THOMSON REUTERS
PRACTICAL LAW™

Data Protection in India: Overview

by Supratim Chakraborty, Sumantra Bose, and Shramana Dwibedi, Khaitan & Co LLP, with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 25 May 2023** | Jurisdiction: **India**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-013-9999**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Q&A guide to data protection in India.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in India, including the main obligations and processing requirements for data controllers, data processors, and other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Data Protection Law

The Digital Personal Data Protection Act 2023 (DPDPA) is India's first comprehensive data protection legislation and will regulate the collection, use, and disclosure of personal data. The DPDPA was published in the Official Gazette on August 11, 2023 and will come into force as notified by the Indian Government in the Official Gazette.

Other Relevant Laws

Until the DPDPA comes into force, the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) will govern privacy and data protection in India. Certain rules such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) implement the IT Act and prescribe general information security requirements. The IT Amendment Act aims to address issues that the original IT Act failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

However, the IT Act's primary focus is information security, rather than data protection, and while it does regulate certain aspects of personal data use on IT networks within India (for more on the IT Act's scope, see Question 2, Question 3, and Question 4), it does not provide comprehensive rules or regulations on personal data processing or transfers (for more on the rules governing transfers, see Question 20).

Indian general laws such as the Indian Penal Code, 1860 (IPC) also regulate some aspects of cybercrime. For example, Section 403 of the IPC imposes penal consequences for dishonest misappropriation or conversion of movable property. While the definition of movable property does not expressly include data, data theft may be tried under this provision.

Some sectoral regulators such as the Reserve Bank of India also regulate data protection through sector-specific regulations. These laws affect organizations operating in:

- **The banking and financial services sector.** For example:
  - the Aadhaar (Targeted Delivery of Financial and Other Subsidiaries, Benefits, and Services) Act 2016 as amended by the Aadhaar and Other Laws (Amendment) Bill, 2019 permits financial institutions to use biometric information to verify individuals' identities when opening bank accounts; and

  - the Credit Information Companies (Regulation) Act, 2005 and other Indian banking laws require customer confidentiality and protection of customer data.

- **The insurance industry.** The Insurance Regulatory and Development Authority of India issues regulations and rules that require insurance companies to protect confidential information they receive from misuse. For more on some of these regulations, see Country Q&A, Data Localization Laws: India.
- **The telecommunications and online service provider sector.** These organizations must comply with the IT Amendment Act, as implemented by the Information Technology (Intermediaries guidelines) Rules 2011 (Intermediaries Rules), which were superseded by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (in English) (IT Rules 2021), which were issued on February 25, 2021 ((as further amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2022 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023). Telecommunications providers must also comply with the Indian Telegraph Act. For more on the Intermediaries Rules, see Practice Note, Information Security Considerations (India): Telecommunications and Online Service Providers and Country Q&A, Email Marketing Compliance: India.

The responses provided in this Q&A focus primarily on the DPDPA, the IT Act (as amended by the IT Amendment Act) and the Privacy Rules.

Scope of Legislation

2. To whom do the laws apply?

The Digital Personal Data Protection Act 2023 (DPDPA) will protect the personal data of data principals, who are individuals to whom the personal data relates (including the parent or guardian of a child and the guardian of a person with a disability). It applies to personal data that the following parties process:

- Data fiduciaries, which means any person who alone or in conjunction with others determines the purposes and means of processing personal data.
- Data processors, which means any person who processes personal data on behalf of a data fiduciary.

(Section 2(i) to (k), DPDPA.)

The DPDPA permits the Indian government to classify certain data fiduciaries as significant data fiduciaries, considering factors including:

- The volume and sensitivity of personal data they process.
- Risk to data principals' rights.
- Potential impact on India's sovereignty and integrity India.
- Risk to electoral democracy.
- Security of the state.
- Public order.

(Section 10, DPDPA.)

The DPDPA imposes additional obligations on significant data fiduciaries (see Question 8).

The DPDPA also applies to consent managers, defined as persons registered with the Data Protection Board of India that acts as a single point of contact to enable a data principal to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform (Section 2(g), DPDPA).

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) do not use the terms data controllers, data processors, or data subjects. They apply to individuals and organizations in and outside of India that process personal information either:

- In India.
- Outside of India if they use a computer, computer system, or computer network located in India.

(Sections 1(2) and 75, IT Act.)

Some sections of the IT Act and IT Amendment Act, including the requirement to implement reasonable security practices and procedures (see Question 8), apply only to companies, known as body corporates under Indian law, meaning corporations, proprietorships, or other associations engaged in professional or commercial activities (Section 43A, IT Act, as amended by Section 22, IT Amendment Act). Practitioners understand this definition to exclude organizations that are not classified as engaging in professional or commercial activities.

The implementation of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

(Privacy Rules) will apply only to body corporates and individuals acting on a body corporate's behalf.

Certain sections of the IT Act addressing damages and punishment for unlawful data disclosure refer only to natural persons rather than organizations (for example, Section 72, IT Act).

The IT Act also prescribes special requirements for intermediaries, specifically organizations that provide connectivity, online marketplaces, and other supporting services in the internet environment that involve an organization receiving, storing, or transmitting an electronic record on another person's behalf (Section 2(1)(w), IT Act, as amended by Section 4, IT Amendment Act). For more on these requirements and their implementing rules, see Practice Note, Information Security Considerations (India): Telecommunications and Online Service Providers.

Other sectoral laws apply to participants in the relevant sector (see Other Relevant Laws).

3. What personal data does the law regulate?

The Digital Personal Data Protection Act 2023 (DPDPA) will regulate personal data, which means any data about an individual who is identifiable by or in relation to that data (Section 2(t), DPDPA). The DPDPA will not apply to personal data:

- An individual processes for personal or domestic purposes.
- Made publicly available by the data principal or a person with a legal obligation to make it publicly available (Section 3(c), DPDPA).

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) is not a comprehensive data protection law governing all aspects of personal data processing. Instead, it sets limits on processing and using both:

- **Personal information.** The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) define personal information as any information that relates to a natural person which, either directly or indirectly, in combination with other available or likely available information, may identify that person (Rule 2(i), Privacy Rules)).
- **Sensitive personal data or information (SPDI) processing.** The Privacy Rules define SPDI to mean personal information relating to a person's:
  - passwords;
  - financial information, including information relating to bank accounts, credit cards, debit cards, and other payment instrument details;
  - physical, physiological, and mental health condition;
  - sexual orientation;
  - medical records and history; and
  - biometric information.

  SPDI also includes any details relating to the above if the person provides the data to a body corporate for service or under a lawful contract for processing or storage. (Rule 3, Privacy Rules.) Information that is freely available, accessible in the public domain, or available under the Right to Information Act 2005, is excluded from the definition of sensitive personal data. For more on SPDI, see Question 11.

Certain sectoral laws such as those governing the financial, telecommunications, and insurance sectors regulate personal data that pertains to that sector (see Sectoral Laws).

4. What acts are regulated?

The Digital Personal Data Protection Act 2023 (DPDPA) will regulate personal data processing, which means a wholly or partly automated operation or set of operations performed on digital personal data, including its:

- Collection or recording.
- Organization, structuring, indexing, or storage.
- Retrieval or use.
- Adaptation, alignment, or combination.
- Sharing or disclosure by transmission, dissemination, or otherwise making available.
- Restriction, erasure, or destruction.

(Section 2(x), DPDPA.)

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) regulate:

- Collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, and disclosing sensitive personal data or information (SPDI) (Sections 5 to 7, Privacy Rules).
- Security practices and procedures for handling SPDI (Section 8, Privacy Rules).

- Data subjects' rights to review and update SPDI and withdraw consent for SPDI processing (Sections 5(6) and 5(7), Privacy Rules).

Some practitioners interpret the Privacy Rules to apply to all personal information with additional requirements for collection and processing that involves SPDI. Under this interpretation, requirements that apply to only SPDI include:

- Obtaining the data subject's prior written consent for collection, disclosure, and transfer of SPDI.
- Ensuring the collection is necessary for or directly related to a lawful purpose.
- Disclosing SPDI to third parties only under limited circumstances.
- Retaining SPDI for only as long as necessary to fulfil the organization's purpose for collecting it.

The IT Act regulates personal information disclosures that:

- Breach a lawful contract.
- Are made without the data subject's consent.

(Section 72A, IT Act, as amended by Section 37, IT Amendment Act.)

Sectoral laws may provide additional regulations applicable to participants in the relevant sector. For more on these sectoral laws, see Sectoral Laws.

5. What is the jurisdictional scope of the rules?

The Digital Personal Data Protection Act 2023 (DPDPA) will apply to processing:

- Personal data within India collected:
  - in digital form; or
  - in non-digital form and digitized subsequently.
- Digital personal data outside India in connection with any activity related to offering goods or services to data principals in India.

(Section 3, DPDPA.)

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) applies to entities in or outside of India that process personal data either:

- In India.
- Using a computer, computer system, or computer network located in India.

The IT Act applies to offenses or contraventions committed outside India if the computer, computer system, or computer network involved in the offense or contravention is located in India. (Sections 1(2) and 75, IT Act.)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (in English) (IT Rules 2021) (as further amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2022 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023) require significant social media intermediaries and online gaming intermediaries to:

- Appoint resident Indian employees to the following roles:
  - a Chief Compliance Officer;
  - a Nodal Contact Person; and
  - a Grievance Officer.
- Publish a physical contact address located in India on its website, mobile app, or both, to receive communications.

(Rules 4(1) and 4(5), IT Rules 2021.)

6. What are the main exemptions (if any)?

The Digital Personal Data Protection Act 2023 (DPDPA) will not apply to personal data:

- An individual processes for personal or domestic purposes.
- Made publicly available by the data principal or a person under a legal obligation to make it publicly available.

(Section 3(c), DPDPA.)

The DPDPA will also not apply to personal data processing:

- By government entities that the Indian government may specify, in the interests of sovereignty, integrity, and security of India, friendly relations with foreign states, maintenance of public order, or preventing related offenses.
- By the Indian government of any personal data that specified government entities provide.
- Necessary for research, archiving, or statistical purposes if the personal data is not used to make any decision specific to a data principal and the processing complies with prescribed standards.

(Section 17(2), DPDPA.)

In addition, DPDPA Chapter II (Obligations of Data Fiduciary) (except for Section 8(1) and (5)), Chapter III

(Rights and Duties of Data Principal), and Section 16 (cross-border data transfer restrictions)) will not apply when processing personal data:

- Is necessary for enforcing any legal right or claim.
- Is carried out by any court, tribunal or other body in India acting in any judicial, quasi-judicial, regulatory, or supervisory function, when the processing is necessary to perform that function.
- For the prevention, detection, investigation, or prosecution of any offense or contravention of any law in force in India.
- Of data principals outside India pursuant to any contract that a person inside India enters into with a person outside India.
- Necessary for a scheme of compromise, arrangement, merger, or amalgamation of two or more companies, a company's reconstruction by demerger or otherwise, transfer of one or more companies to another company, or division of one or more companies, approved by a court, tribunal, or other competent authority.
- To ascertain the financial information, assets, and liabilities of a person who has defaulted on a loan or advance taken from a financial institution, subject to the processing complying with other laws' provisions on disclosure of information or data.

(Section 17(1), DPDPA.)

The DPDPA will also permit the Indian government to, after considering the volume and nature of personal data processed, notify certain data fiduciaries or classes of data fiduciaries, including startups, that certain sections of the DPDPA will not apply, including:

- Section 5 (Notice).
- Section 8(3) (obligation to ensure completeness, accuracy, and consistency of personal data).
- Section 8(7) (obligation to erase personal data).
- Section 10 (Additional obligations of Significant Data Fiduciary).
- Section 11 (Right to access information about personal data).

(Section 17(3), DPDPA.)

The DPDPA will also exempt the Indian government and government entities from complying with Section 8(7) and Section 12(3) (both on the erasure of personal data). When the processing is for a purpose that does not include making a decision that affects the data principal, DPDPA Section 12(2) (correction, completion, and updating personal data) will not apply. (Section 17(4), DPDPA.)

The DPDPA will permit the Indian government to, before 5 years from the DPDPA's commencement, declare by notification that any DPDPA provision will not apply to certain data fiduciaries or classes of data fiduciaries for a specified period of time (Section 17(5), DPDPA).

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) exempt any information that is:

- Freely available or accessible in the public domain.
- Furnished under the Right to Information Act 2005 or any other enforceable law.

The Indian government has clarified that the Privacy Rules apply only to the body corporates that collect information from natural persons. Organizations that provide services relating to collecting, storing, or handling SPDI pursuant to a contractual relationship, such as outsourcing organizations, are exempt from complying with the personal data collection and disclosure obligations set out under Privacy Rules 5 and 6 (Clarification on Privacy Rules, Press Note dated August 24, 2011).

Notification

7. Is notification or registration with a supervisory authority required before processing data?

For information on the supervisory authority's notification, registration, or authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: India: Questions 2 and 3.

For information on individual notification requirements, see Question 12.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The Digital Personal Data Protection Act 2023 (DPDPA) will impose certain obligations on data fiduciaries, including:

- **Legal basis.** Data fiduciaries may only process a data principal's personal data pursuant to a legal basis, including:
  - obtaining data principal consent for the processing (see Question 9); or
  - certain legitimate uses (see Question 10).

  (Section 4, DPDPA.)
- **Accountability.** Data fiduciaries must remain responsible for the personal data processing that they conduct and have data processors conduct on their behalf. Data fiduciaries must have a valid contract in place to engage data processors. (Section 8(1), (2), DPDPA.)
- **Accuracy.** Data fiduciaries must ensure that personal data they process is accurate, complete, and consistent when it is likely to be:
  - used to make a decision that affects the data principal; or
  - disclosed to another data fiduciary.

  (Section 8(3), DPDPA.)
- **Data principal rights.** Data fiduciaries must facilitate the exercise of data principals' rights (Sections 11 to 14, DPDPA; see Question 12 and Question 13).
- **Technical and organizational measures.** Data fiduciaries must implement appropriate technical and organizational measures to ensure compliance with the DPDPA and rules to be issued thereunder. (Section 8(4), DPDPA).
- **Reasonable security safeguards.** Data fiduciaries must implement reasonable security safeguards to protect personal data from any breach, including when data processors process personal data on their behalf (Section 8(5), DPDPA).
- **Personal data breach notification.** In the event of a personal data breach, data fiduciaries must notify the Data Protection Board of India and each affected individual of the breach, in the form and manner as the DPDPA may prescribe and consistent with the rules issued thereunder (Section 8(6), DPDPA).
- **Storage limitation.** Data fiduciaries may only retain personal data for as long as necessary to comply with any law. Data fiduciaries must erase the relevant personal data and ensure its data processors erase it on the earlier of:
  - the data principal withdrawing their consent for the processing; or
  - the processing no longer serving the specified processing purpose.

  (Section 8(7), DPDPA.)
- **Data protection officer (DPO).** Data fiduciaries must publish, in a manner the DPDPA will prescribe, the business contact information of the Data Protection Officer (for significant data fiduciaries) or person capable of answering a data principal's questions about the processing of their personal data (Section 8(9), DPDPA).
- **Grievance redressal.** Data fiduciaries must establish an effective mechanism to redress data principals' grievances (Section 8(10), DPDPA).
- **Additional obligations for significant data fiduciaries.** The DPDPA imposes additional obligations on significant data fiduciaries, including:
  - appointing a DPO based in India that reports to the company board of directors and serves as a contact for the grievance redressal mechanism;
  - appointing an independent data auditor to conduct data audits; and
  - undertaking other measures like conducting periodic data protection impact assessments, audits, and other measures to be prescribed.

  (Section 10, DPDPA.)

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) impose the following main obligations to ensure data is processed properly:

- **Reasonable security practices and procedures.** A body corporate must implement:
  - reasonable security practices, procedures, and standards to handle sensitive personal data or information (SPDI);
  - a comprehensive documented information security program; and
  - policies that contain managerial, technical, operational, and physical security control measures that are proportionate to the information assets it seeks to protect.

  (Rule 8, Privacy Rules; Section 43A, IT Act, as amended by IT Amendment Act.) For more on personal data security, see Question 15.

- **Purpose limitation.** Body corporates should collect SPDI only if it is essential and required for a lawful purpose connected with the body corporate's functions (Rule 5(2), Privacy Rules). The body corporate should use the information only for the purpose for which it was collected and should not retain it for a period longer than required (Rules 5(4) and 5(5), Privacy Rules).
- **Consent and notification.** Under the Privacy Rules, body corporates collecting SPDI from a data subject must obtain the subject's prior written consent (Rule 5(1), Privacy Rules). When collecting information from the data subject, the body corporate must also take reasonable steps to inform the data subject:
  - that the body corporate is collecting the information;
  - the collection's purpose;
  - the intended recipients; and
  - the name and address of the body corporate, or an entity or person acting on its behalf, that is collecting and retaining the information.

  (Rule 5(3), Privacy Rules.) The body corporate must allow the data subject the right to review or amend the SPDI and provide an option to retract consent at any point of time. If consent is withdrawn, the body corporate may stop providing the goods or services for which the information was sought. (Rules 5(6) and 5(7), Privacy Rules.) For more on consent, see Question 9. For more on providing information to data subjects, see Question 12.
- **SPDI transfers.** A body corporate can transfer SPDI to a third party, whether in India or overseas, only if:
  - the receiving party ensures the same level of protection as that provided under the Privacy Rules; and
  - either the transfer is necessary to perform a lawful contract with the data subject or the data subject has consented to the transfer.

  (Rule 7, Privacy Rules.) For more on personal data transfers, see Question 17 and Question 20.
- **SPDI disclosures.** A body corporate may disclose SPDI to a third party only if:
  - a government agency seeks the information to verify identity, or to prevent, detect, or investigate a crime, including cyber incidents, or to prosecute and punish offenses, the agency request clearly states the purpose in writing, and the receiving party does not further disclose the SPDI;
  - it is necessary to comply with a legal obligation; or
  - the data subject agrees to the disclosure in a contract.

  (Rule 6, Privacy Rules.)
- **Privacy policy.** A body corporate must provide a comprehensive privacy policy to data subjects while handling SPDI. The privacy policy must include:
  - a clear and easily accessible statement on its practices and policies;
  - the type of information collected;
  - the purpose of collection and use;
  - the disclosure policy for the information; and
  - the security practices and procedures the body corporate followed.

  The body corporate must publish the privacy policy prominently on its website and make it readily available to data subjects. (Rule 4, Privacy Rules.)
- **Grievance officer.** A body corporate must designate a grievance officer and publish their name and contact details on their website. The grievance officer must address data subject grievances within one month of receiving the complaint. (Rule 5(9), Privacy Rules.) For information on the notification, registration, or authorization requirements for grievance officers, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: India: Questions 4 and 5.

9. Is the consent of data subjects required before processing personal data?

Consent is one of the two legal bases for personal data processing that the Digital Personal Data Protection Act 2023 (DPDPA) will permit. The DPDPA will require consent to be:

- Free.
- Specific.
- Informed.
- Unconditional and unambiguous.
- Restricted to the personal data necessary for a specified purpose.
- Indicated with a clear affirmative action, signifying the data principal's agreement to the processing of their personal data for a specified purpose.

(Section 6(1), DPDPA.)

The DPDPA will require every request for consent to:

- Be presented to the data principal in clear and plain language.

- Give the data principal the option to access the request in English or any language the Eighth Schedule to the Constitution specifies.
- Provide the contact details of the DPO (in case of a significant data fiduciary) or of another person the data fiduciary authorizes to respond to communications from data principals related to the exercise of their rights.

(Section 6(3), DPDPA.)

The DPDPA will give data principals the right to withdraw their consent at any time in a manner comparable to how they provided consent when consent is the legal basis for the processing (Section 6(4), DPDPA). If a data principal withdraws consent, the data fiduciary must stop processing their personal data within a reasonable time and require their data processors to stop processing that personal data, unless processing without consent is required or authorized under the DPDPA, its rules, or any other Indian law (Section 6(6), DPDPA).

A body corporate must have a data subject's prior written consent before collecting or disclosing sensitive personal data or information (SPDI) (Rules 5(1) and 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules)). The consent may be obtained through a letter, fax, email, or any other mode of electronic communication and must indicate how the organization will use the SPDI (Rule 5(1), Privacy Rules).

Given these methods of obtaining consent, practitioners believe that consent must be explicitly and expressly conveyed and may not be implied.

There are no specific provisions relating to obtaining consent from minors.

The body corporate must allow the data subject the option to retract consent at any point of time. If consent is withdrawn, the body corporate may stop providing the goods or services for which the information was sought. (Rules 5(6) and 5(7), Privacy Rules.)

Personal information secured under a lawful contract may not be disclosed without the affected person's consent or in contravention of the contract's provisions (Section 72A, Information Technology Act 2000, as amended by Section 37, the Information Technology (Amendment) Act 2008).

For more on:

- Other legal basis for processing, see Question 10.
- Processing sensitive personal data, see Question 11.

10. If consent is not given, on what other grounds (if any) can processing be justified?

Other than consent, the Digital Personal Data Protection Act 2023 (DPDPA) will permit data fiduciaries to process personal data based on certain legitimate uses, including:

- For the specified purpose for which data principals have voluntarily provided their personal data to the data fiduciary, when they have not indicated that they do not consent to the data fiduciary's use of their personal data.
- For the Government and its instrumentalities to provide or issue to data principals a subsidy, benefit, service, certificate, license, or permit as may be prescribed, based on certain conditions.
- For the Government or any of its instrumentalities to perform any function under any Indian law or in the interest of sovereignty, integrity, or security of India.
- To fulfil any legal obligation to disclose information to the Government or its instrumentalities, consistent with Indian law.
- To comply with any judgment, decree, or order issued under any Indian law or any judgment or order relating to civil or contractual claims under any law outside India.
- To respond to a medical emergency involving a threat to the data principal's or other individual's life or health.
- To provide medical treatment or health services to any individual during an epidemic, disease outbreak, or other public health threat.
- To ensure the safety of or provide assistance or services to any individual during a disaster or breakdown of public order.
- For employment purposes or safeguarding the employer from loss or liability, such as preventing corporate espionage, maintaining confidentiality of trade secrets, intellectual property, and classified information, or providing any service or benefit to data principals who are employees.

(Section 7, DPDPA.)

There are no exceptions under the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) to collect or process sensitive personal data or information without the data subject's consent.

Without the data subject's consent, a body corporate may disclose SPDI if:

- The disclosure is necessary to comply with a legal obligation.
- Applicable law requires the disclosure.
- The disclosure is to a government agency to either:
  - verify an individual's identity; or
  - prevent, detect, investigate (including cyber incidents), prosecute, or punish offenses.

  The body corporate may share this information with government agencies only after receiving a written request that clearly mentions the purpose of seeking the information. Further, the government agency must state that the SPDI shall not be published or shared with any other person.

(Rules 6(1) and 6(2), Privacy Rules.)

For more on body corporates' other key obligations, see Question 8. For more on consent as a legal basis to process, see Question 9.

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The Digital Personal Data Protection Act 2023 (DPDPA) does not distinguish between personal data categories or provide special obligations for specific categories of personal data. The DPDPA will impose additional restrictions on processing the personal data of children under 18 years of age or disabled persons, including:

- Obtaining the consent of the child or disabled person's parent or lawful guardian in a manner to be prescribed.
- Not conducting processing likely to cause any detrimental effect on a child's well-being.
- Not tracking or monitoring children or directing targeted advertising at children.

(Section 9(1) to (3), DPDPA.)

The obligations in the first and third bullets above will not apply to certain prescribed classes of data fiduciaries (Section 9(4), DPDPA). The Indian government may exempt certain data fiduciaries for complying with these obligations if it ensures that they process personal data in a verifiably safe manner (Section 9(5), DPDPA).

Section 43A of the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) apply to sensitive personal data or information (SPDI). The Privacy Rules define SPDI to mean personal information which consists of information relating to a person's:

- Passwords.
- Financial information, including information relating to bank accounts, credit cards, debit cards, and other payment card information.
- Physical, physiological, or mental health.
- Sexual orientation.
- Medical records and history.
- Biometric information.

SPDI also includes any details relating to the above categories even if the person provides the data to a body corporate to provide a service or for processing under a lawful contract. (Rule 3, Privacy Rules.)

As noted in Question 8, a body corporate handling SPDI must:

- **Implement reasonable security practices and procedures.** A body corporate must implement:
  - reasonable security practices, procedures, and standards to handle sensitive personal data or information (SPDI);
  - a comprehensive documented information security program; and
  - policies that contain managerial, technical, operational, and physical security control measures that are proportionate to the information assets it seeks to protect.

  (Rule 8, Privacy Rules; Section 43A, IT Act, as amended by Section 22, IT Amendment Act.) For more on personal data security, see Question 15.
- **Collect and use SPDI for lawful purposes.** A body corporate should collect SPDI only if it is essential and required for a lawful purpose connected with the organization's functions (Rule 5(2), Privacy Rules). The body corporate should use the information only for the purpose for which it was collected and should not retain the information for a period longer than what is required (Rule 5(4), Privacy Rules).

- **Obtain consent from and provide notification to data subjects.** Under the Privacy Rules, a body corporate collecting SPDI from a data subject must obtain the subject's prior written consent (Rule 5(1), Privacy Rules). When collecting information from the data subject, the body corporate must also take reasonable steps to inform the data subject:
  - that the body corporate is collecting the information;
  - the collection's purpose;
  - the intended recipients; and
  - the name and address of the organizations collecting and retaining the information.

  (Rule 5(3), Privacy Rules.) The body corporate must allow the data subject the right to review or amend the SPDI and provide an option to retract consent at any point of time. If consent is withdrawn, the body corporate may stop providing the goods or services for which the information was sought. (Rules 5(6) and 5(7), Privacy Rules.) For more on consent, see Question 9. For more on providing information to data subjects, see Question 12.
- **Follow specific rules when transferring SPDI.** A body corporate can transfer SPDI to a third party, whether in India or overseas, only if:
  - the receiving party ensures the same level of protection as that provided under the Privacy Rules; and
  - either the transfer is necessary to perform a lawful contract with the data subject and the data subject has consented to the transfer.

  (Rule 7, Privacy Rules.) For more on personal data transfers, see Question 17 and Question 20.
- **Follow specific rules when disclosing SPDI to a third party.** A body corporate may disclose SPDI to a third party only if:
  - governmental agencies seek the information or it is necessary to comply with a legal obligation; or
  - the data subject has agreed to the disclosure in a contract.

  (Rule 6, Privacy Rules.)
- **Develop a privacy policy.** A body corporate must provide a comprehensive privacy policy to data subjects while handling SPDI. The privacy policy must include:
  - a clear and easily accessible statement on its practices and policies;
  - the type of information collected;
  - the collection's purpose;
  - the disclosure policy for the information; and
  - the security practices and procedures the body corporate followed.

  The body corporate must publish the privacy policy prominently on its website and make it readily available to data subjects. (Rule 4, Privacy Rules.)
- **Appoint a grievance officer.** A body corporate must designate a grievance officer and publish their name and contact details on their website. A body corporate must address data subject grievances within one month of receiving the complaint. (Rule 5(9), Privacy Rules.) For information on the notification, registration, or authorization requirements for grievance officers, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: India: Questions 4 and 5.

Rights of Individuals

12. What information rights do data subjects have?

The Digital Personal Data Protection Act 2023 (DPDPA) will require data fiduciaries to provide data principals with a notice at or before the time they request their consent for personal data processing that sets out:

- The personal data the data fiduciary will collect and the proposed processing purpose.
- How data principals may exercise their rights to withdraw consent for the processing and redress grievances.
- How data principals may make a complaint to the Data Protection Board of India.

(Section 5(1), DPDPA.)

Data fiduciaries must provide data subjects with the option to access the notice in English or any language specified in the Eighth Schedule to the Constitution (Section 5(3), DPDPA).

When a data principal has consented to the personal data processing before the DPDPA takes effect, data fiduciaries must provide them with a notice containing the information set out in Section 5(1). The data fiduciary may continue to process the personal data unless and until the data principal withdraws their consent. (Section 5(2), DPDPA.)

Under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), body corporates collecting SPDI must take reasonable steps to inform the data subject of:

- The information being collected.
- The body corporate's purpose for collecting the information.
- The intended recipients.
- The name and address of the body corporate:
  - collecting the SPDI; and
  - retaining the SPDI.

(Rule 5(3), Privacy Rules.) The body corporate should use the information only for the purpose for which it was collected and should not retain the information for a period longer than required (Rules 5(4) and 5(5), Privacy Rules).

The body corporate must allow the data subject the right to review or amend the SPDI and provide an option to retract consent at any point of time. If consent is withdrawn, the body corporate may stop providing the goods or services for which the information was sought. (Rules 5(6) and 5(7), Privacy Rules.)

The Privacy Rules also require a body corporate to make a comprehensive privacy policy available on its website to data subjects while handling SPDI. The privacy policy must clearly state:

- The body corporate's practices and policies.
- The type of SPDI collected.
- The body corporate's purpose in collecting and using the information.
- The disclosure policy for the information.
- The security practices and procedures the body corporate followed.

(Rule 4, Privacy Rules.)

Before collecting information, the body corporate must provide the data subject an option not to provide the data (Rule 5(7), Privacy Rules).

For more on other data subject rights, see Question 13.

13. Other than information rights, what other specific rights are granted to data subjects?

The Digital Personal Data Protection Act 2023 (DPDPA) will grant data principals certain rights regarding their personal data, including the right to:

- **Access.** When consent is the legal basis for processing, data principals may request and obtain certain information regarding their personal data from data fiduciaries, including:
  - a summary of personal data that the data fiduciary is processing about them;
  - the processing activities the data fiduciary carries out with respect to their personal data;
  - the identities of all other data fiduciaries and data processors with whom the data fiduciary has shared their personal data, along with a description of the shared personal data; and
  - any other information related to the data principal's personal data and its processing, as the DPDPA may prescribe.

  The information set out under bullets 3 and 4 above will not apply to personal data the data fiduciary has shared for the purpose of preventing, detecting, or investigating offenses or cyber incidents, or for prosecuting or punishing offenses. (Section 11, DPDPA.)
- **Correction and erasure.** When consent is the legal basis for processing, data principals may request and obtain from data fiduciaries:
  - correction of inaccurate or misleading personal data;
  - completion of incomplete personal data;
  - updates to their personal data; and
  - erasure of personal data no longer necessary for which it was processed, unless retention is necessary for the specified collection purpose or for compliance with any law.

  (Section 12, DPDPA.)
- **Grievance redressal.** Data fiduciaries and consent managers must make available an effective and robust grievance redressal mechanism for any grievances that relate to data principals' personal data (Section 13, DPDPA).
- **Nomination.** Data principals may nominate any other individual to exercise their rights on their behalf in the event of their death or incapacity (Section 14, DPDPA).
- **Withdrawal of consent.** When consent is the legal basis for processing, data principals may withdraw consent

for processing any personal data provided in a manner comparable to how they provided consent (Section 6(4), DPDPA).

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) provide the following rights to the data subject:

- The right to be informed about any recipients of the information (Rule 5(3), Privacy Rules).
- The right to access and review the information provided to the organization (Rules 5(6), Privacy Rules).
- The right to amend or update the information if it is inaccurate or incomplete (Rules 5(6), Privacy Rules).
- The right to withdraw consent at any time. A data subject must withdraw consent in writing. A body corporate may decline to provide the goods or services that it sought consent for if the data subject withdraws consent. (Rule 5(7), Privacy Rules.)

A body corporate must comply with a data subject's request to exercise these rights (Rule 5(6), Privacy Rules).

Existing Indian law does not recognize other common data subject rights, such as the right to object to processing, determine the information an organization holds on them, or the right to data portability. It also does not provide data subjects with a specific right to request that a body corporate delete SPDI.

Data subjects have the right to withdraw consent for collection of SPDI. A body corporate does not need to delete collected SPDI after the data subject has withdrawn consent and may opt not to provide the goods or services for which the information was sought. (Rule 5(7), Privacy Rules.)

For information on data subject information rights, see Question 12.

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries to implement any particular security standard. However, it will require data fiduciaries to implement reasonable security safeguards to protect personal data in their possession or control from any breach, including with respect to any processing that data processors conduct on their behalf (Section 8(5), DPDPA).

As noted above (see Question 8), a body corporate must implement:

- Reasonable security practices, procedures, and standards to handle sensitive personal data or information (SPDI).
- A comprehensive documented information security program.
- Policies that contain managerial, technical, operational, and physical security control measures that are proportionate to the information assets it seeks to protect.

(Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules); Section 43A, Information Technology Act 2000 (IT Act), as amended by Section 22, Information Technology (Amendment) Act 2008 (IT Amendment Act).)

The Central Government may prescribe the reasonable security practices (Section 43A(ii), IT Act, as amended by Section 22, IT Amendment Act).

To comply with this requirement, the Privacy Rules specify that a body corporate must:

- Implement either:
  - IS/ISO/IEC 27001 relating to Information Technology-Security Techniques-Information Security Management System–Requirements (Rule 8(2), Privacy Rules); or
  - other standards set by self-regulating industry associations or entities formed under these associations, if the organization notifies the Central Government, and the Central Government or an independent auditor certifies or approves the standard (Rule 8(3), Privacy Rules).
- Undergo an audit annually or and when the body corporate significantly upgraded any of its processes or computer resources (Rule 8(4), Privacy Rules).

For more on security requirements in India, see Practice Notes, Information Security Considerations (India) and Cyber Incident Response and Data Breach Notification (India).

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The Digital Personal Data Protection Act 2023 (DPDPA) will require data fiduciaries to report personal data breaches to the Data Protection Board of India and each affected individual in a manner to be prescribed (Section 8(6), DPDPA).

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) does not require notifications to the government or individuals about personal data breaches. However, the Indian Government requires organizations to notify authorities about cyber security incidents, including personal data breaches, through the rules governing its Computer Emergency Response Team (CERT-In), the agency established under Section 70B of the IT Act to deal with cyber security threats. (Section 70B, IT Act, as amended by Section 36, IT Amendment Act; Rule 12(10(a), Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules).)

CERT-In issued a direction in 2022 (Direction) under Section 70-B(6) of the Information Technology Act 2000 (IT Act), which applies to certain entities. Under the Direction, certain specified types of cyber incidents (such as targeted scanning/probing of critical networks/systems, compromise of critical systems/information, unauthorised access of IT systems/data etc) as more particularly identified under Annexure I of the Direction, are required to be mandatorily reported to CERT-In within 6 (six) hours of noticing such incidents or being brought to notice about such incidents.

CERT-In has developed a system of incident reporting where organizations can report a cybersecurity incident to CERT-In and receive technical assistance from CERT-In. Further, an incident reporting form issued by CERT-In specifies the indicative requirements for organization's cyber security incident reporting including basic information of affected system and whether the affected system/network is critical to the organization's mission.

The cyber-incidents specified in the Direction are incident specific and are not dependent on the nature of data that has been leaked or disclosed because of the incident.

For more on breach notification in India, see Practice Notes, Cyber Incident Response and Data Breach Notification (India) and Global Data Breach Notification Laws Chart: Overview

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The Digital Personal Data Protection Act 2023 (DPDPA) will not impose any specific compliance obligations or penalties on data processors. Instead, the DPDPA will give data fiduciaries responsibility for overall compliance, including for activities of the data processors they engage (Section 8(1), DPDPA). The DPDPA will require data fiduciaries to engage data processors under a valid contract (Section 8(2), DPDPA).

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) require body corporates transferring sensitive personal data or information (SPDI) to ensure that third-party processors receiving the data provide an appropriate level of data protection, including the security requirements discussed in Question 15. A body corporate may transfer SPDI within or outside of India if the person receiving the SPDI ensures the same level of data protection as provided under Indian law and either:

- The transfer is necessary to perform a contract with the data subject.
- The data subject has consented to the transfer.

(Rule 7, Privacy Rules.)

Third-party processors are also prohibited from further disclosing, sharing, or transferring the SPDI to any other entity or person (Rule 6(4), Privacy Rules).

The Indian Government has indicated that an entity that provides services relating to collection, storage, dealing, or handling of SPDI through a contract with a covered body corporate located within or outside India, including third-party processors, are not subject to the Privacy Rules requirements on:

- Consent and notification under Rule 5.
- Data subject requests and grievances under Rule 5.
- Third-party disclosures under Rule 6.

(Clarification on Privacy Rules, Press Note (August 24, 2011).) For more on these obligations, see Question 8.

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act

and IT Amendment Act) and Privacy Rules do not impose liability or additional obligations separately for data processors.

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Digital Personal Data Protection Act 2023 (DPDPA) does not specifically regulate cookies or similar technologies, but to the extent that they collect personal data, data fiduciaries must comply with the DPDPA's requirements.

There is no specific regulation in India addressing cookie storage or installing equivalent devices on the data subject's terminal equipment. However, the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) provides that a person who downloads, copies, or extracts any data, computer database, or information from a computer, computer system, or computer network, without the permission of the owner or the person in charge of the computer, computer system, or computer network, is liable to pay damages to the affected person and criminal penalties (Section 43, IT Act). Some organizations in India use cookie policies, but it is not a common practice.

For more on consent requirements, see Question 9. For more on data subject notification requirements, see Question 12.

For more on marketing rules in India, see Country Q&A, Email Marketing Compliance: India.

19. What rules regulate sending commercial or direct marketing communications?

The Digital Personal Data Protection Act 2023 (DPDPA) will not specifically regulate sending commercial or direct marketing communications, but if a data fiduciary is relying on consent as a legal basis for sending these communications, the DPDPA's standard notice and consent requirements will apply in addition to its other provisions on personal data processing.

Several sectoral laws impose confidentiality requirements and restrict personal information use in ways that may impact email marketing activities, but the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) do not regulate this practice.

For example, the Telecom Commercial Communications Customer Preference Regulations 2018 (Commercial Communications Regulations) attempts to curb the problem of unsolicited commercial calls and messages. Under these regulations, telemarketers and senders sending unsolicited commercial communications in the form of text messages or telephone calls made using the network of licensed telecom service providers must:

- Not make any commercial communications unless registered with the Telecom Regulatory Authority of India (TRAI) (Regulation 3, Commercial Communications Regulations).
- Adhere to guidelines and codes of practice formulated by the telecom service providers (Explanatory Memorandum, Commercial Communications Regulations).
- Not send any commercial communications to any subscriber or customer without their consent, or against their registered preferences, as recorded in the consent register (Schedules I and VI, Commercial Communications Regulations).

For more on marketing rules in India, see Country Q&A, Email Marketing Compliance: India.

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The Digital Personal Data Protection Act 2023 (DPDPA) permits the Indian government to designate certain countries outside India to which it will restrict data fiduciaries' transfer of personal data for processing. However, any Indian law that provides for a higher degree of protection or restriction on transfer of personal data will take precedence over the DPDPA. (Section 16, DPDPA.)

The Indian government has not yet issued a list of countries to which it will restrict personal data transfers.

A person that discloses personal information in contravention of a lawful contract is subject to penalties (Section 72A,

Information Technology Act 2000, as amended by Section 37, Information Technology (Amendment) Act 2008). A personal data transfer in breach of a contract could attract penalties under this provision. Otherwise, Indian law does not provide rules governing personal information transfers.

For more on personal data transfers, see Question 22.

A body corporate may transfer sensitive personal data or information (SPDI) within or outside of India if the person receiving the SPDI ensures the same level of data protection as provided under Indian law and either:

- The transfer is necessary to perform a contract with the data subject.
- The data subject has consented to the transfer.

(Rules 7 and 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011; see Question 8 and Question 17.) If the data subject has consented to the SPDI transfer, an organization may transfer SPDI through a data processing agreement that incorporates these obligations under the Privacy Rules.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries to store any type of personal data inside India. However, it also states that any Indian law that provides for a higher degree of protection or restriction for personal data transfers will take precedence over the DPDPA, any sectoral data localization laws will take precedence (Section 16, DPDPA).

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) do not specifically require personal information to be stored within India.

However, certain sectoral laws require data localization. Specifically:

- The Reserve Bank of India's Directive 2017-18/153 (April 6, 2018) issued under the Payment and Settlement Systems Act 2007. Paragraph 2(i) of the Directive requires covered organizations to store payment data within India.
- The (Indian) Companies Act 2013 (ICA). Section 128 provides that if a company maintains its accounting books and other relevant books and papers (Financial Information) in electronic mode, it must store the Financial Information on in servers located within India. If the Financial Information is stored in servers physically located outside India, the back-up of the Financial Information must be maintained in servers physically located within India. Further, the company must provide certain information to the concerned registrar of companies on an annual basis relating to storage or handling of the Financial Information.
- The IRDAI (Maintenance of Insurance Records) Regulation, 2015. Paragraph 3(9) requires covered organizations to store data relating to all policies issued and all claims made in India in data centers located in India.

For more on data localization requirements, see Country Q&A, Data Localization Laws: India. For an "at-a-glance" Chart that shows certain statutory requirements to store data locally under data localization laws worldwide, see Practice Note: Overview, Data Localization Laws Global Chart: Overview. For more general and country-specific resources to help organizations identify key data localization laws and the data categories the data localization laws cover, see Global Data Localization Laws Toolkit.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries to enter into data transfer agreement when transferring personal data outside India. However, the DPDPA will require that data fiduciaries engage data processors under a valid contract (Section 8(1), DPDPA). The Data Protection Board of India has not yet approved any standard forms or precedents for these contracts.

Other Indian laws do not specifically prescribe data transfer agreements so there are no forms or precedents approved by any national authority. For more on the rules governing transfers, see Question 20.

However, the Indian government has clarified that the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) apply only to the body corporates that collect information from natural persons. Entities that provide services relating to collection, storage, or handling SPDI under a contract with a covered body corporate within

or outside of India, such as outsourcing organizations, are exempt from complying with the personal data collection and disclosure obligations set out under Privacy Rules 5 and 6 (Clarification on Privacy Rules, Press Note dated August 24, 2011).

For general and country-specific resources to help organizations comply with data protection laws when transferring personal data across borders, see Cross-Border Personal Data Transfers Toolkit.

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See Question 20 and Question 22.

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries to enter into data transfer agreements when transferring personal data outside India or obtain Data Protection Board approval for data transfer agreements.

Other Indian laws do not regulate data transfer agreements (see Question 22).

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

The Digital Personal Data Protection Act 2023 (DPDPA) will establish the Data Protection Board of India as the supervisory authority with the power to:

- Direct any urgent remedial or mitigation measures for reported personal data breaches, investigate these breaches, and impose penalties under the DPDPA.
- Investigate data principals' complaints and impose penalties under the DPDPA regarding:
  - personal data breaches and data fiduciaries' breach of their obligations relating to personal data or data principals' rights; and
  - consent managers' breaches of their obligations regarding personal data or registration conditions.
- Investigate matters referred by the central government or a state government or pursuant to a court order and impose penalties under the DPDPA.
- Issue orders to persons with written reasons after they have an opportunity to be heard and modify, suspend, withdraw, or cancel those orders based on a representation made by a person affected by an order.

(Section 27, DPDPA.)

The Ministry of Electronics and Information Technology (MeitY) administers the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and promulgated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), and acts as an enforcement authority in certain cases.

Claims for compensation of less than INR50 million made under section 43A of the IT Act and IT Amendment Act are adjudicated by the adjudicating officer appointed by the Central Government. Claims above INR50 million are adjudicated by the competent courts. (Section 46, IT Act.)

Sectoral laws are enforced by the respective sectoral regulators.

For more on sanctions and remedies for noncompliance, see Question 26.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The Digital Personal Data Protection Act 2023 (DPDPA) will impose certain penalties for violations, including:

- Up to INR2,500,000,000 for failure of data fiduciaries to implement reasonable security safeguards to prevent personal data breaches under Section 8(5).
- Up to INR2,000,000,000 for failure to notify the Data Protection Board of India or affected data principals of a personal data breach under Section 8(6).
- Up to INR2,000,000,000 for breach of obligations related to children under Section 9.
- Up to INR1,500,000,000 for breach of significant data fiduciary obligations under Section 10.
- Up to INR500,000,000 for breach of any other DPDPA provision or rules to be issued thereunder.
- Up to INR10,000 for a data principal's breach of their duties under Section 15.
- Up to extent applicable for the relevant breach for violating any term of voluntary undertaking that the Board accepted under Section 32.

(Section 33(1) Schedule, DPDPA.)

Violations of the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) may trigger the following penalties:

- Damages to compensate an affected individual for a body corporate's negligence in implementing and maintaining "reasonable security practices and procedures" to secure SPDI or personal information (Section 43A, IT Act, as amended by Section 22, IT Amendment Act). Damages are uncapped and may vary from case to case.
- Imprisonment for not more than three years, a INR500,000 fine, or both, for disclosing personal information in breach of lawful contract or without the data subject's consent (Section 72A, IT Act, as amended by Section 37, IT Amendment Act).
- Imprisonment for not more than one year, an INR100,000 fine, or both for a body corporate's failure to provide information to the Computer Emergency Response Team (CERT-In), or comply with CERT-In's directions (Section 70B(7), IT Act, as amended by Section 36, IT Amendment Act).

Regulator Details

The Digital Personal Data Protection Act 2023 will establish the Data Protection Board of India as the data protection supervisory authority, but the law is not yet in effect. India does not currently have a national data protection regulator.

The Ministry of Electronics and Information Technology (MeitY) administers the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and promulgated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules). Sectoral regulators also issue data protection related regulations and standards.

Contributor Profile

Supratim Chakraborty, Partner

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E supratim.chakraborty@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2008

Areas of practice. Data protection; cybersecurity; IT contracts; mergers and acquisitions.

Sumantra Bose, Principal Associate

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E sumantra.bose@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2012

Areas of practice. Data protection; cybersecurity; IT contracts; mergers and acquisitions.

Shramana Dwibedi, Associate

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E shramana.dwibedi@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2020

Areas of practice. Data protection; cybersecurity; IT contracts.