iclg

Data Protection 2025

12th Edition

Contributing Editors:

Tim Hickman & Dr. Detlev Gabel

White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

India


Rachit Bahl


Rohan Bagai


Sumit Ghoshal


Archana Iyer

AZB & Partners

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), enacted on August 11, 2023, is India's principal data protection legislation. As of May 2025, while the DPDP Act has been enacted, its substantive provisions are yet to be notified and enforced. On January 3, 2025, the competent ministry under the Government of India, the Ministry of Electronics and Information Technology ("**MeitY**"), released the Draft Digital Personal Data Protection Rules, 2025 ("**Draft Rules**"), for public consultation. The DPDP Act and the Draft Rules are expected to be enforced in a phased manner, with sufficient sunrise period provided to organisations to transition to the new data protection regime.

Until the DPDP Act is enforced, the current data protection regime is contained under the provisions of the Information Technology Act, 2000 ("**IT Act**"). Section 43A of the IT Act holds a body corporate liable for negligence in implementing reasonable security practices while handling sensitive personal data; and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**"), notified under the IT Act, set out procedures for lawful collection, use, transfer and disclosure of sensitive personal data.

Once the DPDP Act is enforced, it will repeal the existing regime under the IT Act and the SPDI Rules entirely. Given the limited enforcement of the SPDI Rules and the reported expectation of the Government for organisations to move towards compliance with the DPDP Act, we have discussed the relevant provisions of the DPDP Act in this chapter.

1.2 Is there any other general legislation that impacts data protection?

Yes. Some of the other general legislation that may directly or indirectly impact data protection include the following: (a) the IT Act prescribes penalties and consequences for unauthorised access to data and disclosure of data in breach of a lawful contract; (b) the Information Technology (Indian Computer Emergency Response Team ("**CERT-In**") and Manner of Performing Functions and Duties) Rules, 2013, notified under the IT Act, prescribe mandatory reporting of cyber security incidents including data breaches and data leaks; (c) the CERT-In has issued binding directions under the IT Act, requiring entities to retain information and communication technology system logs, report cyber incidents and cybersecurity incidents within strict timelines, etc.; (d) the Consumer Protection Act, 2019, proscribes unfair trade practices, which includes disclosing to another person any personal information given in confidence by the consumer unless such disclosure is in accordance with applicable law; and (e) the *Bhartiya Nyaya Sanhita*, 2023 (which has repealed and replaced the Indian Penal Code, 1860), contains provisions that impose criminal liability for acts such as identity theft, impersonation, cheating, theft of movable property and criminal breach of trust, which may involve misuse of personal information.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. While the DPDP Act and the IT Act (read with the SPDI Rules) constitute the primary legal framework for data protection in India, several sector-specific legislation and regulatory guidelines such as those prescribed by the Securities and Exchange Board of India, the Reserve Bank of India ("**RBI**"), the Insurance Regulatory and Development Authority of India ("**IRDAI**") and the Telecom Regulatory Authority of India ("**TRAI**") impose certain obligations that impact the processing of customer data, which may include personal data. For instance, the RBI's Guidelines on Cyber Security Framework in Banks, Master Directions on Digital Payment Security Controls and Outsourcing of IT Services, Master Direction – Know Your Customer (KYC) Direction, 2016, etc., require regulated entities to implement adequate data protection to protect the integrity and security of data, and customer confidentiality.

Similarly, the IRDAI mandates insurers to establish robust governance mechanisms for protecting policyholder information. Its guidelines require insurers to implement information security policies, ensure confidentiality of customer data and adopt risk-based controls, particularly when outsourcing functions to third-party service providers.

1.4 What authority(ies) are responsible for data protection?

The DPDP Act contemplates the establishment of the Data Protection Board of India ("**DPB**"), which will serve as the enforcement and adjudicatory body under the DPDP Act and will be responsible for functions including inquiring into personal data breaches, directing remedial action and imposing penalties for non-compliance with the DPDP Act.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**
  The DPDP Act defines "Personal Data" as "any data about an individual, who is identifiable by or in relation to such data".
- **"Processing"**
  The DPDP Act defines "Processing" in relation to personal data as a wholly or partly automated operation or set of operations performed on digital personal data and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise, making available, restriction, erasure or destruction.
- **"Controller"**
  The DPDP Act uses the term Data Fiduciary (akin to a controller), defined as "any person who, alone or in conjunction with other persons, determines the purpose and means of the processing of personal data".
- **"Processor"**
  The DPDP Act defines a Data Processor as "any person who processes personal data on behalf of a Data Fiduciary".
- **"Data Subject"**
  The DPDP Act defines and uses the term "Data Principal" (akin to data subjects) as the individual to whom the personal data relates and where such individual is: (i) a child, including parents or lawful guardians of such a child; or (ii) a person with a disability, including her lawful guardian, acting on her behalf.
- **"Sensitive Personal Data"/"Special Categories of Personal Data"**
  The DPDP Act does not sub-categorise personal data into "Sensitive Personal Data" or "Special Categories of Personal Data".
- **"Data Breach"**
  The DPDP Act defines "personal data breach" to mean any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
- **"Automated"**
  The term "automated" has been defined to mean any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, the DPDP Act has extraterritorial applicability and extends to entities established outside India where the processing is carried out outside India in connection with offering goods or services to data principals located within India.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The DPDP Act applies only to: (a) digital personal data (i.e., personal data in digitised form); and (b) personal data collected in non-digital form that is subsequently digitised, and does not apply to: (i) personal data processed by an individual for any personal or domestic purpose; (ii) personal data that is made or is caused to be made publicly available by the data principal, or by a person under a legal obligation; (iii) processing by notified Central or State agencies in the interests of security of State, friendly relations with foreign States, maintenance of public order, etc.; and (iv) processing necessary for research, archiving or statistical purposes, if such personal data is not used for decision making and is carried out in accordance with prescribed standards.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The principle of transparency permeates the provisions of the DPDP Act. For instance, data fiduciaries are required to provide clear, comprehensive and easily accessible notices to data principals to obtain specific and informed consent from data principals, including setting out prescribed details such as categories of personal data to be processed and the purpose of the processing, the manner of exercise of rights available to the data principal, and the mechanism to make a complaint to the DPB. Further, the data principals are provided with rights to access information, including summary of processing activities undertaken by a data fiduciary, identities of all data fiduciaries and data processors with whom their personal data has been shared, etc.
- **Lawful basis for processing**
  The DPDP Act mandates that personal data should be processed only in a lawful manner and for lawful purposes, and in accordance with the provisions contained therein. It contemplates two distinct legal bases for such processing: (i) consent; and (ii) certain legitimate uses. As per Section 6 of the DPDP Act, processing of personal data may be undertaken with the free, specific, informed, unconditional and unambiguous consent of the data principal, obtained through clear affirmative action. Further, Section 7 of the DPDP Act also sets out nine specific "legitimate uses" for processing personal data without consent, such as for the purpose of employment, where processing is necessary for the performance of a legal function, compliance with a judgment or order, etc.
- **Purpose limitation**
  The principle of purpose limitation can be inferred from various provisions of the DPDP Act. Section 6(1) of the DPDP Act provides that the consent provided by the data principal will signify an agreement to the processing of her personal data for the specified purpose set out in the notice provided to them. The principle also applies in the context of legitimate uses specified under Section 7 of the DPDP Act, which permits processing only for certain identified use-cases, such as for the purpose of employment, performance of legal functions, etc.

- **Data minimisation**
  The principle of data minimisation can be inferred from various provisions of the DPDP Act. Section 6 of the DPDP Act states that consent provided by the data principal will be limited to such personal data as is necessary for the specified purpose for which personal data is collected as set out in the privacy notice provided to them.
- **Proportionality**
  This principle is reflected in multiple provisions of the DPDP Act that collectively require that the extent, manner and duration of processing of personal data (either with explicit consent or for legitimate use cases) must bear a reasonable nexus to the permitted purpose for which the personal data is being processed.
- **Retention**
  The DPDP Act provides that the personal data of a data principal may be retained only until (a) the data principal withdraws consent, or (b) as soon as it is reasonable to assume that the specified purpose is no longer being served, unless retention is required to ensure compliance with applicable law.
- **Accuracy**
  Section 8(3) of the DPDP Act requires that every data fiduciary ensure that personal data processed by it is complete, accurate and consistent, particularly where such data is used for decision making or is disclosed to another data fiduciary.
- **Accountability**
  While the term "accountability" is not expressly used, the DPDP Act effectively embeds this principle by providing that the data fiduciary will be responsible for ensuring compliance with the provisions of the DPDP Act, including with respect to any processing carried out on its behalf by a data processor, including by way of implementation of appropriate technical and organisational measures, adoption of reasonable security safeguards to prevent personal data breach, facilitation of exercise of data principal rights, obligation to notify personal data breaches to both the DPB and the affected data principals, etc.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
  The DPDP Act confers upon the data principal, the right to access information about her personal data, which includes obtaining from the data fiduciary, a summary of the personal data being processed in relation to her, details regarding the purpose of processing and the categories of data fiduciaries or data processors with whom such data has been shared.
- **Right to rectification of errors**
  The DPDP Act provides the data principal with the right to request the data fiduciary for the correction, completion or updating of her personal data for which she has previously given her consent, or for certain specified purposes for which the data principal has voluntarily provided such personal data.
- **Right to deletion/right to be forgotten**
  The DPDP Act provides data principals with the right to request erasure of their personal data, where such personal data was provided either based on consent or where the personal data has been voluntarily provided by the data principal for a specified purpose. In such cases, a data fiduciary is obligated to erase the data unless its retention is necessary to fulfil the original purpose or comply with legal obligations.
- **Right to object to processing**
  The DPDP Act does not recognise a standalone right to object to the processing of personal data. However, where processing is based on consent, the right to withdraw consent may be exercised specifically in relation to particular instances of processing.
- **Right to restrict processing**
  The DPDP Act does not confer a general right to restrict processing of personal data. However, where processing is based on consent or voluntarily provided personal data for a specified purpose, data principals may exercise their right to update or correct personal data, withdrawal of consent and/or right to erasure.
- **Right to data portability**
  The DPDP Act does not provide an express right to data portability.
- **Right to withdraw consent**
  The DPDP Act confers on the data principal the right to withdraw her consent at any time with comparable ease with which such consent was given. Such withdrawal of consent does not affect the lawfulness of processing undertaken prior to such withdrawal.
- **Right to object to marketing**
  The DPDP Act does not confer an express right to object to direct marketing. However, since consent is likely the primary basis for processing personal data for marketing purposes, the data principal may withdraw consent for such purpose at any time.
- **Right protecting against solely automated decision-making and profiling**
  The DPDP Act does not contain any express provisions restricting or regulating automated decision-making or profiling. However, please see our response to question 6.1 on prohibitions relating to children's data and question 19.1 for additional obligations on Significant Data Fiduciaries ("**SDFs**") for use of automated software.
- **Right to complain to the relevant data protection authority(ies)**
  The DPDP Act provides data principals with the right to complain to the DPB in respect of any breach of obligations by a data fiduciary or a consent manager. This right is subject to the prior exhaustion of the data fiduciary's grievance redressal mechanism.
- **Other key rights:**
  - **Right to grievance redressal**: Section 13 of the DPDP Act provides data principals with the right to have a readily available means of grievance redressal provided by a data fiduciary or consent manager regarding the performance of its obligations contained thereunder.
  - **Right to nominate**: Section 14 of the DPDP Act confers on data principals the right to nominate one or more individuals to exercise their rights under the DPDP Act in the event of their death or incapacity.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

No, the DPDP Act does not provide any such right to data principals.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Under the DPDP Act, data fiduciaries must obtain verifiable consent from a parent or guardian before processing a child's personal data, with a child defined as an individual under 18 years of age. The Draft Rules require technical safeguards to ensure consent and due diligence to verify the adult's identity, using existing data or voluntarily provided details including authorised credentials like virtual tokens. The DPDP Act also prohibits tracking, targeted advertising and harmful processing of children's data. Pursuant to enabling provisions under the DPDP Act, the Central Government proposes to exempt certain data fiduciaries such as healthcare, education and childcare providers from consent and monitoring restrictions, provided processing is limited to necessary functions for child welfare.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, under the DPDP Act, there is no general obligation for data fiduciaries to register with or notify the DPB merely by virtue of engaging in personal data processing. That said, the Draft Rules envisage a specific registration requirement for entities intending to function as consent managers, which is an entity that enables a data principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform. Rule 4 of the Draft Rules propose that a consent manager is required to obtain registration from the DPB as per the prescribed eligibility conditions, including the requirement for it to be a company incorporated in India, and other obligations that must be satisfied or fulfilled prior to and during the term of such registration.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please refer to our response to question 7.1 above.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please refer to our response to question 7.1 above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to our response to question 7.1 above.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to our response to question 7.1 above.

7.6 What are the sanctions for failure to register/notify where required?

Please refer to our response to question 7.1 above. Failure by a consent manager to obtain registration may attract penalties of up to INR 50 crores.

7.7 What is the fee per registration/notification (if applicable)?

Please refer to our response to question 7.1 above. Any fees for registration as a consent manager are currently not provided under the Draft Rules; however, they may be stipulated by the DPB.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to our response to question 7.1 above. The Draft Rules currently do not contemplate renewal of registration of a consent manager but provide for suspension or cancellation of registration upon any contravention by such entities of any of their obligations.

7.9 Is any prior approval required from the data protection regulator?

Please refer to our response to question 7.1 above. No such prior approval is required for a consent manager.

7.10 Can the registration/notification be completed online?

Please refer to our response to question 7.1 above. The DPB is envisaged to be a completely digital office and therefore, the registration process in respect of a consent manager is likely to be online.

7.11 Is there a publicly available list of completed registrations/notifications?

Please refer to our response to question 7.1 above. The Draft Rules provide for publication of particulars of registered consent managers on the DPB's website.

7.12 How long does a typical registration/notification process take?

Please refer to our response to question 7.1 above. There are no timelines stipulated as of now under the Draft Rules for completion of the process of registration as a consent manager.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

All the data fiduciaries are required to publish, in the prescribed form, the business contact details of either (a) the Data Protection Officer ("**DPO**") (if appointed), or (b) another designated person capable of addressing questions raised by the data principal regarding the processing of their personal data. The requirement to appoint a DPO arises only where a data fiduciary is designated as an SDF by the Central Government under Section 10(1) of the DPDP Act.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO may lead to monetary penalties of up to INR 150 crores.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The DPDP Act does not contain any such specific protections.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. The DPDP Act does not prohibit or address the appointment of a single DPO to serve multiple entities. However, such DPO will need to comply with other conditions such as being based in India and also be practically required to be responsible to the Board of Directors or similar governing body of the SDF, as well as act as the point of contact for the grievance redressal mechanism of such SDFs. Therefore, if a DPO is appointed to cover multiple entities, such DPO will need to be able to effectively perform their functions in relation to each such entity covered.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPDP Act does not prescribe any specific qualifications for the appointment of a DPO. Practically, any person appointed as the DPO will need to be qualified, experienced and capable of complying with their obligations.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please refer to our response to question 8.5 for the responsibilities of a DPO prescribed under the DPDP Act.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The DPDP Act does not require SDFs to register/notify the appointment of DPO to the DPB or any other authorities.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPDP Act requires that the business contact information of the DPO (if appointed) or a contact person, must be: (i) prominently published on the website or app of the data fiduciary; and (ii) included in every response issued to a data principal in relation to the exercise of their rights contained thereunder. The DPDP Act does not prescribe any specific requirements relating to the placement of the DPO details on its website or app, and accordingly, may be named in a public-facing privacy policy published on its website as well. Further, the details of such DPO will need to be provided in the notice provided to the data principal to obtain their consent.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Section 7(b) of the DPDP Act mandates a data fiduciary (which includes a business/entity) to engage, appoint, use, or otherwise involve a data processor to process personal data on its behalf only under a valid contract.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The DPDP Act does not prescribe specific formalities or mandatory clauses for agreements to be entered into between a data fiduciary and a data processor. However, given the DPDP Act places the responsibility of the processing undertaken by a data processor on the data fiduciary, it is recommended that the agreement between the data fiduciary and the data processor records the obligations of the data processor, including scope and limits of the processing activities, reasonable security measures to be adopted, personal data breach reporting obligations, etc., and appropriate representations and warranties backed by indemnities are sought.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The DPDP Act does not prescribe any specific restrictions on sending of electronic direct marketing. However, it is likely that organisations will need to rely on consent as the basis for processing personal data for marketing purposes. Accordingly,

the notice and consent obligations provided under the DPDP Act will need to be complied with.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The DPDP Act applies to processing of any digital personal data that relates to an individual, regardless of the business context, i.e., the DPDP Act does not differentiate between business-to-consumer and business-to-business context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

In addition to the notice and consent requirements under the DPDP Act, in the event of sending marketing or promotional messages or calls, the Telecom Commercial Communications Customer Preference Regulations, 2018, issued by the TRAI, prescribe certain requirements such as obtaining prior consent for promotional messages, providing opt-out mechanisms to customers, checking the National Customer Preference Register, etc.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the DPDP Act has extraterritorial applicability and extends to entities established outside India, if such processing of personal data is in connection with offering goods or services to data principals located within India.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

At the time of writing, there is limited enforcement of the data protection framework envisaged under the SPDI Rules. However, once the DPDP Act is enforced and as the law evolves, we expect that the DPB will be active in enforcement of the notice and consent requirements mentioned thereunder, which will apply to marketing.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The DPDP Act does not explicitly prohibit purchase of marketing lists or payment of any consideration for acquisition of such lists. However, given that consent is likely to be the primary basis for processing personal data for marketing purposes, it is recommended to ensure, through contractual arrangements, that appropriate consent has been obtained from the data principal by the transferor to share such personal data, as well as for the receiving/transferee entity to process such personal data for marketing purposes, in addition to seeking appropriate representations and warranties backed by indemnities.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Failure to observe compliance under the DPDP Act relating to personal data processed for sending marketing communications may lead to monetary penalties of up to INR 50 crores, with the exact amount of penalty to be determined by the DPB based on factors such as the nature, severity, type of personal data affected, etc.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The DPDP Act does not specifically address the use of cookies. If the cookies (or similar technologies) collect/process personal data, then the requirements under the DPDP Act will need to be complied with. For most use cases, we expect consent to be the basis for processing personal data collected through such cookies. Accordingly, data fiduciaries will need to provide appropriate notice and obtain consent as required under the DPDP Act. Further, in case of children's personal data, the prohibitions on tracking or behavioural monitoring of children or targeted advertising directed at children, will need to be adhered to.

Additionally, the IT Act prohibits unauthorised access to computer systems and data. Accordingly, consent may need to be obtained from the owners or authorised users of the computer systems and data in order to place cookie files or use similar technologies on their systems.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The DPDP Act does not specifically address the use of cookies and therefore, it does not distinguish between different types of cookies. However, to meet the requirements of consent (such as free, specific, etc.) separate consents may need to be obtained depending on the purposes for which the personal data collected through cookies is utilised (such as functional, advertising, etc.).

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

At the time of writing, given the DPDP Act is yet to be enforced, there have not been any such reported enforcement actions.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

If cookies are used to collect or process personal data of data principals in breach of the requirements prescribed under the DPDP Act, such processing may lead to monetary penalties of up to INR 250 crores depending on the type of non-compliance.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Section 16 of the DPDP Act allows free cross-border transfer of personal data except to countries notified by the Government of India as restricted/prohibited (this is yet to be notified). In this regard, Rule 12 of the Draft Rules proposes certain restrictions relating to the transfer of personal data to other jurisdictions in the context of SDFs, wherein the Central Government, based on recommendations of a committee it constitutes, may specify certain personal data sets and the traffic data pertaining to its flow that cannot be transferred outside India. Further, as per the Draft Rules, cross-border transfer of personal data by any data fiduciary is proposed to be permitted subject to compliance with conditions prescribed by the Central Government, in respect of making such personal data available to foreign States or entities under their control.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Any transfer of personal data abroad will need to be in accordance with consent provided by the data principal or based on one of the nine specified legitimate uses, or under one of the exempted grounds provided under Section 17(1) of the DPDP Act, such as for the purpose of enforcement of a legal right or claim, for the purpose of a merger or amalgamation sanctioned by a competent authority, etc. The DPDP Act does not provide any further requirements in relation to cross-border transfer. However, organisations typically enter into data processing agreements recording the details of the transfer and obtain appropriate representations, warranties and indemnities, depending on the role of the transferor and transferee entities.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no requirement under the DPDP Act to obtain any registration/notification or prior approval from the DPB or any other authority for the purpose of transfer of personal data to other jurisdictions.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

No, there are no such transfer impact assessments prescribed under the DPDP Act. However, as per Section 10 of the DPDP Act, SDFs are required to undertake periodic data protection impact assessments, which may include transfer-related risks.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

There has been no such guidance issued as of the time of writing by any competent authority.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There has been no such guidance issued as of the time of writing by any competent authority. However, as a matter of practice, and as may be required under foreign laws, many organisations, especially multinational organisations, adopt standard contractual clauses issued by competent authorities under the EU GDPR and other competent foreign authorities in implementing international data transfers.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no specific whistleblower protection requirements under the DPDP Act. The principal legislation on this subject, the Whistleblower Protection Act, 2014 ("**Whistleblower Act**"), which aims to safeguard individuals reporting corruption or abuse of power by public servants, has not yet been brought into force. However, the Companies Act, 2013, and applicable securities regulations mandate certain classes of companies to establish vigil or whistleblower mechanisms, offering protection against victimisation of employees or directors raising concerns. The mechanism enables reporting of unethical behaviour, suspected fraud, or violations of the company's code of conduct or ethics policy. Additionally, the RBI's Master Directions on Frauds (dated July 1, 2016) require commercial banks and select financial institutions to adopt whistleblower policies that encourage reporting of fraudulent activities in accounts and ensure protection for whistleblowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Please see our response to question 13.1 above. While the laws discussed above do not prohibit anonymous reporting, the identification of the whistleblower may be required to seek additional clarifications or information from such individuals. Under the Whistleblower Act, identification of the whistleblower is expressly required to prevent abuse of process.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, there are no such registration/notification/prior approval requirements prescribed under the DPDP Act. However, depending on the use case for processing of personal data collected through CCTV, such as where the CCTV is installed in a public place, within a private property, commercial property, etc., the legal basis for such processing may need to be evaluated. As a recommended best practice, there should be an evaluation of reasonable expectation of privacy of an individual and appropriate notices by way of a high visibility sign, etc.

14.2 Are there limits on the purposes for which CCTV data may be used?

Depending on the legal basis for processing personal data captured through CCTV, purpose limitation and retention requirements should be adhered to.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

One of prescribed legitimate uses (for which consent is not required) includes processing of personal data for the purpose of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by an employee. In such cases, employee monitoring through various means such as CCTV, email and device monitoring, etc., may be permitted.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Please see our response to question 15.1 above.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The DPDP Act does not prescribe notification to or consultation with representatives of works councils/trade unions/employees.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

If such processing can be justified under the legitimate use cases described in our response to question 15.1, we believe such employee attendance information may be permitted to be processed. For abundant caution, consent may be sought by organisations for such use cases that may not strictly be justified under the permitted legitimate use.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, Section 8(4) of the DPDP Act requires every data fiduciary to implement reasonable security measures to prevent personal data breaches. The Draft Rules propose certain minimum-security measures to be implemented, including: encryption; access control; maintenance of logs to monitor, review and detect unauthorised access and take remedial measures; and data backups to mitigate operational disruption caused by compromise in confidentiality or availability of personal data; etc.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, the DPDP Act requires the data fiduciary to intimate the DPB in the event of a personal data breach. As per the Draft Rules, the data fiduciary, upon becoming aware of the personal data breach, must provide to the DPB, without delay, a preliminary notification containing the description of the breach including its nature, extent, timing, location and potential impact. Thereafter, a more detailed intimation needs to be made to the DPB within 72 hours (or within such extended timeline permitted by the DPB) with updated information, including measures implemented or proposed to mitigate risk, findings of the investigation, remedial measures undertaken and intimations given to affected data principals.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, the DPDP Act requires the data fiduciary to intimate the affected data principals in the event of a personal data breach. As per the Draft Rules, the affected data principals must be notified without delay, through their user account or any other mode of communication opted by the data principal, with the details of the nature and extent of the breach, potential consequences for the data principal, the safety measures to be implemented by them to protect their interests, and business contact information of a person who can answer their queries.

16.4 What are the maximum penalties for personal data security breaches?

Under the DPDP Act, failure by a data fiduciary to take reasonable security safeguards to prevent personal data breaches can attract a monetary penalty of up to INR 250 crores.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative powers:** The DPB can initiate inquiries into personal data breaches or non-compliance by data fiduciaries, processors or consent managers. At DPB's discretion, it may also direct the parties concerned to attempt resolution of the dispute through mediation by a mutually agreed mediator, or as provided by any applicable law.

(b) **Corrective powers:** The DPB may issue binding directions to require remedial or mitigation measures in case of a personal data breach or issue directions to data fiduciaries or consent managers pursuant to an investigation in relation to non-compliance with the DPDP Act. It may also accept voluntary undertakings from parties to ensure compliance, which can include commitments to specific actions or refraining from certain conduct.

(c) **Authorisation and advisory powers:** The DPB does not currently have explicit authorisation or advisory powers under the DPDP Act.

(d) **Imposition of administrative fines for infringements of specified legal provisions:** The DPB is empowered to impose monetary penalties of up to INR 250 crores for violations of the DPDP Act, following an opportunity to be heard.

(e) **Non-compliance with a data protection authority:** Failure to comply with the terms of a voluntary undertaking may lead to enforcement proceedings and penalties under Section 33 of the DPDP Act, following an opportunity to be heard. Any person aggrieved by an order or direction made by the DPB may prefer an appeal before the Appellate Tribunal. An order passed by the Appellate Tribunal will be executable by it as a decree of the civil court.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The DPB has broad powers to issue such directions as it may consider necessary, for the effective discharge of its functions and also direct remedial or corrective measures in case of a personal data breach. Such directions may include a ban on a particular processing activity, if considered necessary by the DPB.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As the DPDP Act is yet to be enforced and the DPB is yet to be established, we currently do not have any precedents to establish the DPB's approach.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

As discussed under our response to question 3.1, the DPDP Act does have extra-territorial applicability in certain cases. We will need to see how the enforcement trends evolve once the DPDP Act is notified, in order to establish the manner of enforcement against businesses established abroad. Having noted that, the Indian Supreme Court is hearing a case involving challenge to WhatsApp's privacy policy for violating the right to privacy, in particular, where the policy update of 2021 permits WhatsApp to share data with Facebook and all its group companies for the purposes of commercial advertising and marketing. In this case, the Supreme Court has ordered that in the interim, WhatsApp must publicise that users of WhatsApp who have not yet accepted the privacy policy update of 2021 may continue to use WhatsApp without fear of their accounts being deleted.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses typically evaluate the scope of the request as well as its legal validity, prior to disclosure of personal data. Most contracts under which businesses may have received information may have requirements to inform the transferor regarding such requests to enable them to obtain necessary stay or similar protective orders in respect of such requests, as well as to share only limited information necessary to comply with such requests.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There has been no such guidance issued. However, the Draft Rules propose that such transfer is to be permitted subject to compliance with conditions prescribed by the Central Government, in respect of making such personal data available to foreign States or entities under their control.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

No, there are no such requirements. However, the Draft Rules propose that SDFs are required to observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of data principals.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

No formal guidance has been issued under the DPDP Act on AI-related personal data processing. However, the MeitY has issued directions to address AI-related harms such as deepfakes. Notably, MeitY's AI Governance Report (dated January 6, 2025) outlines non-binding recommendations for

AI developers and deployers to comply with data protection laws, respect user privacy and implement safeguards like data quality and security-by-design.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Given the nascency of the DPDP Act, and its impending notification, there have been no notable enforcement trends to report during the previous 12 months.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

The DPDP Act is yet to be enforced, and the DPB is yet to be constituted; however, several "hot topics" are already drawing regulatory and stakeholder attention. Some of these include the treatment of cross-border data transfers, with a focus on potential data localisation requirements for SDFs. Another critical area is the processing of children's data, where the mechanism for obtaining verifiable parental consent is still under debate. Additionally, the use of publicly available personal data, particularly for purposes like profiling, targeted advertising or AI training, is under scrutiny to ensure such usage aligns with the provisions and requirements of the DPDP Act.

Acknowledgments

We would like to extend our sincere gratitude to Prateek Pushkarna and Shruti Agrawal, Associates at AZB & Partners, for their invaluable contributions to this chapter.

Rachit Bahl is a Senior Partner in the Firm's Delhi office with over 20 years of experience advising multinational corporations, including several *Fortune 500* companies, on complex regulatory, policy, and strategic matters. His practice focuses on data protection and privacy, technology law, telecommunications, fintech, and digital business models. He has worked extensively on issues relating to the implementation of global and Indian data protection frameworks, including the Digital Personal Data Protection Act, 2023, and sector-specific privacy obligations. Rachit regularly assists clients in developing cross-border data transfer mechanisms, privacy risk assessments, data breach response protocols, and privacy-by-design integration for digital products and services.

AZB & Partners
AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: rachit.bahl@azbpartners.com
LinkedIn: www.linkedin.com/in/rachit-bahl-14a502102

Rohan Bagai is a Senior Partner in the Firm's Delhi office with over 18 years of experience and deep expertise in data protection, privacy, and digital business regulation. He regularly counsels domestic and international clients on legal, regulatory, and compliance frameworks relating to data protection and privacy, digital payments, fintech, and e-commerce. Rohan has considerable experience advising on data protection and privacy matters under the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and sectoral guidelines issued by regulators such as the Reserve Bank of India (RBI). His work includes data discovery and mapping, privacy impact assessments, consent and data retention frameworks, cross-border data transfer strategies, and review of vendor and intra-group data processing arrangements.

AZB & Partners
AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: rohan.bagai@azbpartners.com
LinkedIn: www.linkedin.com/in/rohanbagai

Sumit Ghoshal is a Senior Partner based in the Delhi office with over 18 years of experience advising clients on legal, regulatory, and commercial aspects of e-commerce, digital platforms, technology transactions, and data protection. His practice focuses on supporting businesses in launching and operating digital services in India, including online marketplaces, digital content platforms, and next-generation consumer technology products. He has advised a wide range of clients on structuring and implementing e-commerce models, including website operations, online sale and marketing of products, licensing and registration requirements, and drafting commercial contracts and platform agreements.

AZB & Partners
AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: sumit.ghoshal@azbpartners.com
LinkedIn: www.linkedin.com/in/sumit-ghoshal-ab2534125

Archana Iyer is a Senior Associate with over nine years of specialised experience in TMT law, with a focus on data protection and artificial intelligence (AI). She advises clients across diverse sectors, including e-commerce, digital products, healthcare, AI, digital advertising, fintech, and telecommunications. Archana has developed deep expertise in India's evolving data protection landscape, particularly under the Digital Personal Data Protection Act, 2023. She supports clients through data discovery, data mapping, and identifying compliance gaps, while recommending actionable compliance roadmaps. Her privacy practice includes reviewing UI/UX for consent mechanisms, drafting or review of SOPs, privacy policies, data retention, and archiving policies, etc.

AZB & Partners
AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: archana.iyer@azbpartners.com
LinkedIn: www.linkedin.com/in/archana-iyer-22b6a032

AZB & Partners was founded in 2004 with a clear purpose to provide reliable, practical and full-service advice to clients, across all sectors. Having grown steadily since its inception, the Firm now has offices across Mumbai, Delhi, Bangalore, Pune, and Chennai.
The Firm has an accomplished and driven team of 650+ lawyers committed to delivering best-in-class legal solutions to help every client achieve their objectives. The Firm works on both advisory and transactional mandates and often in a cross-jurisdictional context.

www.azbpartners.com

AZB & PARTNERS
ADVOCATES & SOLICITORS

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2025 features four expert analysis chapters and 27 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence

The International Comparative Legal Guides are published by: glg Global Legal Group