Data Protection in India: Overview

by Supratim Chakraborty, Khaitan & Co LLP, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 12-Apr-2021 | India

A Q&A guide to data protection in India.

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

To compare answers across multiple jurisdictions in our Data Privacy Advisor Product, visit the Data Privacy Advisor Data Protection Country Q&A Tool. To compare answers across multiple jurisdictions available in our Global Guides product, visit the Global Guides Data Protection Country Q&A Tool.

Regulation

Legislation

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

Data Protection Law

There is no overarching national law in India that regulates the collection and use of personal data.

A proposed legislative data protection framework in India would significantly change the law. The Personal Data Protection Bill, 2019 was presented in the 2019-2020 winter session of the Parliament after the Cabinet approved the final text of the bill. A Joint Parliamentary Committee continued to review and revise the bill throughout 2020.

Other Relevant Laws

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) provides certain provisions relating to personal data privacy and protection in India. Certain rules such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) implement the IT Act and prescribe general information

security requirements. The IT Amendment Act aims to address issues that the original IT Act failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

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

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

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

- **The banking and financial services sector.** For example:
    - the Aadhaar (Targeted Delivery of Financial and Other Subsidiaries, Benefits, and Services) Act 2016 as amended by the Aadhaar and Other Laws (Amendment) Bill, 2019 permits financial institutions to use biometric information to verify individuals' identities when opening bank accounts; and
    - the Credit Information Companies (Regulation) Act, 2005 and other Indian banking laws require customer confidentiality and protection of customer data.
- **The insurance industry.** The Insurance Regulatory and Development Authority of India issues regulations and rules that require insurance companies to protect confidential information they receive from misuse. For more on some of these regulations, see Country Q&A, Data Localization Laws: India.
- **The telecommunications and online service provider sector.** These organizations must comply with the IT Amendment Act, as implemented by the Information Technology (Intermediaries guidelines) Rules 2011 (Intermediaries Rules), which were superseded by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (in Hindi) (IT Rules 2021), which were issued on February 25, 2021. Telecommunications providers must also comply with the Indian Telegraph Act. For more on the Intermediaries Rules, see Practice Note, Information Security Considerations (India): Telecommunications and Online Service Providers and Country Q&A, Email Marketing Compliance: India.

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

Scope of Legislation

2. To whom do the laws apply?

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

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

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

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

The implementing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) apply only to body corporates and individuals acting on a body corporate's behalf.

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

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

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

3. What personal data does the law regulate?

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

- **Personal information.** The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) define personal information as any information that relates to a natural person which, either directly or indirectly, in combination with other available or likely available information, may identify that person (Rule 2(i), Privacy Rules)).

- **Sensitive personal data or information (SPDI) processing.** The Privacy Rules define SPDI to mean personal information relating to a person's:
    - passwords;
    - financial information, including information relating to bank accounts, credit cards, debit cards, and other payment instrument details;
    - physical, physiological, and mental health condition;
    - sexual orientation;
    - medical records and history; and
    - biometric information.

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

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

4. What acts are regulated?

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

- Collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, and disclosing sensitive personal data or information (SPDI) (Sections 5 to 7, Privacy Rules).
- Security practices and procedures for handling SPDI (Section 8, Privacy Rules).
- Data subjects' rights to review and update SPDI and withdraw consent for SPDI processing (Sections 5(6) and 5(7), Privacy Rules).

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

- Obtaining the data subject's prior written consent for collection, disclosure, and transfer of SPDI.
- Ensuring the collection is necessary for or directly related to a lawful purpose.

- Disclosing SPDI to third parties only under limited circumstances.
- Retaining SPDI for only as long as necessary to fulfill the organization's purpose for collecting it.

The IT Act regulates personal information disclosures that:

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

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

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

5. What is the jurisdictional scope of the rules?

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

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

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

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (in Hindi) (IT Rules 2021) require significant social media intermediaries to:

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

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

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

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

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

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

Notification

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

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

For information on individual notification requirements, see Question 12.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

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

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

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

  (Rule 8, Privacy Rules; Section 43A, IT Act, as amended by IT Amendment Act.) For more on personal data security, see Question 15.
- **Purpose limitation.** Body corporates should collect SPDI only if it is essential and required for a lawful purpose connected with the body corporate's functions (Rule 5(2), Privacy Rules). The body corporate should use the information only for the purpose for which it was collected and should not retain it for a period longer than required (Rules 5(4) and 5(5), Privacy Rules).
- **Consent and notification.** Under the Privacy Rules, body corporates collecting SPDI from a data subject must obtain the subject's prior written consent (Rule 5(1), Privacy Rules). When collecting information from the data subject, the body corporate must also take reasonable steps to inform the data subject:
  - that the body corporate is collecting the information;
  - the collection's purpose;
  - the intended recipients; and
  - the name and address of the body corporate, or an entity or person acting on its behalf, that is collecting and retaining the information.

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

- either the transfer is necessary to perform a lawful contract with the data subject or the data subject has consented to the transfer.

(Rule 7, Privacy Rules.) For more on personal data transfers, see Question 17 and Question 20.

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

(Rule 6, Privacy Rules.)

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

The body corporate must publish the privacy policy prominently on its website and make it readily available to data subjects. (Rule 4, Privacy Rules.)

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

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

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

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

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

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

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

For more on:

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

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

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

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

- The disclosure is necessary to comply with a legal obligation.
- Applicable law requires the disclosure.
- The disclosure is to a government agency to either:
    - verify an individual's identity; or

- prevent, detect, investigate (including cyber incidents), prosecute, or punish offenses.

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

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

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

Special Rules

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

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

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

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

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

- **Implement reasonable security practices and procedures.** A body corporate must implement:
    - reasonable security practices, procedures, and standards to handle sensitive personal data or information (SPDI);

- a comprehensive documented information security program; and
- policies that contain managerial, technical, operational, and physical security control measures that are proportionate to the information assets it seeks to protect.

(Rule 8, Privacy Rules; Section 43A, IT Act, as amended by Section 22, IT Amendment Act.) For more on personal data security, see Question 15.

- **Collect and use SPDI for lawful purposes.** A body corporate should collect SPDI only if it is essential and required for a lawful purpose connected with the organization's functions (Rule 5(2), Privacy Rules). The body corporate should use the information only for the purpose for which it was collected and should not retain the information for a period longer than what is required (Rule 5(4), Privacy Rules).
- **Obtain consent from and provide notification to data subjects.** Under the Privacy Rules, a body corporate collecting SPDI from a data subject must obtain the subject's prior written consent (Rule 5(1), Privacy Rules). When collecting information from the data subject, the body corporate must also take reasonable steps to inform the data subject:
  - that the body corporate is collecting the information;
  - the collection's purpose;
  - the intended recipients; and
  - the name and address of the organizations collecting and retaining the information.

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

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

  (Rule 6, Privacy Rules.)

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

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

Rights of Individuals

12. What information rights do data subjects have?

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

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

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

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

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

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

(Rule 4, Privacy Rules.)

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

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

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

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

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

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

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

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

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

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

See Question 13.

Security Requirements

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

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

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

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

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

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

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

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

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

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

CERT-In has developed a system of incident reporting where organizations can report a cybersecurity incident to CERT-In and receive technical assistance from CERT-In. Further, the CERT-In Rules and a form specify the requirements for organization's cyber security incident reporting including:

- The time the incident occurred.
- Information regarding the affected systems or network.
- The symptoms observed.
- Relevant technical information.

(Rule 12(1)(a), CERT-In Rules; CERT-In Incident Reporting Form.)

The CERT-In Rules are incident specific and are not dependent on the nature of data that has been leaked or disclosed because of the incident.

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

Processing by Third Parties

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

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) require body corporates transferring sensitive personal data or information (SPDI) to ensure that third-party processors receiving the data provide an appropriate level of data protection, including the security requirements discussed in Question 15. A body corporate may transfer SPDI within India or to a different jurisdiction only if both:

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

(Rule 7, Privacy Rules.)

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

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

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

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

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and Privacy Rules do not impose liability or additional obligations separately for data processors.

Electronic Communications

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

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

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

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

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

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

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

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

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

International Transfer of Data

Transfer of Data Outside the Jurisdiction

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

SPDI Transfers

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

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

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

Personal Information Transfers

A person that discloses personal information in contravention of a lawful contract is subject to penalties (Section 72A, Information Technology Act 2000, as amended by Section 37, Information Technology (Amendment) Act 2008). A personal data transfer in breach of a contract could attract penalties under this provision. Otherwise, Indian law does not provide rules governing personal information transfers.

For more on personal data transfers, see Question 22.

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

The Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and the Information Technology (Reasonable Security Practices and Procedures and

Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) do not specifically require personal information to be stored within India.

However, certain sectoral laws require data localization. Specifically:

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

The Ministry of Electronics and Information Technology (MeitY) issued a draft Data Centre Policy 2020 to encourage the development of in-country data center parks. MeitY issued the draft policy in contemplation of future compliance with the data localization requirements in the proposed Personal Data Protection Bill, 2019, which require data center infrastructure within India.

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

Data Transfer Agreements

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

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

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

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

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

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

See Question 20 and Question 22.

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

Indian law does not regulate data transfer agreements (see Question 22).

Enforcement and Sanctions

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

India has no dedicated national regulator for data protection and data privacy. However, the Ministry of Electronics and Information Technology (MeitY) administers the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and promulgated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), and acts as an enforcement authority in certain cases.

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

Sectoral laws are enforced by the respective sectoral regulators.

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

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

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

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

Regulator Details

India does not have a national data protection regulator. However, the Ministry of Electronics and Information Technology (MeitY) administers the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and promulgated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules). Sectoral regulators also issue data protection related regulations and standards.

Contributor Profile

Supratim Chakraborty, Partner

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E supratim.chakraborty@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2008

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

END OF DOCUMENT