

**THE DIGITAL PERSONAL DATA
PROTECTION ACT, 2023
AND
THE DIGITAL PERSONAL DATA
PROTECTION RULES, 2025**

FAQs

FOREWORD

The increasing use of personal data in commercial activities, public administration and everyday digital interactions has made data protection an essential part of India's legal framework. The Digital Personal Data Protection Act, 2023 recognises the right of individuals to protect their personal data and the need to process such data for lawful purposes. It establishes a statutory framework governing the processing of digital personal data, with responsibilities for entities determining the purposes and means of processing and rights for the individuals to whom the data relates.

The Digital Personal Data Protection Rules, 2025, notified in November 2025, provide the detailed requirements for implementing this framework. The Act and the Rules are being brought into force in phases, with institutional provisions taking effect first, followed by provisions relating to Consent Managers and the principal obligations governing data processing. As of September 2026, the framework remains in transition, with the main compliance requirements scheduled to take effect in May 2027 under the notified implementation schedule.

The Act covers personal data collected digitally and data collected in non-digital form and subsequently digitised, subject to its exclusions and exemptions. Its scope also extends to processing outside India in connection with offering goods or services to individuals within India. Consent is a principal basis for processing, alongside the "certain legitimate uses" specified under the Act. Where consent is relied upon, it must meet the statutory requirements and relate to the personal data necessary for the specified purpose.

The framework addresses accountability throughout the handling of personal data through requirements relating to notices, security safeguards, retention, erasure and grievance redressal. The Rules specify measures for protecting personal data, including appropriate access controls, monitoring, continuity arrangements and contractual safeguards for processing undertaken on behalf of a Data Fiduciary. They also prescribe notification of personal data breaches to affected individuals and the Data Protection Board of India, including initial intimation without delay and further reporting to the Board within the prescribed period.

Individual rights form another central part of the framework, including access to information about processing, correction and erasure of personal data, grievance redressal and nomination. Additional safeguards address children's personal data, and enhanced obligations apply to entities designated as Significant Data Fiduciaries. The enforcement framework provides for inquiries into breaches, remedial directions and monetary penalties, with the statutory maximum for failure to take reasonable security safeguards extending to INR 250 crore.

This booklet presents the principal provisions of the Act and the Rules through frequently asked questions, covering their scope, consent and legitimate uses, the obligations of Data Fiduciaries, individual rights, security safeguards, breach reporting, cross-border processing and enforcement. It aims to provide a clear and accessible reference for understanding the legal framework and its phased implementation.

CONTENTS

1. What is the Digital Personal Data Protection Act, 2023?.....	5
2. What are the Digital Personal Data Protection Rules, 2025, and how do they supplement the Act?.....	5
3. When do the Act and the Rules come into force?	5
4. What is Personal Data and Digital Personal Data?.....	5
5. Who is a Data Principal?.....	6
6. Which processing activities fall within the territorial scope of the Act?	6
7. What activities constitute processing of digital personal data?	6
8. What are the key exemptions from the applicability of the Act?	7
9. Who is a Data Fiduciary and Data Processor?	7
10. Who is a Significant Data Fiduciary?.....	7
11. Which organisations need to register with the Board or appoint a Data Protection Officer? ..	7
12. What are the lawful grounds for processing personal data?	7
13. What are the legitimate uses and how do they differ from deemed consent?.....	8
14. Can employers process employee personal data without consent?.....	8
15. What constitutes valid consent?	8
16. What information must a privacy notice contain?.....	9
17. What happens to consent obtained before the relevant provisions commence?	9
18. How can consent be withdrawn and what follows withdrawal?.....	9
19. What is a Consent Manager and is its use mandatory?	10
20. What requirements apply to Consent Managers?	10
21. What are the principal obligations of a Data Fiduciary under the Act?.....	10
22. What responsibilities apply when processing is outsourced?.....	11
23. What security safeguards are prescribed?	11
24. What constitutes a personal data breach?.....	12
25. Who must be notified of a breach and within what period?	12
26. What does the 3-year inactivity period mean?	12
27. What separate 1-year retention obligation does Rule 8 impose?.....	13
28. What contact information must organisations publish?.....	13
29. What are the requirements for processing the personal data of children?	13
30. How must a Data Fiduciary verify parental consent?.....	14

31. What exemptions are available for processing children’s personal data, and in what circumstances do they apply?.....	14
32. What requirements apply to processing personal data of persons with disabilities?	15
33. What additional obligations apply to Significant Data Fiduciaries?	15
34. What information can a Data Principal request?	15
35. How can individuals seek correction or erasure?	16
36. How are rights requests submitted?	16
37. How can grievances be raised?	16
38. Can another individual be nominated to exercise rights?	16
39. What duties must Data Principals observe?	17
40. Can personal data be transferred outside India?	17
41. What conditions govern processing by the State?	17
42. What exemptions apply to legal claims, judicial functions and other specified activities? ...	18
43. What exemption applies to research, archiving and statistics?.....	18
44. Are startups and smaller organisations automatically exempt?	18
45. What other State and notification-based exemptions are provided?.....	18
46. What is the Data Protection Board of India?	19
47. How does the Board conduct inquiries?	19
48. Can a dispute be resolved through mediation or a voluntary undertaking?	19
49. How can an order of the Board be appealed?	20
50. What monetary penalties may be imposed?	20
51. Does the Act provide compensation to affected individuals?.....	20
52. Can repeated contraventions result in blocking directions?	21
53. Can the Government require information from organisations?	21
54. How does the DPDP framework interact with the IT Act and other laws?	21
55. What organisational measures are required to give effect to the Act and Rules?	22
PRIVACY AND DATA PROTECTION OFFERINGS BY LEXORBIS	23

1. What is the Digital Personal Data Protection Act, 2023?

The Digital Personal Data Protection Act, 2023 (DPDP Act or Act) establishes a framework for processing digital personal data that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes. It specifies the obligations of Data Fiduciaries, the rights and duties of Data Principals, the functions of the Data Protection Board of India and the monetary penalties for contraventions.

The Act received Presidential assent on August 11, 2023. Section 1(2) authorises the Central Government to appoint different commencement dates for different provisions, and the provisions have been brought into force in phases through the notification dated November 13, 2025.

2. What are the Digital Personal Data Protection Rules, 2025, and how do they supplement the Act?

The Digital Personal Data Protection Rules, 2025 (Rules) were notified through G.S.R. 846(E), dated November 13, 2025, under Section 40 of the DPDP Act. The Rules prescribe requirements for notices, Consent Managers, security safeguards, breach notifications, retention and erasure, parental and guardian consent, Significant Data Fiduciaries, individual rights, the Board and appeals.

3. When do the Act and the Rules come into force?

The Act and the Rules have a phased commencement framework. Under the notification dated November 13, 2025, certain institutional and administrative provisions of the Act came into force upon publication, while other provisions are scheduled to commence 1 year or 18 months after publication.

Date and Status	Provisions of the Act	Provisions of the Rules
November 13, 2025 Commenced	Section 1(2); Section 2; Sections 18-26; Sections 35, 38-43; and Sections 44(1) and 44(3).	Rules 1, 2 and 17-21.
November 13, 2026 Scheduled	Section 6(9) and Section 27(1)(d), relating to Consent Manager registration and breaches of registration conditions.	Rule 4 on registration and obligations of Consent Managers.
May 13, 2027 Scheduled	Sections 3-5; Sections 6(1)-(8) and 6(10); Sections 7-17; Section 27 other than Section 27(1)(d); Sections 28-34, 36 and 37; and Section 44(2).	Rules 3, 5-16, 22 and 23.

Accordingly, all the Rules do not become operational simultaneously, and organisations must consider the applicable commencement date for each obligation.

4. What is Personal Data and Digital Personal Data?

Section 2(t) defines “personal data” as data of an individual who is identifiable by or in relation to that data. The definition covers information that identifies an individual directly and information through which the individual can be identified in conjunction with other available information.

Section 2(n) defines “digital personal data” as personal data in digital form, and Section 3 extends the Act to data collected digitally as well as data collected in non-digital form and subsequently digitised.

The application of the Act depends on whether the information relates to an identifiable individual. Information that has been irreversibly anonymised so that the individual is no longer identifiable falls outside this definition, but replacing a name with a code does not have that effect if the information can still be linked to the individual.

5. Who is a Data Principal?

Under Section 2(j), a “Data Principal” is the individual to whom the personal data relates. Where the individual is a child, the definition includes the parents or lawful guardian of that child, and where the individual is a person with a disability, it includes the lawful guardian acting on that individual’s behalf.

The inclusion of a lawful guardian must be read with Section 9(1) and Rule 11, which address persons with disabilities who have a lawful guardian and prescribe the verification required before consent is accepted from that guardian. These provisions do not require every individual with a disability to exercise rights or provide consent through another person.

6. Which processing activities fall within the territorial scope of the Act?

Section 3 applies to the processing of digital personal data within India where the data is collected in digital form or is collected in non-digital form and digitised subsequently. It also applies to processing outside India where the processing is connected with an activity relating to the offering of goods or services to Data Principals within India.

The territorial application is determined by the circumstances of the processing and the connection specified in Section 3, rather than solely by the place of incorporation of the organisation or the citizenship of the individual. An organisation located outside India may fall within the Act when its processing is connected with offering goods or services to individuals within India.

7. What activities constitute processing of digital personal data?

Section 2(x) defines processing as a wholly or partly automated operation or set of operations performed on digital personal data, including:

- a) Collecting or recording personal data.
- b) Organising, structuring, indexing, or storing personal data.
- c) Retrieving or using personal data.
- d) Adapting, aligning, or combining personal data.
- e) Sharing or disclosing by transmission, dissemination, or otherwise making personal data available.
- f) Restricting, erasing, or destroying personal data.

The definition covers the handling of digital personal data throughout its lifecycle, including storage and deletion, and is not confined to its collection or disclosure. Personal data maintained exclusively in non-digital form remains outside the scope of the Act unless it is subsequently digitised.

8. What are the key exemptions from the applicability of the Act?

The DPDP Act shall not apply to the following:

1. Personal data processed by an individual for any personal or domestic purpose and
2. Personal data that is made or caused to be made publicly available by
 - (a) the Data Principal to whom such personal data relates; or
 - (b) Any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

9. Who is a Data Fiduciary and Data Processor?

A “Data Fiduciary” is a person who determines the purpose and means of processing personal data, either alone or in conjunction with other persons, and a “Data Processor” is a person who processes personal data on behalf of a Data Fiduciary. The distinction depends on the role performed in relation to the processing activity. For example, an organisation that determines how customer data will be used acts as a Data Fiduciary, and a service provider engaged to process that data on its behalf acts as a Data Processor to the extent of that engagement.

Section 2(s) defines a person to include an individual, a Hindu undivided family, a company, a firm, an association or body of individuals, the State and other artificial juristic persons. The same organisation may act as a Data Processor for activities undertaken on another organisation’s behalf and as a Data Fiduciary for activities whose purpose and means it determines independently.

10. Who is a Significant Data Fiduciary?

A “Significant Data Fiduciary” is a Data Fiduciary or class of Data Fiduciaries designated by Central Government notification. The assessment factors include:

- The volume and sensitivity of personal data.
- Risks to individual rights.
- Potential effects on India’s sovereignty and integrity.
- Risks to electoral democracy, State security and public order.

11. Which organisations need to register with the Board or appoint a Data Protection Officer?

The Act requires a person acting as a Consent Manager to obtain registration with the Board under Section 6(9) and Rule 4. It does not impose a corresponding general registration requirement on every Data Fiduciary or Data Processor.

Section 10(2) requires a Significant Data Fiduciary to appoint a Data Protection Officer who is based in India and is responsible to its board of directors or a similar governing body. Other Data Fiduciaries are required under Section 8(9) and Rule 9 to publish the business contact information of a person who can answer questions about the processing of personal data on their behalf, and Section 8(10) requires an effective grievance-redressal mechanism.

12. What are the lawful grounds for processing personal data?

Personal data may be processed in accordance with the Act for a lawful purpose on the basis of consent or for one of the certain legitimate uses specified in Section 7. A lawful purpose is a purpose not expressly forbidden by law.

An organisation must identify the applicable ground for each processing activity and remain within its conditions. A commercial interest or a contractual relationship is not an additional general processing ground under Section 4.

13. What are the legitimate uses and how do they differ from deemed consent?

Section 7 permits processing for specified purposes without obtaining consent under Section 6, subject to the conditions of the relevant clause. These uses cover:

1. Data voluntarily provided for a specified purpose without an indication of non-consent.
2. Prescribed State benefits and services subject to the statutory conditions.
3. Performance of State functions under law or specified sovereign and security interests.
4. Legally required disclosures to the State.
5. Compliance with Indian judgments, decrees or orders and specified foreign civil or contractual judgments or orders.
6. Medical emergencies.
7. Public-health measures; disaster or public-order responses.
8. Specified employment purposes or those related to safeguarding the employer from loss or liability.

The Act describes these grounds as certain legitimate uses rather than deemed consent. Each ground is limited by its statutory conditions, and voluntary provision of data for one purpose does not permit its use for an unrelated purpose. The statutory illustration of a customer providing a telephone number for a purchase receipt demonstrates the application of Section 7(a) to the particular purpose for which the number was supplied.

14. Can employers process employee personal data without consent?

Section 7(i) permits processing for employment purposes or purposes relating to safeguarding the employer from loss or liability. The provision gives examples including prevention of corporate espionage, protection of trade secrets, intellectual property and classified information, and provision of a service or benefit sought by an employee.

The provision does not exempt employee data from the entire Act. The employer must assess whether the activity falls within Section 7(i) and comply with the other applicable requirements, including security safeguards and relevant retention obligations.

15. What constitutes valid consent?

Section 6 requires consent to be free, specific, informed, unconditional and unambiguous, and to be expressed through a clear affirmative action. Consent must signify agreement to processing for the specified purpose and must be limited to the personal data necessary for that purpose. Any part of consent that infringes the Act, the Rules or another applicable law is invalid to the extent of the infringement.

A request for consent must be presented in clear and plain language, with an option to access it in English or a language specified in the Eighth Schedule to the Constitution. It must include the contact details of the Data Protection Officer, where applicable, or another person authorised to respond to communications relating to the exercise of Data Principal rights. Under Section 6(10), the Data Fiduciary bears the burden of proving that the required notice was given and consent was obtained in accordance with the law when the issue arises in proceedings.

16. What information must a privacy notice contain?

Section 5 requires a notice to accompany or precede every request for consent under Section 6. The Data Principal must be given the option to access the notice in English or a language specified in the Eighth Schedule to the Constitution. Rule 3 requires the notice to be understandable independently of other information provided by the Data Fiduciary and to contain sufficient detail in clear and plain language to enable specific and informed consent. The notice must contain:

- An itemised description of the personal data to be processed.
- The specified purposes of processing and an itemised description of the goods, services or uses enabled by that processing.
- The manner of withdrawing consent and seeking grievance redressal.
- The manner of making a complaint to the Board.
- The particular communication link for the website or app and details of other available means through which the individual may withdraw consent, exercise rights and make a complaint to the Board.

17. What happens to consent obtained before the relevant provisions commence?

Section 5(2) applies where the Data Principal gave consent before commencement of the relevant provision. It requires the Data Fiduciary to give the prescribed notice as soon as reasonably practicable after commencement, identifying the personal data and the purpose for which it has been processed, the manner of withdrawing consent and seeking grievance redressal, and the manner of making a complaint to the Board.

The provision permits the Data Fiduciary to continue processing until the individual withdraws consent. It provides a transitional notice requirement for existing consent-based processing without requiring fresh consent in every case solely because the provision has commenced. The continued processing remains subject to the scope of the consent and the other applicable requirements of the Act and Rules.

18. How can consent be withdrawn and what follows withdrawal?

Under Section 6(4), a Data Principal may withdraw consent at any time, and the ease of withdrawal must be comparable to the ease with which consent was given. Withdrawal does not affect the legality of processing undertaken on the basis of consent before its withdrawal, and the consequences of withdrawal are borne by the individual.

Section 6(6) requires the Data Fiduciary, within a reasonable time, to cease the processing and cause its Data Processors to do the same, unless continued processing without consent is required or authorised by the Act, the Rules or any other Indian law. The effect of withdrawal on an existing service depends on the processing required for that service and any continuing legal obligations. For example, the statutory illustration permits an online shopping service to stop accepting further orders after withdrawal but recognises continued processing for goods already ordered and paid for. Erasure of retained records is governed separately by Section 8(7), Rule 8 and applicable legal retention requirements.

19. What is a Consent Manager and is its use mandatory?

A “Consent Manager” is a person registered with the Board who acts as a single point of contact through which a Data Principal may give, manage, review and withdraw consent using an accessible, transparent and interoperable platform. Sections 6(7) and 6(8) provide for this method of managing consent and require the Consent Manager to remain accountable to the Data Principal and act on that individual’s behalf.

The Act permits the use of a Consent Manager without making that route mandatory for every consent transaction. The statutory status arises through registration under Section 6(9) and Rule 4, and is distinct from merely supplying software that helps an organisation maintain its own consent records.

20. What requirements apply to Consent Managers?

Rule 4 and the First Schedule prescribe the conditions for registration and the obligations of Consent Managers. An applicant must be a company incorporated in India with adequate technical, operational and financial capacity, a net worth of at least INR 2 crore, suitable management and governance arrangements, and the independent certification required for its platform. Registration is granted by the Board after it is satisfied that the prescribed conditions are met.

The First Schedule requires a Consent Manager to:

- Maintain records of consent given, denied or withdrawn, notices preceding or accompanying consent requests, and the relevant sharing of personal data.
- Provide the Data Principal with access to those records and enable requests for information in machine-readable form in accordance with the platform’s terms of service.
- Retain the records for at least 7 years, or for a longer period agreed with the individual or required by law.
- Ensure that the contents of personal data made available or shared through the platform are not readable by the Consent Manager.
- Implement reasonable security safeguards and act in a fiduciary capacity towards Data Principals.
- Comply with the prescribed conflict-of-interest, disclosure and audit requirements.
- Refrain from subcontracting or assigning its obligations under the Act and Rules.

Rule 4 empowers the Board to require corrective measures and, after following the prescribed procedure, suspend or cancel registration.

21. What are the principal obligations of a Data Fiduciary under the Act?

A Data Fiduciary is responsible for ensuring that personal data is processed in accordance with the Act and applicable Rules. Its key obligations include:

- Processing personal data for a lawful purpose and on a valid legal basis.
- Providing Data Principals with the required notice and obtaining valid consent, where applicable.
- Ensuring the accuracy and completeness of personal data where it is likely to be used to make decisions affecting a Data Principal or disclosed to another Data Fiduciary.

- Implementing reasonable security safeguards to prevent personal data breaches.
- Notifying the Data Protection Board and affected Data Principals in the event of a personal data breach.
- Erasing personal data when the purpose is no longer served, subject to applicable legal retention requirements.
- Establishing an accessible grievance-redressal mechanism and facilitating the exercise of Data Principal rights.
- Ensuring that its Data Processors process personal data under a valid contract and appropriate safeguards.

The Data Fiduciary remains responsible for compliance even where processing is undertaken on its behalf by a Data Processor.

22. What responsibilities apply when processing is outsourced?

Under Section 8(2), a Data Fiduciary may engage, appoint or otherwise involve a Data Processor for activities relating to the offering of goods or services to Data Principals only under a valid contract. The engagement does not transfer the Data Fiduciary's statutory responsibility, since Section 8(1) expressly extends that responsibility to processing carried out on its behalf.

The contractual arrangements must support compliance with the obligations applicable to the processing. Rule 6 requires appropriate contractual provisions for reasonable security safeguards, and Section 8(7) requires the Data Fiduciary to cause its processor to erase personal data when erasure is required. A processor's failure to perform its contractual obligations does not, by itself, relieve the Data Fiduciary of responsibility under the Act.

23. What security safeguards are prescribed?

Section 8(5) requires reasonable security safeguards to prevent personal data breaches in respect of personal data in the possession or under the control of a Data Fiduciary, including data processed on its behalf. Rule 6 prescribes the following minimum safeguards:

- Appropriate data security measures, such as encryption, obfuscation, masking or virtual tokens mapped to personal data.
- Access controls for the computer resources used by the Data Fiduciary or its Data Processor, as applicable.
- Logs, monitoring and review that provide visibility into access and enable unauthorised access to be detected, investigated and remedied.
- Measures to ensure continued processing following compromise of the confidentiality, integrity or availability of personal data, including appropriate backups.
- Retention of the relevant logs and personal data for 1 year to support detection, investigation, remediation, prevention of recurrence and continued processing, unless another applicable law requires otherwise.
- Appropriate contractual provisions requiring Data Processors to implement reasonable security safeguards.
- Technical and organisational measures to ensure effective observance of the safeguards.

24. What constitutes a personal data breach?

Section 2(u) defines a personal data breach as unauthorised processing of personal data, or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises its confidentiality, integrity or availability. The definition extends beyond disclosure to an unauthorised recipient and can include an event that corrupts personal data or makes it unavailable.

Whether an event is a personal data breach depends on these statutory elements. The notification obligation under Section 8(6) and Rule 7 does not prescribe a separate threshold of likely harm or significant risk that must be established before a qualifying breach is reported.

25. Who must be notified of a breach and within what period?

Section 8(6) requires a Data Fiduciary to notify the Board and each affected Data Principal of a personal data breach in the prescribed manner. Under Rule 7, the notification to an affected individual must be made without delay after the Data Fiduciary becomes aware of the breach, through the individual's user account or a registered mode of communication, using clear and plain language.

The notification to affected Data Principals must include:

- The nature, extent and timing of the breach.
- The consequences likely to be relevant to the affected individual.
- The measures implemented or being implemented to mitigate risk.
- The safety measures the individual may take to protect their interests.
- The business contact information of a person able to respond to queries on behalf of the Data Fiduciary.

The Board must also be informed without delay. The initial intimation must describe the nature, extent, timing and location of the breach and its likely impact. Within 72 hours of becoming aware of the breach, the Data Fiduciary must provide the following further information, unless the Board allows a longer period on a written request:

- Updated and detailed information about the breach.
- The broad facts relating to the events, circumstances and reasons leading to the breach.
- The measures implemented or proposed to mitigate risk, if any.
- Any findings regarding the person who caused the breach.
- The remedial measures taken to prevent recurrence.
- A report of the intimations provided to affected Data Principals.

26. What does the 3-year inactivity period mean?

Rule 8(1), read with the Third Schedule, prescribes an inactivity period for the classes of Data Fiduciaries and purposes. The period is 3 years from the date on which the Data Principal last approached the Data Fiduciary for performance of the specified purpose or exercised rights in relation to the processing, or from commencement of the Rules, whichever is later.

Where the prescribed conditions are met, the purpose is deemed no longer to be served, and the data must be erased unless retention is necessary for compliance with law. This is a rule for determining when specified processing purposes cease to be served; it does not require every Data Fiduciary to retain all personal data for 3 years. The Schedule excludes processing to

enable access to a user account or to a virtual token issued by or on behalf of the Data Fiduciary, stored on its digital facility or platform and usable to obtain money, goods or services. For this purpose, an e-commerce entity does not include a seller merely offering goods or services on a marketplace platform.

Class of Data Fiduciary	Registered users in India
E-commerce entity	At least 2 crore
Online gaming intermediary	At least 50 lakh
Social media intermediary	At least 2 crore

Under Rule 8(2), the Data Fiduciary must inform the Data Principal at least 48 hours before the applicable period expires that the data will be erased unless the individual logs into the user account, otherwise initiates contact for the specified purpose or exercises rights in relation to the processing. The notice gives the individual an opportunity to act before erasure, and any legal requirement for continued retention remains applicable.

27. What separate 1-year retention obligation does Rule 8 impose?

Rule 8(3) requires a Data Fiduciary to retain personal data, associated traffic data and other logs relating to the processing for a minimum period of 1 year from the date of processing, for the purposes specified in the Seventh Schedule. The obligation applies to processing carried out by the Data Fiduciary and processing undertaken on its behalf by a Data Processor.

After the minimum period, the data and logs must be erased unless further retention is required by another law or by a notification of the Central Government. This obligation is distinct from the 3-year inactivity provision in Rule 8(1) and the security-related retention requirement in Rule 6(1)(e), and each provision must be applied to the records and purposes it covers.

28. What contact information must organisations publish?

Section 8(9) requires a Data Fiduciary to publish the business contact information of its Data Protection Officer, where applicable, or a person able to answer questions raised by Data Principals about the processing of their personal data. Rule 9 requires that information to be displayed prominently on the Data Fiduciary's website or app and included in every response to a communication through which a Data Principal exercises rights under the Act.

The contact must provide an effective means of addressing questions about the processing. For a Significant Data Fiduciary, Section 10(2)(a) separately requires the Data Protection Officer to represent the organisation under the Act and serve as the point of contact for grievance redressal.

29. What are the requirements for processing the personal data of children?

Section 2(f) defines a child as an individual who has not completed 18 years of age. Under Section 9(1), a Data Fiduciary must obtain verifiable consent from the child's parent or lawful guardian before processing the child's personal data, subject to the exemptions authorised by the Act and Rules.

Section 9(2) prohibits processing that is likely to cause any detrimental effect on the well-being of a child. Section 9(3) separately prohibits tracking or behavioural monitoring of children and targeted advertising directed at children. The exemptions under Rule 12 and the Fourth Schedule

apply to the requirements in Sections 9(1) and 9(3) within their stated conditions; they do not remove the prohibition in Section 9(2).

30. How must a Data Fiduciary verify parental consent?

Rule 10 requires a Data Fiduciary to adopt appropriate technical and organisational measures to obtain verifiable parental consent before processing a child's personal data. It must exercise due diligence to establish that the person identifying as the parent is an adult who can be identified if required for compliance with Indian law.

The verification may rely on reliable identity and age details already available to the Data Fiduciary, or on identity and age details voluntarily provided by the individual. It may also rely on a virtual token mapped to those details and issued by an entity entrusted by law or by the Central or State Government with issuing such details or tokens, or a person appointed or permitted by that entity, including details or tokens verified and made available through a Digital Locker service provider. The Rule does not prescribe one universal document or require every parent to use the same verification method.

31. What exemptions are available for processing children's personal data, and in what circumstances do they apply?

Rule 12 and Part A of the Fourth Schedule exempt the following classes of Data Fiduciaries from Sections 9(1) and 9(3), only to the extent and for the purposes specified in the Schedule:

- Healthcare professionals and clinical or mental-health establishments processing personal data as necessary for the child's health.
- Allied healthcare professionals processing personal data to support treatment or referral.
- Educational institutions undertaking tracking or behavioural monitoring for educational activities or child safety.
- Persons entrusted with the care of children in a crèche or daycare centre undertaking tracking or behavioural monitoring for child safety.
- Transport providers engaged by educational, crèche or daycare institutions tracking the child's location during travel.

Part B provides exemptions for processing necessary for the following specified purposes, subject to the conditions of each entry:

- Performance of functions under law in the interests of a child.
- Provision of specified State benefits or services under Section 7(b).
- Creation of a user account restricted to communication by email.
- Determination of a child's real-time location for safety and protection.
- Prevention of access to information, services or advertisements likely to be detrimental to the child's well-being.
- Confirmation that an individual is not a child and compliance with Rule 10.

These exemptions do not remove the prohibition under Section 9(2) on processing likely to cause a detrimental effect on a child's well-being. Section 9(5) separately permits the Central Government, after being satisfied that a Data Fiduciary processes children's personal data in a verifiably safe manner, to notify the age above which that Data Fiduciary is exempt from all or specified obligations under Sections 9(1) and 9(3). Such a notification does not amend the general definition of a child or disapply Section 9(2).

32. What requirements apply to processing personal data of persons with disabilities?

Section 9(1) requires verifiable consent from the lawful guardian before processing the personal data of a person with a disability who has a lawful guardian. Rule 11 requires the Data Fiduciary to verify that the guardian was appointed by a court, a designated authority or a local-level committee under the applicable guardianship law.

The Rule identifies the guardianship framework under the Rights of Persons with Disabilities Act, 2016 and the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999. The definition covers a person who cannot make legally binding decisions despite appropriate and adequate support. The requirement depends on the statutory conditions and the existence of a lawful guardianship arrangement, rather than disability alone.

33. What additional obligations apply to Significant Data Fiduciaries?

Section 10(2) and Rule 13 impose the following additional obligations on a Significant Data Fiduciary:

- Appoint a Data Protection Officer based in India who represents it under the Act, is responsible to its board of directors or similar governing body and serves as the point of contact for grievance redressal.
- Appoint an independent data auditor to evaluate compliance with the Act.
- Undertake a Data Protection Impact Assessment and audit once every 12 months from the date of notification as a Significant Data Fiduciary, and cause the person carrying out the assessment and audit to furnish the Board with a report containing significant observations.
- Exercise due diligence to verify that algorithmic software used for hosting, display, uploading, modification, publication, transmission, storage, updating or sharing of personal data is not likely to pose a risk to Data Principal rights.

Rule 13(4) also requires measures ensuring that personal data specified by the Central Government, on the recommendations of the committee constituted for that purpose, is processed subject to the restriction that the data and traffic data relating to its flow are not transferred outside India. This restriction applies to the data specified under that mechanism, rather than automatically to every dataset held by a Significant Data Fiduciary.

34. What information can a Data Principal request?

Section 11 gives a Data Principal the right to obtain the following information from a Data Fiduciary to whom the individual has previously given consent, including consent referred to in Section 7(a):

- A summary of the personal data being processed and the processing activities.
- The identities of other Data Fiduciaries and Data Processors with whom personal data has been shared, together with a description of the data shared.
- Any other prescribed information relating to the personal data and its processing.

Section 11(2) limits the requirements concerning recipient identities and other prescribed information where data has been shared with another Data Fiduciary authorised by law to obtain it, following a written request for the prevention, detection or investigation of offences or cyber incidents, or prosecution or punishment of offences. The provision establishes a right to the specified information and does not expressly confer a general right to data portability.

35. How can individuals seek correction or erasure?

Section 12 gives a Data Principal the right to correction, completion, updating and erasure of personal data for which consent was previously given, including consent referred to in Section 7(a), in accordance with applicable legal requirements and procedures. On receiving a correction request, the Data Fiduciary must correct inaccurate or misleading data, complete incomplete data and update data that is out of date.

On receiving an erasure request, the Data Fiduciary must erase the personal data unless retention is necessary for the specified purpose or for compliance with a law in force. The right to erasure is subject to these statutory grounds for retention, and the treatment of a particular record depends on the purpose for which it remains necessary and the legal requirements applicable to it.

36. How are rights requests submitted?

Rule 14 requires a Data Fiduciary and a Consent Manager, as applicable, to publish prominently on their website or app the means through which a Data Principal may exercise rights and the particulars needed to identify the individual under their terms of service. These particulars may include a username or another identifier that enables the request to be matched to the relevant individual and processing activity.

Requests for access, correction and erasure must be made to the Data Fiduciary to whom consent was previously given, through the published means and with the required particulars. The procedure facilitates verification and handling of requests but does not replace the substantive rights and conditions prescribed in Sections 11 and 12.

37. How can grievances be raised?

Section 13 entitles a Data Principal to readily available means of grievance redressal from a Data Fiduciary or Consent Manager in respect of an act or omission relating to its obligations concerning personal data or the exercise of rights under the Act. The individual must exhaust this opportunity for redressal before approaching the Board.

Rule 14 requires publication of a reasonable period for responding to grievances, which must not exceed 90 days, and appropriate technical and organisational measures to ensure an effective response within that period. The 90-day limit relates to grievance responses and is not expressed as a general deadline for every access, correction or erasure request.

38. Can another individual be nominated to exercise rights?

Section 14 permits a Data Principal to nominate another individual to exercise the Data Principal's rights in the event of death or incapacity. Incapacity means an inability to exercise those rights because of unsoundness of mind or infirmity of body.

Rule 14 permits nomination of one or more individuals through the means provided by the Data Fiduciary, in accordance with its terms of service and applicable law. The nomination authorises exercise of the statutory rights in the stated circumstances; it does not itself create an unrestricted entitlement to use or disclose the deceased or incapacitated individual's personal data for other purposes.

39. What duties must Data Principals observe?

Section 15 requires a Data Principal to observe the following duties:

- Comply with applicable laws when exercising rights under the Act.
- Refrain from impersonating another person when providing personal data for a specified purpose.
- Refrain from suppressing material information when providing personal data for a document, unique identifier, proof of identity or proof of address issued by the State or its instrumentalities.
- Refrain from registering a false or frivolous grievance or complaint with a Data Fiduciary or the Board.
- Furnish only information that is verifiably authentic when exercising the right to correction or erasure.

Breach of these duties may attract a monetary penalty of up to INR 10,000 under the Schedule, subject to the inquiry and penalty provisions of the Act.

40. Can personal data be transferred outside India?

Section 16 authorises the Central Government to notify countries or territories to which a Data Fiduciary may not transfer personal data for processing. Section 16(2) preserves any other Indian law that provides a higher degree of protection or restriction in relation to transfers outside India, so applicable sector-specific restrictions continue to operate.

Rule 15 makes overseas transfers subject to requirements specified by the Central Government by general or special order concerning the making available of personal data to a foreign State or to a person, entity or agency under its control. This provision regulates such availability and does not itself direct organisations to disclose personal data to foreign governments.

Significant Data Fiduciaries are additionally subject to Rule 13(4) in respect of data specified by the Central Government under that provision. The legal position for a proposed transfer depends on the applicable notifications and orders, the status of the Data Fiduciary and any other law governing the data.

41. What conditions govern processing by the State?

Section 7(b) permits the State and its instrumentalities to process personal data for providing or issuing a prescribed subsidy, benefit, service, certificate, licence or permit where the individual has previously consented to such processing or the data is available in a database, register, book or other document maintained by the State or an instrumentality and notified by the Central Government. Processing under this clause must comply with the prescribed standards and any applicable government policy or law governing personal data.

Rule 5 and the Second Schedule prescribe standards that include lawful processing for the specified purpose, use of personal data limited to what is necessary, reasonable efforts to ensure completeness, accuracy and consistency, appropriate retention and security safeguards, provision of information and contact details to individuals, and accountability for observance of the standards. Section 7(c) separately permits processing for the performance of State functions under law or in the specified interests of sovereignty, integrity or State security. Any exemption under Section 17 must be assessed under its own terms.

42. What exemptions apply to legal claims, judicial functions and other specified activities?

Section 17(1) disapplies Chapter II, except Sections 8(1) and 8(5), together with Chapter III and Section 16, for the following specified processing activities:

- Processing necessary to enforce a legal right or claim.
- Processing necessary for the performance of a judicial, quasi-judicial, regulatory or supervisory function by a court, tribunal or other entrusted body.
- Processing in the interests of preventing, detecting, investigating or prosecuting an offence or a contravention of Indian law.
- Processing in India of personal data of individuals outside India under a contract with a person outside India.
- Processing necessary for specified mergers, amalgamations, demergers, arrangements, reconstructions, business transfers or divisions approved by a court, tribunal or other competent authority.
- Processing to ascertain the financial information, assets and liabilities of a person who has defaulted on a loan or advance, subject to the conditions in Section 17(1)(f).

The exemption is limited to processing that meets the relevant clause. Section 8(1), which preserves the Data Fiduciary's responsibility, and Section 8(5), which requires reasonable security safeguards, continue to apply to these activities.

43. What exemption applies to research, archiving and statistics?

Section 17(2)(b) exempts processing necessary for research, archiving or statistical purposes where the personal data is not used to take a decision specific to a Data Principal and the processing complies with the standards prescribed under the Rules.

Rule 16 makes the Second Schedule applicable to this processing. Its standards address lawful and necessary processing, limitation of data to what is required, data quality, retention, reasonable security safeguards and accountability. The exemption depends on both the nature of the activity and compliance with the prescribed standards, and is unavailable merely because an organisation describes an activity as research.

44. Are startups and smaller organisations automatically exempt?

Section 17(3) authorises the Central Government to notify Data Fiduciaries or classes of Data Fiduciaries, including startups, to which Sections 5, 8(3), 8(7), 10 and 11 do not apply. The Government must have regard to the volume and nature of the personal data processed when exercising this power.

The exemption is dependent on a notification and applies only to the provisions and persons covered by it. A startup or a smaller business is not automatically exempt by reason of its size or description, and obligations outside the notified exemption, including the applicable security and breach-notification requirements, remain relevant.

45. What other State and notification-based exemptions are provided?

Section 17(2)(a) excludes processing by an instrumentality of the State notified by the Central Government in the interests of sovereignty and integrity, State security, friendly relations with foreign States, maintenance of public order or prevention of incitement to a cognisable offence relating to those matters. It also covers processing by the Central Government of personal data furnished by such an instrumentality.

Section 17(4) separately disappplies Sections 8(7) and 12(3) to processing by the State or its instrumentalities. It also disappplies Section 12(2) where that processing is for a purpose that does not include making a decision affecting the Data Principal. These are specific statutory exemptions from the identified erasure and correction provisions.

Section 17(5) permits the Central Government, before expiry of 5 years from commencement of the Act, to notify that specified provisions will not apply to a Data Fiduciary or class of Data Fiduciaries for the period stated in the notification. The scope and duration of an exemption under this power depend on the notification issued.

46. What is the Data Protection Board of India?

The Data Protection Board of India is the body established under Section 18 to perform the functions assigned to it by the Act. The Central Government established the Board through G.S.R. 844(E), dated 13 November 2025, with its headquarters in the National Capital Region. It is a body corporate, and the Act provides for its composition, qualifications, appointment terms and functioning.

Section 27 assigns the Board functions that include directing urgent remedial or mitigation measures after a breach intimation, inquiring into specified contraventions following the statutory triggers and imposing monetary penalties where justified. Rule 20 provides for its functioning as a digital office. The Board's establishment and the commencement of its substantive inquiry and enforcement functions are governed by the separate commencement phases set out in FAQ 3.

47. How does the Board conduct inquiries?

Section 28 requires the Board to function as an independent body, observe the principles of natural justice and record reasons for its actions, orders and directions. On receiving a matter within its jurisdiction, it must first determine whether sufficient grounds exist to proceed with an inquiry; if they do not, it must close the matter for recorded reasons.

For an inquiry, the Board has the powers conferred by the Act, including specified civil-court powers relating to attendance, examination, production of documents and receipt of evidence. It must give the person affected an opportunity of being heard before issuing an interim order and must follow the statutory procedure before making a final determination. Under Rule 19(9), an inquiry must be completed within 6 months from receipt of the relevant intimation, complaint, reference or direction, subject to extensions of up to 3 months at a time for reasons recorded in writing.

48. Can a dispute be resolved through mediation or a voluntary undertaking?

Section 31 permits the Board to direct parties to attempt resolution through mediation where it considers a complaint suitable for that process. The mediation is to be undertaken through a mediator mutually agreed upon by the parties or as provided under another applicable law.

Section 32 allows the Board to accept a voluntary undertaking at any stage of proceedings concerning observance of the Act. An undertaking may require a specified action, forbearance from an action or publication of the undertaking, and the Board may vary its terms with the consent of the person giving it. Acceptance bars proceedings regarding its contents, subject to the statutory consequence of breach: non-compliance is treated as a breach of the Act, and the Board may proceed under Section 33 after giving an opportunity of being heard.

49. How can an order of the Board be appealed?

Under Section 29, a person aggrieved by an order or direction of the Board may appeal to the Telecom Disputes Settlement and Appellate Tribunal within 60 days from receipt of the order or direction. The Tribunal may admit an appeal after that period if it is satisfied that sufficient cause prevented timely filing.

Rule 22 provides for digital filing and the prescribed appeal fee, including the power of the Tribunal's Chairperson to reduce or waive the fee at her discretion. The Tribunal must give the parties an opportunity of being heard and endeavour to dispose of the appeal within 6 months from its presentation; if that period is exceeded, it must record the reasons. The Act also makes applicable the identified provisions governing further appeals from the Tribunal.

50. What monetary penalties may be imposed?

Section 33 authorises the Board to impose a monetary penalty where, after an inquiry and an opportunity of being heard, it determines that a breach of the Act or Rules is significant. The Schedule prescribes the maximum penalty for each category of contravention, as set out below.

Contravention	Maximum penalty
Failure to take reasonable security safeguards under Section 8(5)	INR 250 crore
Failure to notify the Board or affected Data Principals under Section 8(6)	INR 200 crore
Breach of additional obligations relating to children under Section 9	INR 200 crore
Breach of Significant Data Fiduciary obligations under Section 10	INR 150 crore
Breach of Data Principal duties under Section 15	INR 10,000
Breach of an accepted voluntary undertaking	Up to the applicable maximum for the underlying breach
Other contraventions of the Act or Rules	INR 50 crore

In determining the amount, Section 33(2) requires the Board to consider the nature, gravity and duration of the breach, the type and nature of the personal data affected, any repetition, any gain or loss avoided, the action taken to mitigate the effects and consequences, the proportionality and effectiveness of the penalty in achieving compliance and deterring breaches, and its likely impact on the person. The amounts in the Schedule are statutory ceilings, and the appropriate penalty depends on the circumstances established in the inquiry.

51. Does the Act provide compensation to affected individuals?

The Act does not create a statutory award of compensation to a Data Principal through proceedings before the Board. Section 34 requires sums realised as penalties under the Act to be credited to the Consolidated Fund of India.

A monetary penalty imposed by the Board is distinct from compensation for an individual's loss. Any claim for damages or other relief under a separate law must be assessed under that law, including its requirements, remedies and rules governing jurisdiction.

52. Can repeated contraventions result in blocking directions?

Section 37 empowers the Central Government or an authorised officer to direct blocking of public access to information generated, transmitted, received, stored or hosted in a computer resource that enables a Data Fiduciary to offer goods or services to Data Principals in India. The power arises on a reference from the Board that a monetary penalty has been imposed on that Data Fiduciary on two or more occasions and that blocking is advised in the interests of the general public.

Before issuing the direction, the Data Fiduciary must be given an opportunity of being heard, and the Government must record its reasons in writing. Repeated penalties do not automatically produce blocking, and the statutory reference, public-interest assessment and hearing requirements must also be satisfied.

53. Can the Government require information from organisations?

Section 36 empowers the Central Government to require the Board, a Data Fiduciary or an intermediary to furnish information for the purposes of the Act. Rule 23 and the Seventh Schedule specify the purposes and the authorised officers through whom information may be required, including matters relating to sovereignty and integrity or State security, performance of functions and fulfilment of disclosure obligations under law, and assessment for designation of Significant Data Fiduciaries.

Where disclosure of the fact that information has been furnished is likely to prejudicially affect India's sovereignty and integrity or State security, Rule 23 restricts disclosure of that fact without the prior written permission of the authorised officer. The information power and the associated restriction must be applied within their statutory purpose and conditions.

54. How does the DPDP framework interact with the IT Act and other laws?

Section 38 provides that the Act operates in addition to other laws and prevails to the extent of a conflict between its provisions and those of another law. Section 16(2) expressly preserves other Indian laws that impose a higher degree of protection or restriction on transfers of personal data outside India, so compliance with the DPDP framework does not displace applicable sector-specific transfer restrictions.

Section 44(2) amends the Information Technology Act, 2000 by omitting Section 43A and making the related change to Section 81. This amendment falls within the 18-month commencement phase scheduled for 13 May 2027. Until the applicable amendment commences, the existing Section 43A framework must be considered, and it is incorrect to treat that provision and its associated regime as already displaced solely because the DPDP Act has been enacted or the Rules notified.

Section 44(3), which amends the personal-information exemption in Section 8(1)(j) of the Right to Information Act, 2005, falls within the initial commencement phase of 13 November 2025. The different dates illustrate why the legal effect of each amendment must be determined from the commencement notification.

55. What organisational measures are required to give effect to the Act and Rules?

Section 8(4) requires a Data Fiduciary to implement appropriate technical and organisational measures to ensure effective observance of the Act and Rules. These measures must enable the organisation to apply the lawful ground for each processing purpose, provide the prescribed notices, obtain and demonstrate valid consent where required, give effect to withdrawal and Data Principal rights, and comply with retention and erasure obligations.

The measures must also support contractual control over processing undertaken on the organisation's behalf, the security safeguards under Rule 6, breach notification under Rule 7 and effective grievance redressal. Processing involving children or persons with disabilities who have lawful guardians requires the applicable verification arrangements, and designation as a Significant Data Fiduciary triggers the additional governance, assessment, audit and other requirements under Section 10 and Rule 13. The commencement provisions determine when each duty becomes legally operative.

PRIVACY AND DATA PROTECTION OFFERINGS BY LEXORBIS

LexOrbis assists organisations in assessing their data protection obligations and developing policies, contractual arrangements and governance procedures suited to their operations. Our services cover regulatory advice, compliance assessments, privacy management and ongoing support.

Service Area	Our Offerings
Data Protection Regulations	Advice on applicable privacy and data protection laws, including the Digital Personal Data Protection Act, 2023 and the Rules framed under it, and their implications for business operations.
Data Mapping	Assisting organisations in identifying the personal data they handle and documenting its collection, use, storage, sharing and retention across business functions.
Due Diligence and Gap Analysis	Reviewing data protection practices, contracts and documentation to identify compliance gaps and recommend corrective measures, including in commercial transactions.
Data Protection Policies and Procedures	Drafting and reviewing privacy notices, consent documentation, internal policies and procedures for retention, erasure, individual rights requests and breach response.
Data Protection Officer Support	Providing Data Protection Officer services and advisory support for internal oversight, grievance handling and coordination of compliance activities, subject to applicable statutory requirements.
Data Processing and Transfer Agreements	Drafting and negotiating agreements governing data processing and transfers, including responsibilities, confidentiality, security safeguards and cross-border arrangements.
Data Protection Impact Assessments (DPIA)	Assisting with assessments of proposed or existing processing activities to identify data protection risks and determine appropriate measures to address them.
Privacy Impact Assessments (PIA)	Assessing the privacy implications of products, services, technologies and business processes, and recommending safeguards for their design and implementation.
Review of Data Protection Frameworks	Evaluating existing governance structures, policies and controls for alignment with applicable legal requirements and organisational practices.
Vendor and Service Provider Assessments	Reviewing third-party data-handling arrangements, contractual commitments and compliance documentation to identify risks and required safeguards.
Development of Privacy Management Program	Assisting in developing a coordinated privacy programs that define responsibilities, establish internal procedures and provide mechanisms for monitoring and review.
Audits and Compliance Management	Conducting legal compliance reviews, assisting with remediation plans and supporting periodic assessment of data protection policies and practices.
Tailored Training Programmes	Providing training for management, employees and relevant business teams on data protection obligations and their application to everyday operations.



709/ 710, Tolstoy House, 15-17, Tolstoy Marg, New Delhi – 110 001
T: +91 11 2371 6565 | F: +91 11 2371 6556

NEW DELHI . MUMBAI . BENGALURU . CHENNAI . AHMEDABAD . PUNE
✉ mail@lexorbis.com | 🌐 www.lexorbis.com