of employee records to an unintended recipient.
- Loss of access to personal data due to a ransomware attack or system failure.

Obligations Following a Data Breach

In the event of a personal data breach, a Data Fiduciary is required to take the following steps:

Steps a Data Fiduciary Must Take Following a Personal Data Breach

1. Contain the Breach Take immediate steps to contain and assess the breach.	2. Notify the Board Notify the Data Protection Board of India as prescribed.
3. Notify Data Principals Inform affected individuals without delay.	4. Remediate Maintain safeguards to minimise the risk of future incidents.

- Maintain appropriate security safeguards to minimise the risk of future incidents.

Rule 7: Personal Data Breach Intimation

Rule 7 separates the information to be given to affected Data Principals from the information to be furnished to the Data Protection Board.

Intimation to Affected Data Principals

On becoming aware of a personal data breach, the Data Fiduciary must, to the best of its knowledge, intimate each affected Data Principal without delay. The communication should be concise, clear and in plain language and should be made through the Data Principal's user account or another registered mode of communication.

- A description of the breach, including its nature, extent and timing.
- The consequences relevant to the Data Principal that are likely to arise from the breach.
- The measures implemented and being implemented to mitigate the risk.
- Safety measures that the Data Principal may take to protect their interests.
- Business contact information of a person who can respond to the Data Principal's queries on behalf of the Data Fiduciary.

Intimation to the Data Protection Board

- An initial description of the breach must be provided without delay, including its nature, extent, timing and location of occurrence and the likely impact.
- Within 72 hours of becoming aware of the breach, the Data Fiduciary must provide updated and detailed information, unless the Board allows a longer period on a written request.
- The detailed/update intimation covers the broad facts, circumstances and reasons leading to the breach; measures implemented or proposed to mitigate risk; findings regarding the person who caused the breach, where available; remedial measures taken to prevent recurrence; and a report regarding the intimations given to affected Data Principals.

⚠ Important Distinction

The 72-hour period in Rule 7 applies to the detailed information to the Board. The Rule requires communication to affected Data Principals without delay; it does not prescribe the same 72-hour deadline for that communication.

Penalties under the DPDP Act

The Act adopts a civil penalty regime, with monetary penalties determined by the Data Protection Board of India based on the nature and seriousness of the breach of the provisions of the DPDP Act or DPDP rules, as the case may be, committed by any person. The maximum imposable penalty in case of breach as aforesaid is described under the Schedule to the DPDP Act.

Contravention	Maximum Penalty
Failure to implement reasonable security safeguards resulting in a personal data breach under Section 8(5)	Up to ₹250 Crore
Failure to notify the Data Protection Board or affected Data Principal about personal data breach under Section 8(6)	Up to ₹200 Crore

Contravention	Maximum Penalty
Non-compliance with obligations relating to children under Section 9	Up to ₹200 Crore
Failure to comply with additional obligations of Significant Data Fiduciaries under Section 10	Up to ₹150 Crore
Breach in observance of Duties by Data Principal under Section 15	Up to ₹10K
Breach of any term of voluntary undertaking accepted by the Board under Section 32	Upto the extent applicable for the breach in respect of which the proceedings under Section 28 were instituted
Violation of other provisions of the Act	Up to ₹50 Crore

Note

- The Data Protection Board considers factors such as the nature, gravity, duration, and impact of the breach, as well as any mitigating measures taken by the Data Fiduciary, before determining the appropriate penalty (*Refer Section 33 of the Act*).

Data Protection Board of India (Chapter V)

The DPDP Act establishes the Data Protection Board of India (“Board”) to perform the functions (*as elucidated under, inter alia, Section 27 of the Act*) assigned to it under the Act, including inquiries into specified non-compliance and the imposition of monetary penalties.

The Board performs several important functions, including:

- Receiving and inquiring into complaints relating to non-compliance with the Act;
- Directing remedial measures where necessary;
- Imposing monetary penalties in accordance with the Schedule to the Act;
- Accepting voluntary undertakings from Data Fiduciaries; and
- Performing such other functions as may be assigned under the Act.

The Act also provides for appeals against the orders of the Board before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

The Act establishes the Data Protection Board of India as the regulatory body responsible for dealing with contraventions of the Act and performing the functions assigned to it. Rules 17–22 of the DPDP Rules provide the procedural framework with regard to the appointments, meetings, digital functioning, staffing and appeals thereto.

Rule 17 — Appointment of Chairperson and Members

The Central Government constitutes Search-cum-Selection Committees for recommending individuals for appointment as Chairperson and for appointment as other Members of the Board. The committees include specified senior government officials and two experts of repute having special knowledge or practical experience in a field considered useful to the Board. The Central Government appoints the Chairperson or Member after considering the suitability of the recommended individuals.

Rule 18 and Fifth Schedule — Service Conditions

The salary, allowances and other terms and conditions of service of the Chairperson and Members of the Board are governed by the Fifth Schedule. The Schedule deals with salary, provident fund, pension and gratuity, travel, medical assistance, leave, leave travel concession and other service conditions, including conflict-of-interest requirements.

The Fifth Schedule provides a consolidated monthly salary of ₹4.5 lakh for the Chairperson and ₹4 lakh for each other Member, without the facility of a house or car, along with the specified service benefits and conditions.

Rule 19 — Procedure of the Board

- The Chairperson fixes the date, time and place of meetings and approves the agenda.

- The Chairperson presides over meetings; in her absence, the Members present choose another Member to chair the meeting.
- One-third of the Board's membership constitutes the quorum.
- Questions are decided by majority vote of Members present and voting. In case of equality, the Chairperson or person chairing the meeting, as the case maybe, has a casting vote.
- A Member having an interest in an item of business cannot participate or vote on that item.
- In an emergent situation where a meeting cannot feasibly be called, the Chairperson may take necessary action for recorded reasons, which must be communicated to Members within seven days and placed before the Board for ratification at its next meeting.
- An item may be decided by circulation where directed by the Chairperson and approved by a majority of Members.
- Orders, directions and instruments may be authenticated by the Chairperson, a Member or an authorised individual.
- An inquiry is ordinarily to be completed within **six months** from receipt of the relevant intimation, complaint, reference or direction under Section 27 of the Act. The said period of 6 months may be extended for reasons, recorded in writing, by further periods of not more than three months at a time.

Rule 20- Digital Office

The Board functions as a digital office. It may adopt techno-legal measures so that proceedings can be conducted without requiring the physical presence of individuals, while retaining its statutory power to summon persons and examine them on oath.

Rule 21 and Sixth Schedule -Board Officers and Employees

With prior approval of the Central Government, the Board may appoint officers and employees necessary for the efficient discharge of its functions. The Sixth Schedule sets out service conditions, including deputation, gratuity, travel, medical assistance, leave, leave travel concession and conduct/service rules.

Rule 22 -Appeals

A person aggrieved by an order or direction of the Board may prefer an appeal before the Appellate Tribunal. The appeal is to be filed in digital form in the manner decided by the Appellate Tribunal.

The appeal carries a fee equivalent to the fee applicable to an appeal under the Telecom Regulatory Authority of India Act, 1997, unless the Chairperson of the Appellate Tribunal reduces or waives such fee. The fee is payable digitally through UPI or another payment system authorised by the Reserve Bank of India.

The Appellate Tribunal is not bound by the Code of Civil Procedure, 1908, but is guided by the principles of natural justice and may regulate its own procedure subject to the Act. It also functions as a digital office and may use techno-legal measures to conduct proceedings without requiring physical presence.

◆ Practical Implication

Organisations should maintain record of notices, submissions, incident records, compliance evidence and decision trails in a form that can be retrieved and produced electronically if regulatory proceedings arise.

Rule 23 and Seventh Schedule: Government Requests for Information

Rule 23 gives the Central Government a mechanism to call for information from a Data Fiduciary or intermediary for specified purposes under the Act. The request is made through the authorised person identified in the Seventh Schedule and must be complied with within the period specified in the request.

Purpose (as mentioned in the Seventh Schedule)	Authorised Person / Effect
Use by the State or its instrumentalities, of the personal data of a Data Principal, in the interest of India's sovereignty and integrity or security of the State	The officer of the State or its instrumentality designated under the relevant statutory mechanism.
Performance of a function under law or disclosure of information required by law	The person authorised under the applicable law.
Assessment for notifying a Data Fiduciary or class of Data Fiduciaries as an SDF	The designated officer in MeitY specified in the Seventh Schedule.

Where disclosure of the fact that information has been furnished is likely to prejudice the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary not to disclose that fact to the affected Data Principal or any other person without prior written permission of the authorised person.

For Rule 23, the term “intermediary” carries the meaning assigned to it under the Information Technology Act, 2000.

The Seven Schedules - Quick Reference

Schedule	Subject	Why it Matters
First Schedule	Consent Managers	Registration conditions and detailed operational, transparency, security, audit and conflict-of-interest obligations.
Second Schedule	State processing and research/archiving/statistical processing	Sets standards on lawfulness, purpose, necessity, accuracy, retention, security, notice/contact information and accountability.
Third Schedule	Specified erasure periods	Sets the three-year deemed-purpose period for specified large e-commerce entities, online gaming intermediaries and social media intermediaries.

Schedule	Subject	Why it Matters
Fourth Schedule	Exemptions in relation to personal data of Child	Lists specified Data Fiduciaries and purposes for which Sections 9(1) and 9(3) do not apply, subject to conditions.
Fifth Schedule	Board Chairperson and Members	Sets salary, allowances and service conditions.
Sixth Schedule	Board officers and employees	Sets appointment and service conditions.
Seventh Schedule	Power to call for information	Identifies the purposes and authorised persons relevant to Rule 23 and the one-year retention requirement in Rule 8(3).

DPDP Act, 2023 - Compliance Checklist

The following checklist provides an overview of the key compliance measures that organisations should consider while implementing the requirements of the Digital Personal Data Protection Act, 2023 (“DPDP Act”). Depending on the nature, scale, and complexity of processing activities, additional measures may be required.

Compliance Requirement	Status
Identify whether the organisation acts as a Data Fiduciary or Data Processor. For the check, whether the organization is involved in collection of digital personal data in any manner.	☐
Map all categories of digital personal data collected, processed, stored, and shared. Also, Identify the manner and source of collection of such digital personal data.	☐
Identify the lawful basis for processing (Consent or Legitimate Use).	☐
Prepare and publish a clear and accessible Privacy Notice.	☐
Obtain valid consent before processing personal data, where required.	☐
Implement a mechanism for withdrawal of consent.	☐
Establish procedures for handling Data Principal requests (access, correction, erasure, grievance, nomination).	☐
Maintain reasonable technical and organisational security safeguards.	☐
Develop and implement a Personal Data Breach Response Plan.	☐
Establish a grievance redressal mechanism and designate responsible personnel.	☐
Ensure contracts with Data Processors contain appropriate data protection obligations.	☐
Erase personal data once the purpose of processing is fulfilled, unless retention is required by law.	☐
Conduct periodic review of privacy policies, security controls, and compliance measures.	☐
Assess whether the organisation qualifies as a Significant Data Fiduciary and comply with additional obligations, if notified.	☐
Train employees on privacy, cybersecurity, and data protection practices. Conduct regular due diligence regarding the compliances.	☐
Confirm which Rules are in force for the relevant compliance date and maintain a commencement calendar.	☐

Compliance Requirement	Status
Review every privacy notice for Rule 3: standalone presentation, plain language, itemised data, specified purposes, goods/services or uses, withdrawal route, rights route and Board complaint route.	☐
If the organisation proposes to operate as a Consent Manager, assess all First Schedule registration conditions and obligations.	☐
For State processing under Section 7(b), document compliance with the Second Schedule standards.	☐
Review security architecture against Rule 6, including encryption/obfuscation/masking/tokenisation, access control, logging, monitoring, backups, processor contracts and technical/organisational measures.	☐
Build a breach response workflow capable of sending affected-Data-Principal communications without delay and providing the Board's detailed information within 72 hours, subject to any permitted extension.	☐
Identify whether the organisation falls within the Third Schedule thresholds and establish the relevant erasure and 48-hour pre-erasure notice process.	☐
Separate the Rule 6 one-year security retention requirement from the Rule 8(3) one-year Seventh Schedule retention requirement.	☐
Publish the Rule 9 business contact details of the DPO or appropriate processing-contact person.	☐
Publish the means for Data Principal rights requests and required identifiers under Rule 14.	☐
Ensure the grievance mechanism states a reasonable response period not exceeding 90 days and is supported by appropriate technical and organisational measures.	☐
Where children's data is processed, establish a Rule 10 parental age/identity verification process.	☐
Where relevant, establish Rule 11 verification of lawful guardianship for persons with disabilities.	☐
Before relying on a Fourth Schedule child-data exemption, confirm the precise class/purpose and applicable condition.	☐
For SDFs, maintain a 12-month DPIA and audit cycle and document algorithmic due diligence.	☐
Monitor Central Government specifications affecting SDF localisation.	☐
Map international transfers and monitor any requirements issued under Rule 15.	☐

Compliance Requirement	Status
Where relying on the Rule 16 research/archiving/statistical exemption, document compliance with every applicable Second Schedule standard.	☐
Maintain electronic records capable of supporting Board or appellate proceedings.	☐
Create a protocol for responding to Rule 23 information requests and assess whether any confidentiality direction applies.	☐

Quick Compliance Roadmap

Seven-Step Roadmap to DPDP Act Compliance

1. Assess Determine the organisation's role and data flows.	2. Map Inventory all categories of personal data processed.
3. Establish Legal Basis Identify consent or legitimate use for each activity.	4. Notify Publish clear, accessible privacy notices.
5. Safeguard Implement technical and organisational security measures.	6. Enable Rights Build mechanisms for access, correction, erasure and grievances.
7. Review Periodically audit and update the compliance framework.	

Best Practices

- Adopt a Privacy by Design approach.
- Collect only the minimum personal data necessary.
- Periodically review and update privacy notices.
- Implement appropriate technical and organisation measures to protect personal data
- Train employees on data protection obligations.
- Maintain documentation to demonstrate compliance.
- Regularly assess third-party vendors and Data Processors.

Final Takeaway

- Compliance with the DPDP Act is not a one-time exercise, but an ongoing governance process. Organisations should embed privacy into their business operations, periodically review their compliance framework, and foster a culture of accountability. A proactive approach to data protection not only reduces regulatory risk but also strengthens stakeholder confidence and supports sustainable digital growth.

From the Editor's Desk

THE MINDS BEHIND THIS HANDBOOK

Mohit Khandelwal

Advocate, Rajasthan High Court

Adv. Mohit Khandelwal is a practising advocate and the founder of Mohit Khandelwal & Associates (MKA). He is a Gold Medalist from National Law University, Punjab, holds an LL.M. in Business Laws, and is a qualified Company Secretary.

This handbook has been compiled and edited with the intent to spread the awareness of this evolving area of law. In order to prepare a reader friendly content, we have taken the assistance from the AI tools, however, the content of the compilation has been prepared in consonance with the DPDPA Act and the Rules made thereunder. Further, it is a free content which has been created solely for academic and reading purposes. This should not be used for any commercial advantage. This content may not be relied for any professional advice.

I recognize the efforts made by Advocate Prakruti Sharma and Advocate Chetanaya Sharma in finalizing this compilation.

MOHIT KHANDELWAL & ASSOCIATES

Advocates & Consultants

E:mkalegal.jaipur@gmail.com

W: www.mkajaipur.com

P:141-4036587

A GLIMPSE OF THE TEAM

Mohit Khandelwal		
Aditi Gupta	Aditya Gupta	Pranav Sharma
Chetan Pareek	Keshav Dadhich	Prakruti Sharma
Prakhar Choudhary	Harsh Khandelwal	Arpit Khandelwal
Rajendra Choudhary	Sourabh Kuntal	Chaitanya Agarwal