PANORAMIC

# DATA PROTECTION & PRIVACY

India

LEXOLOGY

# Data Protection & Privacy

Contributing Editors

**Aaron P Simpson and Lisa J Sotto**

Hunton Andrews Kurth LLP

**Generated on: July 12, 2024**

# Contents

## Data Protection & Privacy

## SHARING AND CROSS-BORDER TRANSFERS OF PI



## RIGHTS OF INDIVIDUALS



## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS



## SPECIFIC DATA PROCESSING



## UPDATE AND TRENDS

# Contributors

## India

Kochhar & Co

**Stephen Mathias** stephen.mathias@bgl.kochhar.com
**Arun Babu** arun.babu@bgl.kochhar.com

## LAW AND THE REGULATORY AUTHORITY

### Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

India's current data protection law

India currently has minimal data privacy laws that solely govern the processing of a special category of personal information termed Sensitive Personal Data or Information (SPDI). The relevant statute is the Information Technology Act, 2000 (the IT Act) and the applicable statutory provision is section 43A of the IT Act. Section 43A defines SPDI to mean passwords, financial information (such as bank account, credit card, debit card or other payment instrument details), sexual orientation, health information, medical records and biometrics, and obligates an entity processing SPDI to implement Reasonable Security Practices and Procedures (RSPP) to protect such data. An entity negligent in implementing RSPP is obligated to pay compensation to the persons affected if such negligence results in a wrongful gain or a wrongful loss.

Under section 43A of the IT Act, the government has notified the Information Technology (RSPP and SPDI) Rules 2011 (Privacy Rules). The Privacy Rules prescribe, among others:

- notice and consent requirements for the collection and processing of SPDI;
- compliance requirements for the disclosure and transfer (including cross-border transfer) of SPDI; and
- examples of information security standards that would be deemed to be RSPP.

It is, however, important to note that compliance with the Privacy Rules is not mandatory. This is because RSPP is defined to mean a law in force (there is none) or as agreed between the parties, and in the absence of the same, the rules formed by the government. This means that if a data controller and data subject agree on what is meant by RSPP, their agreement would govern over the Privacy Rules. Further, even if one does not comply with the Privacy Rules, there is no legal consequence unless a data breach or some perverse event occurs in relation to SPDI and it results in a wrongful gain or wrongful loss. It may be noted that wrongful gain or wrongful loss under India's criminal code is associated with dishonest or fraudulent conduct.

India's new data protection law

India's current data privacy laws will soon be replaced by a new data protection law, the Digital Personal Data Protection Act 2023 (DPDPA). The DPDPA is India's first comprehensive data protection statute and was enacted by the Indian Parliament in August 2023. The DPDPA has, however, not yet come into force, and the government is expected to implement the law by end of 2024.

The DPDPA regulates the processing of all PI maintained in digital form, and prescribes among others:

- notice and consent requirements for processing digital PI;
- certain legitimate uses of PI for which consent is not required;
- rights and duties of data principals (akin to data subjects under the GDPR);
- obligations of data fiduciaries (akin to data controllers under the GDPR); and
- monetary penalties for non-compliance.

The DPDPA is not specifically based on any international instrument or laws of other jurisdictions. It includes the typical rights of data principals and obligations of data fiduciaries that are generally included in the laws of most jurisdictions.

It is relevant to note that the requirements for obtaining valid consent under the DPDPA are almost identical to those under the GDPR. However, unlike the GDPR, the DPDPA does not include other lawful grounds of processing, such as legitimate interest and contractual necessity, and does not include rights such as the right to data portability and the right to not be subjected to automated decision-making.

**Law stated - 13 June 2024**

## Data protection authority

### Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

Data protection authority under India's current data protection laws

India presently does not have a data protection authority. The Ministry of Electronics and Information Technology (Meity) administers the IT Act, and the Meity can therefore be considered as the authority responsible for overseeing the implementation of India's current data protection law (ie, section 43A of the IT Act). The Meity, however, does not have any specific investigative powers, including powers to require information or to carry out audits or inspections, under section 43A of the IT Act.

Data protection authority under the DPDPA

The DPDPA provides for the establishment of the Data Protection Board of India (DPBI). The DPBI has, however, not yet been set up and notified, but the government is expected to do this within the next few months.

The DPDPA grants powers to the DPDPA to inquire into:

- a PI breach upon receiving a breach notification; or
- a complaint made by a data principal or a reference made to the DPBI by the government or a court, regarding a PI breach.

The DPBI is also granted powers to investigate complaints against a data fiduciary in relation to a breach of their obligations under the DPDPA or in relation to non-compliance by a data fiduciary in the case of exercise of data principals' rights. The DPBI is also empowered to investigate complaints against a 'Consent Manager' in relation to a breach of their obligations under the DPDPA. A consent manager is an entity registered with the DPBI that acts as a single point of contact to enable data principals to grant, manage and withdraw consent through an electronic platform.

To discharge its abovementioned investigative powers under the DPDPA, the DPBI is vested with the powers of a civil court and is empowered to summon any person and examine such person on oath, receive evidence by way of affidavit, require the discovery and production of documents, and inspect any document, register, books of accounts, etc.

Further, the DPDPA also empowers the government to call for information from the DPBI or any data fiduciary or any intermediary, for purposes related to the DPDPA.

It may be noted that the rule-making powers under the DPDPA vest with the government and not with the DPBI. Accordingly, both the government and the DPBI can be considered data protection authorities under the new law.

**Law stated - 13 June 2024**

## Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

No, there are no specific obligations under India's data privacy laws (including the DPDPA) that require data protection authorities to cooperate with other data protection authorities.

There is also no specific mechanism to resolve different approaches. The DPDPA, however, states that its provisions will not restrict the applicability of any other law in India that provides for a higher degree of protection for or restriction on, cross-border transfer of PI. In this regard, it is relevant to note that India has sector-specific laws that impose data localisation restrictions on certain types of data sets and certain types of regulated entities operating in sectors such as payments, digital lending, insurance, telecom and securities.

Further, the DPDPA also stipulates that its provisions shall be in addition to and not in derogation of any other law in India, and that in the event of a conflict with any other law, the provisions of the DPDPA would prevail.

**Law stated - 13 June 2024**

## Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

A breach of India's current data protection law (ie, section 43A of the IT Act) can only result in a payment of compensation to the persons affected, and criminal penalties are not prescribed.

On a related note, section 72A of the IT Act prescribes criminal punishment where a service provider who secures access to PI (any PI, not just SPDI) discloses such PI without consent or in breach of contract with the intention of or knowing that it is likely to result in wrongful gain or wrongful loss. The language of this provision is such that it largely deals with criminal behaviour.

A breach of the DPDPA can only lead to monetary penalties, and there are no criminal penalties prescribed. The DPDPA empowers the DPBI to issue administrative orders or sanctions while discharging its powers. Upon receiving a complaint regarding a breach of the DPDPA and on determining that there are sufficient grounds to proceed with an inquiry, the DPBI will investigate the matter. While performing such inquiry, the DPBI has the same powers vested in a civil court under Indian law, and the DPBI is empowered to summon and enforce the attendance of any person, receive evidence on affidavit, and inspect any data, documents, books of account, etc. On conclusion of the inquiry, if the DPBI concludes that a significant breach of the DPDPA has occurred, the DPBI can issue a monetary penalty as prescribed under the DPDPA. The DPBI is also empowered to issue a warning or impose costs on the complainant in the case of false or frivolous complaints.

A breach of India's cybersecurity regulations can result in a term of imprisonment of one year or a fine of 10 million rupees, or both. However, the relevant regulator (the Computer Emergency Response Team) has clarified that its powers to prosecute will only be exercised reasonably and on occasions of deliberate non-compliance.

**Law stated - 13 June 2024**

### Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Yes, as per the DPDPA, a person aggrieved by an order of the DPBI can appeal to the Telecom Dispute Settlement and Appellate Tribunal (TDSAT), a quasi-judicial body established under the Telecom Regulatory Authority of India Act, 1997. An appeal against an order of the TDSAT can lie in the Supreme Court of India.

**Law stated - 13 June 2024**

## SCOPE

### Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

India's current data privacy law covers all sectors and applies to all bodies corporate. A body corporate is any company, including a firm, sole proprietorship or other association of

individuals, engaged in any commercial or professional activity. The law does not apply to the government.

The Digital Personal Data Protection Act 2023 (DPDPA) covers all sectors and all types of organisations.

There are, however, certain exemptions available to the government. The DPDPA grants the power to the government to exempt certain government agencies (to be notified by the government) from compliance with the law. Certain grounds are mentioned: the interests of sovereignty, integrity and security of India; friendly relations with foreign states; maintenance of public order; and preventing any cognisable offence related to the foregoing. Further, there is a direct exemption given to any agency involved in the performance of judicial, quasi-judicial, regulatory or supervision functions. Limitations on retention of data also do not apply to the government.

The DPDPA also does not apply to the processing of PI necessary for research, archiving or statistical purposes if such PI is not used to take a decision specific to a data principal and such processing is carried out in accordance with standards to be prescribed by the government.

Further almost all the substantive provisions of the DPDPA do not apply to the processing of PI necessary for:

- enforcing any legal right or claim;
- the prevention, detection, investigation or prosecution of any offence;
- a scheme of compromise or arrangement or merger or amalgamation or demerger of a company, or transfer of undertaking, or division of a company, approved by a court or any other competent authority; and
- ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance from a financial institution.

In addition, almost all the substantive provisions of the DPDPA do not apply where the PI of foreign data principals is processed by a person in India pursuant to a contract entered into with a person outside India.

**Law stated - 13 June 2024**

## Interception of communications and surveillance laws

### Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

India's data privacy laws (including the DPDPA) do not cover the interception of communications, electronic marketing, or monitoring and surveillance of individuals.

However, under the DPDPA, unless exempted by the government, data fiduciaries are prohibited from undertaking tracking or behavioural monitoring of children, or targeted advertising directed at children. A child is defined under the DPDPA as a person aged less than 18 years.

The relevant laws governing the interception of communications, and monitoring and surveillance of individuals are the Information Technology Act, 2000 (IT Act) and the Indian Telegraph Act, 1885 (Telegraph Act).

The IT Act authorises government agencies to intercept, monitor, or decrypt any information transmitted, received or stored through any computer system if the government deems such actions necessary in the interest of:

1. the sovereignty, integrity, defence or security of India;
2. friendly relations with foreign countries;
3. public order;
4. preventing incitement to the commission of any cognisable offence relating to (1)–(3); or
5. investigation of any offence.

The IT Act also authorises government agencies to monitor and collect traffic data or information generated, transmitted, received or stored in any computer system for cybersecurity purposes or for the identification, analysis and prevention of computer contaminants.

The Telegraph Act authorises government entities to take temporary possession of the telecommunications infrastructure, direct that any messages or class of messages to or from any person or class of persons not be transmitted, and direct that any messages or class of messages to or from any person or class of persons be intercepted or detained or be disclosed to the government if these messages are brought for transmission by or transmitted or received by any telegraph. The government can exercise its said powers under the Telegraph Act only in case of a public emergency or in the interest of public safety or in case of grounds for exercising surveillance powers under the IT Act (listed above).

Further, the Telecom Commercial Communication Customer Preference Regulations 2018 govern the transmission of commercial communications, including marketing communications, using telecommunication services.

**Law stated - 13 June 2024**

## Other laws

### Are there any further laws or regulations that provide specific data protection rules for related areas?

India has sector-specific data protection laws that apply to regulated entities operating in various sectors such as banking, insurance, securities, payments and telecommunications. Further, there are specific data protection laws that apply to credit information companies and credit institutions.

India also has intermediary regulations that prescribe due diligence measures and content takedown requirements for social media platforms.

There is, however, no specific law governing employee monitoring and e-health records.

**Law stated - 13 June 2024**

## PI formats

What categories and types of PI are covered by the law?

India's current data privacy laws solely apply to the processing of Sensitive Personal Data or Information (SPDI). The law does not apply to SPDI that is freely accessible in the public domain or furnished under any other law.

The DPDPA applies to the processing of all PI maintained in digital form. The DPDPA, however, does not apply to the processing of PI that is made publicly available by the data principal or by any person obligated under law to do so. There is also no distinction under the law between PI and sensitive PI.

**Law stated - 13 June 2024**

## Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The reach of India's current data protection laws is limited to PI owners and processors physically established or operating in India, and the law does not have extraterritorial applicability.

With regard to the PI of Indians processed outside India, the DPDPA applies to the PI of persons in India processed outside India, where such processing is in connection with any activity related to offering of goods and services to data principals within India.

With regard to the PI of persons outside India but processed in India, almost all substantive provisions of the DPDPA do not apply where the PI of foreign PI owners is processed by a person in India pursuant to a contract entered into with a person outside India.

**Law stated - 13 June 2024**

## Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

India's current data protection laws apply to all processing or use of SPDI. The law does not distinguish between data controllers and data processors. Further, controllers' and processors' duties and obligations do not differ. Further, the law does not stipulate any specific duties or obligations on data owners.

The DPDPA applies to all processing or use of PI maintained in digital form, except for the use of PI for personal or domestic purposes, processing by notified government agencies

in certain situations, and for processing necessary for research, archiving, or statistical purposes in a prescribed manner.

The DPDPA distinguishes between a data principal (the person to whom the PI belongs); a data fiduciary (the person who controls the purpose and means for processing); and a data processor (a person providing processing services to the data fiduciary). There are specific duties prescribed under the DPDPA for data principals and data fiduciaries. There are, however, no specific duties stipulated for data processors, and a data fiduciary is responsible for compliance with the DPDPA in respect of any processing undertaken by its data processors on its behalf.

**Law stated - 13 June 2024**

## LEGITIMATE PROCESSING OF PI

### Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

No, India's current data privacy laws do not include any specific grounds legitimising the processing of PI. The Information Technology (RSPP and SPDI) Rules 2011 (the Privacy Rules) require that consent be obtained to process Sensitive Personal Data or Information (SPDI). However, compliance with the Privacy Rules is not mandatory.

Consent is the main lawful basis for processing PI under the Digital Personal Data Protection Act 2023 (DPDPA). However, the law prescribes certain 'legitimate uses' of PI for which consent is not required to be obtained. These include processing for:

- a specified purpose for which the data principal has voluntarily given his or her PI without any indication that consent is not granted;
- purposes related to employment or to safeguard an employer from loss or liability or to provide a benefit or service sought by a data principal who is an employee;
- responding to a medical emergency, or taking measures to provide medical treatment or services during an epidemic or outbreak of disease, or to provide assistance in case of a disaster or breakdown of public order;
- performance of state functions;
- compliance with any judgment or court order; and
- compliance with any law that requires disclosure of any information to the government.

**Law stated - 13 June 2024**

### Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

No, India's current data privacy laws do not impose more stringent rules for processing specific categories of PI. However, the law does not apply to all PI and only applies to the processing of SPDI.

The DPDPA does not impose more stringent rules for processing specific categories and types of PI. There are, however, additional safeguards prescribed for processing children's PI. A child is defined under the law as a person aged less than 18 years.

It is also relevant to note that India has sector-specific data protection laws that prescribe rules for processing certain specific types of PI, such as payment data, insurance records and telecommunications customer information, by regulated entities operating in various sectors, such as banking, payments, insurance, securities and telecommunications.

**Law stated - 13 June 2024**

## DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

### Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Information Technology (RSPP and SPDI) Rules 2011 (the Privacy Rules) require entities that collect, receive, possess, store or deal with or handle Sensitive Personal Data or Information (SPDI) to provide a privacy policy that includes:

- clear and easily accessible statements of its practices and policies;
- the types of SPDI collected;
- the purpose of collection and usage of such SPDI;
- details regarding the disclosure of SPDI to third parties; and
- the Reasonable Security Practices and Procedures (RSPP) adopted by such entity.

However, compliance with the Privacy Rules is not mandatory.

The Digital Personal Data Protection Act 2023 (DPDPA) obligates a data fiduciary to provide a privacy notice at or prior to, the time of obtaining consent. Such privacy notice must contain the PI intended to be collected and the purposes for which such collected PI would be used, the manner in which the data principal can withdraw consent and exercise his or her right to grievance redressal, and the manner in which a data principal may make a complaint to the Data Protection Board of India.

**Law stated - 13 June 2024**

### Exemptions from transparency obligations

When is notice not required?

There are no exemptions to the notice requirements under the Privacy Rules. However, compliance with the Privacy Rules is not mandatory.

Under the DPDPA, a notice is required to be provided only where PI is processed based on consent or where PI is given voluntarily without any indication that consent is not granted. A notice is not required to be provided where PI is processed for the 'legitimate uses' listed above.

**Law stated - 13 June 2024**

## Data accuracy

### Does the law impose standards in relation to the quality, currency and accuracy of PI?

India's current data privacy laws do not impose any mandatory standards in relation to the quality, currency and accuracy of PI.

Under the DPDPA, a data fiduciary is obligated to ensure the completeness, accuracy and consistency of PI, where such PI is used to make a decision that affects the data principal or is disclosed to another data fiduciary.

**Law stated - 13 June 2024**

## Data minimisation

### Does the law restrict the types or volume of PI that may be collected?

Indian data protection laws, including the DPDPA, do not specifically restrict the types or volume of PI that may be collected.

However, under the DPDPA, where PI is processed based on consent, such consent is deemed to be limited to the PI necessary for fulfilling the purposes specified in the privacy notice.

**Law stated - 13 June 2024**

## Data retention

### Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Under the Privacy Rules, unless retention is required under any other law, an entity processing SPDI can only retain such PI until the time the purpose of collection is fulfilled. However, as stated, compliance with the Privacy Rules is not mandatory.

The data retention requirements under the DPDPA apply only when PI is processed based on consent or where PI is voluntarily provided for processing for a specified purpose without any indication that consent is not provided. In such cases, unless there is a data retention obligation under any other applicable law, data fiduciaries are obligated to delete PI once consent is withdrawn or if the purpose for which it is collected is served. The DPDPA deems

the purpose of collection to be served if the data principal does not approach the data fiduciary for performance of the purpose for which the data was collected, and for exercise of any of the data principal's rights in relation to such processing for a period to be specified by the government.

**Law stated - 13 June 2024**

### Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The Privacy Rules stipulate that SPDI must be used only for the purposes for which it was collected. However, as stated, compliance with the Privacy Rules is not mandatory.

The DPDPA does not include restrictions on the purposes for which PI can be used. However, where processing is based on the consent of the data principal, the purposes of processing must be made known to the data principal via a privacy notice, specific consent must be obtained for each purpose of processing listed in the privacy notice and the PI can be used only for those specified purposes.

**Law stated - 13 June 2024**

### Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There are no restrictions under India's current data privacy laws on the use of PI for making automated decisions without human intervention that affect individuals, including profiling.

Under the DPDPA, a data fiduciary is obligated to ensure the completeness, accuracy and consistency of PI used to make a decision that affects the data principal. Further, unless exempted by the government, data fiduciaries are prohibited from undertaking tracking or behavioural monitoring of children, or targeted advertising directed at children. A child is defined under the law as a person aged less than 18 years. However, there is no prohibition on processing PI through automated decisions without human intervention.

**Law stated - 13 June 2024**

## SECURITY

### Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Under India's current data privacy laws, an entity processing Sensitive Personal Data or Information is obligated to implement Reasonable Security Practices and Procedures to protect such data.

Likewise, under the Digital Personal Data Protection Act 2023 (DPDPA) a data fiduciary is obligated to implement reasonable security safeguards to prevent any breach of PI processed by it. Additionally, a data fiduciary is also obligated to implement appropriate organisational and technical measures to ensure compliance with the DPDPA. There are, however, no security obligations on data processors under the DPDPA, and the law obligates a data fiduciary to implement security safeguards to protect PI processed by its data processors.

India's current data privacy laws do not require performance of risk assessments. Under the DPDPA, a subset of data fiduciaries termed Significant Data Fiduciaries (SDFs) are obligated to undertake periodic data protection impact assessments and periodic data audits. SDFs are data fiduciaries or a class of data fiduciaries, a list of which will be notified by the government based on factors such as the volume and sensitivity of PI they process, risks to the rights of data principals, impact on sovereignty, security or integrity of India or public order, and risk to electoral democracy.

**Law stated - 13 June 2024**

## Notification of data breach

### Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are no breach reporting requirements under India's current data privacy laws.

Breach reporting requirements under cybersecurity regulations

Under the cybersecurity regulations notified under the Information Technology Act, 2000, all service providers in India (including foreign entities servicing customers in India), are mandatorily required to report cyber security incidents to India's Computer Emergency Response Team (CERT) within six hours of noticing such incidents or being notified about such incidents. A cybersecurity incident is defined under the regulations as any real or suspected adverse event that results in unauthorised access, denial of service or disruption, unauthorised use of a computer system or changes in data without authorisation. The breach reporting obligations under the regulations apply to breaches of all data and not just PI. Under the FAQs to the regulations, the CERT has clarified that only those cybersecurity incidents that meet the following criteria need to be reported:

- cyber incidents and cybersecurity incidents of a severe nature, such as denial of service, intrusion or the spread of contaminants on any part of the public information infrastructure;
- data breaches or data leaks;
- large-scale incidents, such as intrusion into computer resources and websites; and

- cyber incidents that impact human safety.

Breach reporting requirements under the DPDPA

A PI breach is broadly defined under the DPDPA to mean any unauthorised processing or accidental disclosure, use, alteration, destruction or loss of access to PI that compromises its confidentiality, integrity or availability. The DPDPA requires all PI breaches to be reported to the affected data principal and the Data Protection Board of India and does not prescribe any impact thresholds or criteria for reporting PI breaches. The law also does not prescribe the timeline and the modalities for breach reporting and empowers the government to prescribe rules in this regard. The government has not yet notified the said rules.

Breach reporting requirements under sector-specific laws

In addition to the foregoing, there are breach notification requirements under various sector-specific regulations, such as those applicable to regulated entities operating in the banking, securities and insurance sectors. In general, under said sector-specific regulations, breach reporting must be made to the relevant sectoral regulator (the Reserve Bank of India or the Securities and Exchange Board of India or the Insurance Regulatory and Development Authority of India, or any other regulator as the case may be) within six hours of noticing or being notified about a cybersecurity incident.

**Law stated - 13 June 2024**

## INTERNAL CONTROLS

### Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

There are no accountability obligations under India's current data privacy laws.

There are also no such specific obligations under the Digital Personal Data Protection Act 2023 (DPDPA). However, the DPDPA obligates a data fiduciary to implement appropriate technical and organisational measures to ensure compliance with the law. The law does not specify any such measures.

**Law stated - 13 June 2024**

### Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

India's current data privacy laws do not require the appointment of a data protection officer.

The DPDPA obligates a Significant Data Fiduciary (SDF) to appoint a data protection officer. Such person shall be based in India, represent the SDF under the provisions of the DPDPA, be responsible to the SDF's board of directors or similar governing body, and be the point of contact for the SDF's grievance redressal mechanism for data principals. Except as stated above, the DPDPA does not prescribe any other criteria that a person must satisfy to act as a data protection officer. However, note that under the DPDPA, data fiduciaries other than SDFs are obligated to appoint a person who will, on behalf of data fiduciaries, address questions raised by data principals regarding the processing of their PI.

**Law stated - 13 June 2024**

## Record-keeping

### Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

No, there is no such mandatory requirement under India's current data privacy laws.

Under the DPDPA, data fiduciaries or data processors are not specifically obligated to maintain internal records relating to the PI they hold. However, a data fiduciary would potentially need to maintain such records to comply with at least some of their obligations under the DPDPA. For instance, where PI is processed based on consent or where a data principal voluntarily provides PI for processing for a specified purpose without any indication that consent is not granted, the data principal has a right to obtain from the data fiduciary a summary of their PI processed by such data fiduciary. Further, the DPDPA prescribes data storage restrictions for data fiduciaries, and obligates data fiduciaries to facilitate the exercise of data principals' rights to correct, complete, update and erase PI.

**Law stated - 13 June 2024**

## Risk assessment

### Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

India's current data privacy laws do not require carrying out risk assessment in relation to the use of PI.

Under the DPDPA, SDFs obligated to undertake periodic data protection impact assessments, which must be a process comprising a description of the rights of data principals, the purpose of processing of PI, assessment and management of risk to rights of data principals, and such other matters regarding such process as the government may prescribe. The DPDPA does not prescribe the circumstances in which such data protection impact assessments must be undertaken. SDFs are also obligated to undertake periodic data audits, and to appoint independent data auditors to carry out such audits.

**Law stated - 13 June 2024**

### Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

No, there are no specific obligations under Indian data privacy laws (including the DPDPA) in relation to how PI processing systems must be designed. However, on a related note, the DPDPA obligates a data fiduciary to implement reasonable security safeguards to prevent a PI breach, and appropriate technical and organisational measures to ensure compliance with the DPDPA.

**Law stated - 13 June 2024**

## REGISTRATION AND NOTIFICATION

### Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No, data fiduciaries or processors of PI are not obligated to register with any supervisory authority.

**Law stated - 13 June 2024**

### Other transparency duties

Are there any other public transparency duties?

There are no mandatory public transparency duties under India's current data privacy laws.

Under the Digital Personal Data Protection Act 2023, in addition to the privacy notice requirements, a data fiduciary is obligated to publish in a manner, to be prescribed by the government, the business contact information of a person who can answer on behalf of such data fiduciary questions raised by a data principal about the processing of his or her PI.

**Law stated - 13 June 2024**

## SHARING AND CROSS-BORDER TRANSFERS OF PI

### Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

India's current data privacy laws do not have any specific or mandatory obligations for sharing PI with entities that provide outsourced processing services.

Under the Digital Personal Data Protection Act 2023 (DPDPA), a data fiduciary is obligated to appoint or engage a data processor only under a valid contract. The DPDPA does not

prescribe any contractual obligations that must be imposed on the data processor. However, as stated, the data fiduciary is responsible for compliance with the DPDPA in relation to processing undertaken on its behalf by a data processor. It is hence recommended that data fiduciaries must obtain from their data processors appropriate representations and warranties backed by specific indemnities to protect them from loss or liability in case of their data processors' non-compliance with the DPDPA.

Further, in case the entity providing outsourced processing services constitutes a data fiduciary under the DPDPA, the data fiduciary sharing the PI is obligated to ensure the completeness, accuracy and consistency of such PI.

**Law stated - 13 June 2024**

## Restrictions on third-party disclosure

### Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under India's data privacy laws (including the DPDPA), there are no mandatory restrictions on sharing of PI with recipients that are not processors or service providers.

However, under the DPDPA, a data fiduciary is obligated to ensure the completeness, accuracy and consistency of PI, in case such PI is shared with another data fiduciary.

**Law stated - 13 June 2024**

## Cross-border transfer

### Is the transfer of PI outside the jurisdiction restricted?

No, there are no restrictions under Indian data privacy laws, including the DPDPA, on the transfer of PI outside India. However, under the DPDPA, the government is empowered to notify a blacklist of countries to which the transfer of PI would be restricted. Such a blacklist has not yet been notified.

**Law stated - 13 June 2024**

## Further transfer

### If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

As stated, except for the transfer of PI to blacklisted counties to be notified by the government under the DPDPA, there are no restrictions under Indian data privacy laws on the transfer of PI outside India.

**Law stated - 13 June 2024**

### Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no data localisation restrictions under Indian data privacy laws, including the DPDPA. However, as stated, the DPDPA empowers the government to notify a blacklist of countries to which the transfer of PI would be restricted.

Note also that there are data localisation restrictions for certain data sets, such as payment data, telecommunications customer information and insurance records, under sector-specific laws that apply to regulated entities operating in sectors such as banking, digital lending, insurance, securities and telecommunications.

**Law stated - 13 June 2024**

## RIGHTS OF INDIVIDUALS

### Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Information Technology (RSPP and SPDI) Rules 2011 (the Privacy Rules), individuals have a right to review the Sensitive Personal Data or Information (SPDI) provided to an entity. However, compliance with the Privacy Rules is not mandatory.

Under the Digital Personal Data Protection Act 2023 (DPDPA), where PI is processed based on consent or where data principals voluntarily provide their PI for processing for a specified purpose without any indication that consent is not granted, data principals have a right to obtain from the data fiduciary a summary of the PI processed by such data fiduciary and the processing activities undertaken, the identities of all data fiduciaries and data processors with whom such PI has been shared, and any other information related to such PI as may be prescribed by the government.

The abovementioned rights to obtain the identities of data fiduciaries and said other information to be prescribed by the government are not available where PI is shared by a data fiduciary with any other data fiduciary authorised under law to obtain such PI or where such sharing is for the prevention, investigation, prosecution, or punishment of offences or cyber incidents.

The DPDPA does not prescribe the manner in which the right to access can be exercised by individuals and empowers the government to do so. As of now, the government has not notified rules in this regard.

**Law stated - 13 June 2024**

### Other rights

### Do individuals have other substantive rights?

Under the Privacy Rules, individuals have a right to review the SPDI they have provided to an entity, and for the correction of inaccurate or deficient SPDI. However, as stated, compliance with the Privacy Rules is not mandatory. Additionally, under section 43A of the Information Technology Act, 2000, individuals have a right to receive compensation in the case that an entity is negligent in implementing Reasonable Security Practices and Procedures (RSPP) and where such negligence results in a lawful gain or lawful loss.

Under the DPDPA, where PI is processed based on consent or where PI is voluntarily provided for processing for a specified purpose without any indication that consent is not granted, individuals have rights to correction, completion, updating and erasure of PI, and the right to withdrawal of consent. Further, irrespective of whether PI is processed based on consent, individuals have a right to grievance redressal, and a right to nominate any other individual who can exercise their rights in case of their death or incapacity.

The DPDPA does not include rights to object to or opt out of any particular kind of disclosures or processing activities.

**Law stated - 13 June 2024**

## Compensation

### Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under India's current data privacy laws, individuals are entitled to compensation if an entity processing their SPDI is negligent in implementing RSPP to protect such SPDI, and where such negligence results in a wrongful gain or wrongful loss. Wrongful gain and wrongful loss are associated with fraudulent or dishonest conduct under penal laws. The law solely refers to payment of compensation in case of a breach of SPDI, and there is no case law to conclude what types of losses are covered or where injury to feelings is sufficient to award compensation.

Under the DPDPA, individuals are not entitled to monetary damages or compensation if they are affected by a breach of the law.

**Law stated - 13 June 2024**

## Enforcement

### Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Violation of rights under India's current data privacy laws can lead to an individual claiming for compensation through the judicial system.

The rights under the DPDPA can be enforced by the Data Protection Board of India or the judicial system or both.

**Law stated - 13 June 2024**

## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

### Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Other than those already described, Indian data privacy laws (including the Digital Personal Data Protection Act 2023) do not include any other derogations, exclusions or limitations.

**Law stated - 13 June 2024**

## SPECIFIC DATA PROCESSING

### Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

India's current data privacy laws do not regulate the use of cookies or equivalent technology.

The use of cookies is, however, technically covered under the Information Technology Act, 2000, wherein there is a requirement for gaining consent for extracting any 'data' or 'information' from a computer system or a computer network, from the owner or person in charge of such computer system or computer network. Where it is understood that the person or agency collecting the cookies also owns the computer, computer system or computer network (such as in some employment scenarios), such consent is not required.

Further, the Digital Personal Data Protection Act 2023 (DPDPA) would apply to the use of cookies or equivalent technology where such cookies or equivalent technology process PI.

**Law stated - 13 June 2024**

### Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Yes, the Telecom Commercial Communication Customer Preference Regulations 2018 govern the transmission of marketing calls and messages using telecommunication services. India does not have any specific law governing email marketing and marketing through social media.

**Law stated - 13 June 2024**

### Targeted advertising

Are there any rules on targeted online advertising?

Under India's current data privacy laws, there are no specific rules governing targeted online advertising.

However, under the DPDPA, unless exempted by the government, data fiduciaries are prohibited from undertaking tracking or behavioural monitoring of children, or targeted advertising directed at children. A child is defined under the law as a person aged less than 18 years. Further, data fiduciaries are obligated to ensure the completeness, accuracy and consistency of the PI used to make a decision that affects a data principal.

**Law stated - 13 June 2024**

## Sensitive personal information

### Are there any rules on the processing of 'sensitive' categories of personal information?

India's current data protection laws do not govern the processing of all PI and solely apply to the processing of Sensitive Personal Data or Information.

The DPDPA does not categorise PI based on sensitivity and does not include any rules for the processing of 'sensitive' categories of PI.

It is also relevant to note that India has sector-specific data protection laws that prescribe additional rules for processing certain specific types of data sets, such as payment data, insurance records, and telecommunications customer information, by regulated entities operating in various sectors, such as banking, payments, insurance, securities and telecommunications.

**Law stated - 13 June 2024**

## Profiling

### Are there any rules regarding individual profiling?

India's current data privacy laws do not regulate individual profiling.

Under the DPDPA, a data fiduciary is obligated to ensure the completeness, accuracy and consistency of PI used to make a decision that affects the data principal. Further, unless exempted by the government, data fiduciaries are prohibited from undertaking tracking or behavioural monitoring of children, or targeted advertising directed at children. A child is defined under the law as a person aged less than 18 years.

**Law stated - 13 June 2024**

## Cloud services

### Are there any rules or regulator guidance on the use of cloud computing services?

Under India's data privacy laws (including the DPDPA), there are no specific rules or regulatory guidance on the use of cloud computing services. There are, however, sector-specific rules that apply to outsourcing and availing of cloud computing services by government agencies, and regulated entities operating in sectors such as securities and banking.

**Law stated - 13 June 2024**

## UPDATE AND TRENDS

### Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

A key development of the past year was the enactment of the Digital Personal Data Protection Act 2023 (DPDPA). When the DPDPA was enacted in August last year, the government stated that it expected to implement the law within 10 months. The implementation of the law was, however, delayed due to India's federal elections in 2024. Nevertheless, it is expected that the rules implementing the DPDPA will be notified in summer 2024 and that the DPDPA will come into force by the end of 2024. Given that India presently has minimal data privacy laws and low privacy standards in general, it is also expected that the government will allow organisations a reasonable time frame to prepare for and start complying with the new law.

**Law stated - 13 June 2024**