COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

India

DATA PROTECTION & CYBER SECURITY

Contributing firm

ANA Law Group

Anoop Narayanan

Founding Partner | anoop@anaassociates.com

Ms. Rashi Chandhoke

Associate |

This country-specific Q&A provides an overview of data protection & cyber security laws and regulations applicable in India.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

INDIA
DATA PROTECTION & CYBER SECURITY

1. Please provide an overview of the legal and regulatory framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws)?

Summary of key laws and the applicability

The right to privacy to all citizens is a part of the fundamental right to life and personal liberty under Articles 19 and 21 of the Constitution of India. The Supreme Court of India had recognized the right of privacy as a fundamental right in the landmark judgement of *Justice K S Puttaswamy (Retd) and Another* v. *Union of India and Others* (2017) 10 SCC 1.

The Information Technology Act, 2000 (the "IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Privacy Rules") govern personal and sensitive personal information in India.

The Privacy Rules are applicable to corporate entities, and sensitive personal data.

The Privacy Rules describe sensitive personal information as the information relating to password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information.

India does not currently have a comprehensive data privacy law. The Ministry of Electronics and Information Technology (MeitY) had formed the Justice BN Srikrishna Committee which had introduced the Draft Personal Data Protection Bill, 2019 (the "PDP Bill").

The PDP Bill aims to become a comprehensive data protection law in India.

The PDP Bill intends to be applicable to the government, companies incorporated in India, and foreign companies dealing with personal data of individuals in India.

The PDP Bill was introduced in Lok Sabha (the lower house of the Indian Parliament) on 11 December 2019, and was immediately referred to a Joint Parliamentary Committee for further discussion. The government had directed the Parliamentary Committee to submit its report to the Lok Sabha by February 2020. This deadline was extended until February 2021. However, the Parliamentary Committee has not as yet filed its report to the Lok Sabha.

Enforceability

The IT Act prescribes appointment of adjudicating officers in each State to adjudicate the matters wherein the claims of injury or damages do not exceed INR 50,000,000 (USD 670,439 approximately). The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 prescribe that a written complaint can be made to the adjudicating officer in a prescribed form based on the location of computer system or the computer network, along with the fee based on the damages claimed as compensation. Thereafter, the adjudicating officer issues a notice to the parties notifying the date and time for further proceedings. Based on the parties' evidence, the adjudicating officer may impose penalty or award for such compensation. An appeal can be filed before the Appellate Tribunal against the adjudicating officer's decision, and the second appeal can be filed before the High Court.

India does not have a data protection authority as yet.

The PDP Bill intends to establish the data protection authority (the "DPA"), and empowers DPA to appoint an adjudicating officer to impose penalties on the data fiduciary. The maximum penalty for violation under PDP Bill is prescribed as INR 150,000,000 (more than USD 2 million approximately) or 4% of the data fiduciary's total global turnover in the preceding financial year, whichever is higher. The PDP Bill also intends to

prescribe imprisonment of three (3) years or a maximum penalty of INR200,000 (USD 2,700 approximately) if any person knowingly re-identifies personal data which has been de-identified by a data fiduciary.

The PDP Bill proposes to establish an appellate tribunal to adjudicate the first appeals against the DPA's decision, and the second appeal can be filed before the Supreme Court of India.

Sector specific laws and regulators

- Telecom – The Unified Access Service License ensures data protection to telecom networks and third party operators. The telecom networks are regulated by the Telecom Regulatory Authority of India (TRAI), the Department of Telecoms (DoT), the Telecoms Disputes Settlement and Appellate Tribunal (TDSAT), the Group on Telecom and IT (GOTIT), the Wireless Planning Commission (WPC) and the Digital Communications Commission) (DCC).
- Security – The Securities and Exchange Board of India (SEBI) has issued several guidelines on cyber security and cyber resilience framework for stock brokers, stock exchange and depositories. In October 2020, SEBI has constituted a Market Data Advisory Committee to recommend data privacy and data access regulations applicable to market data.
- Health – The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 governs patient confidentiality, and the Digital Information Security in Healthcare Act, 2018 (DISHA) governs collection, storage, transmission and access of health data. The DISHA prescribes for the establishment of a National Digital Health Authority to enforce privacy and security measures for health data and to regulate storage and exchange of health records. In December 2020, the Ministry of Health and Family Welfare has issued the Health Data Management Policy for the protection of individuals'/data principal's personal digital health data privacy.
- Banking – The Reserve Bank of India (RBI) is the central banking authority in India. The RBI's Cyber Security Framework mandates banks to have a privacy policy. The RBI has the power to conduct audits and enquiries into banks' security frameworks and impose penalties on banks for non-compliance. The Cyber Security and Information Technology Examination (CSITE) Cell of the Department of Banking Supervision periodically reviews the implementation of the Cyber Security Framework by the banks. The RBI's internal ombudsman scheme for commercial banks with more than ten branches is a redressal forum and proposes setting up an online portal to investigate and address cybersecurity concerns and complaints. The RBI has also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways in March 2020 directing payment aggregators to implement data security standards (such as PCI-DSS, PA-DSS), incident reporting, cyber security audit and reports and framing IT policy.
- Insurance – The Insurance Regulatory and Development Authority of India (IRDAI) has issued several regulations which contain provisions relating to data protection. The IRDAI had issued the guidelines on Information and Cyber Security for Insurers in 2017 under the IRDAI Act, 1999 containing a comprehensive cyber security framework for the insurance sector to implement appropriate mechanism to mitigate cyber risks. The IRDAI has updated the guidelines in December 2020, and mandate the insurers to conduct assurance audit and security tests annually. The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, the IRDAI (Maintenance of Insurance Records) Regulations 2015, IRDAI (Health Insurance Regulations), 2016 and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, are some of the relevant regulations on data security.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

There are no registration or licensing requirements under the current Indian law. However, the PDP Bill prescribes that the data fiduciary (notified as a significant data fiduciary by the DPA) must register itself with the DPA.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII?

What other key definitions are set forth in the laws in your jurisdiction?

The Privacy Rules define "personal information" and "sensitive personal data or information" as follows:

- Personal information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- Sensitive personal data or information of a person means such personal information which consists of information relating to password, financial information such as bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information.

The PDP Bill intends to broaden the scope of "personal data" and "sensitive personal data". The definition of personal data under the PDP Bill additionally includes any data from which an inference can be drawn for the purpose of profiling, and the definition of sensitive personal data additionally includes genetic data, caste, tribe and religious or political belief or affiliation. The definitions of personal and sensitive personal data under the PDP Bill are as follows:

- Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.
- Sensitive personal data means such personal data, which may, reveal, be related to, or constitute financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe and religious or political belief or affiliation.

The PDP Bill also intends to define the following important terms:

- Data fiduciary – means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.
- Data processor – means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.
- Data principal – means the natural person to whom the personal data relates.

4. What are the principles related to, the general processing of personal data or PII?

The principles for processing sensitive personal data prescribed under the Privacy Rules are as follows:

- A body corporate which collects, receives, possess, stores, deals or handles the data, must provide a privacy policy for handling personal information including sensitive personal data, and ensure that the privacy policy is available for view by the information providers, who has provided the information under lawful contract.
- The privacy policy must contain clear and easily accessible statements of its practices and policies, purpose of collection and usage of such information, disclosure of information including sensitive personal data or information and reasonable security practices and procedures.
- The body corporate must obtain a written consent (through letter, fax or e-mail) from the information provider.
- The body corporate must collect sensitive personal data for a lawful purpose, and the collection of the sensitive personal data or information must be necessary for that purpose.
- The body corporate must ensure that the information provider has the knowledge of the fact that the information is being collected, the purpose of collection, the intended recipients of the information and the name and address of agency collecting and retaining the information.
- The body corporate must not retain the information longer than is required for the purpose.
- The body corporate must permit the information providers to review the information, to amend the incorrect information, and to ensure the accuracy of the information collected.
- The body corporate, prior to collection of information, must provide an option to the information provider to not to provide the

information sought to be collected.
- The information provider must have an option to withdraw its consent given earlier to the body corporate.
- The body corporate must designate a grievance officer to address discrepancies and grievances of the information provider. The body corporate must publish name and contact details of the grievance officer on its website.
- The body corporate must obtain prior permission from the information provider for disclosure of sensitive personal data. However, the sensitive personal data can be shared without prior consent in case any Government agency requests such data from the body corporate in writing for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.
- The body corporate must not publish the sensitive personal data.
- The body corporate can transfer sensitive personal data to any other body corporate or a person in India or located in other country, that ensures the same level of data protection that is adhered by the body corporate. The transfer of sensitive personal data is allowed only if it is necessary for performance of the lawful contract between the body corporate and the information provider.
- The body corporate must implement reasonable security practices an, technical, operational and physical security control measures. The IS/ISO/IEC 27001 on "Information Technology – Securityd procedures. The body corporate must have a comprehensive documented information security programme and information security policies that contain managerial Techniques – Information Security Management System – Requirements" is one of the standards prescribed under the Privacy Rules. A body corporate which is following other than IS/ISO/IEC codes of best practices for data protection, must get its codes of best practices duly approved and notified by the Central Government for effective implementation.

The PDP Bill proposes to apply the data processing principles to personal data as well. The data processing principles prescribed under the PDP Bill are as follows:

- Personal data must be processed for a lawful purpose.
- The data processor must process the personal data in a fair and reasonable manner and ensure privacy of the data principal.
- The personal data must be collected only to the extent that is necessary for the purposes of processing of such personal data.
- A data fiduciary must issue a notice to the data principal before or at the time of collecting the personal data. The notice must contain the purpose of collection of personal data, the nature and categories of personal data being collected, the identity and contact details of the data fiduciary, rights of the data principal, the basis for such processing, and the consequences of the failure to provide such personal data, the source of such collection, the individuals or entities with whom such personal data may be shared, information regarding any cross-border transfer of the personal data, the period for which the personal data shall be retained, the procedure for grievance and any other information as prescribed by the regulations.
- The data fiduciary must take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated.
- The data fiduciary must not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and must delete the personal data at the end of the processing.
- The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

The Privacy Rules mandate the body corporates to obtain a written consent (through letter, fax or e-mail) from the information provider prior to the collection of sensitive personal data. The Privacy Rules do not mandate consent for collection of personal data. Further, the Privacy Rules do not prescribe any consent form.

The PDP Bill mandates that consent must be obtained before collection of personal as well as sensitive personal data. The PDP Bill also does not prescribe any

consent form.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

The Privacy Rules and the PDP Bill do not prohibit collection of any category of personal data.

The requirements for processing the sensitive personal data are elaborated in our response to query no. 4.

7. How do the laws in your jurisdiction address children's personal data or PII?

The Privacy Rules do not specifically address children's personal data.

However, the PDP Bill intends to prescribe that the data fiduciary must verify a child's age and obtain the consent of the child's parent or guardian before processing of any personal data of a child (i.e., person below 18 years). Further, the data fiduciary must be prohibited from profiling, tracking or behaviorally monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

8. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The IT Act prescribes for exemption from liability of an intermediary in the following situations:

- The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
- The intermediary does not initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission; or
- The intermediary observes due diligence while discharging his duties under the IT Act.

Note: The IT Act defines an intermediary as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

The PDP Bill prescribes the following exemptions:

- The PDP Bill empowers the Central Government to exempt any government agency from the application of all or certain provisions of the PDP Bill.
- Provisions relating to collection, processing and transfer of personal data and rights of data principal will not apply in the following situations:
    i. In case the personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any contravention of any law;
    ii. In case the disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;
    iii. In case the processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function.
    iv. In case the personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or
    v. In case the processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organization.
- The Central Government is empowered to exempt processing of personal data of data principals outside India by any data processor incorporated under the Indian law, pursuant to any contract entered between the data principal and the data processor.
- The DPA is empowered to exempt the application of the provisions of the PDP Bill if the processing of personal data is necessary

for research, archiving, or statistical purposes.
- The PDP Bill exempts small entities from applications of certain provisions relating to the processing of personal data.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The IT Act or the Privacy Rules do not define the terms “data protection by design” or “data protection by default”. However, the Privacy Rules incorporate the following provisions (explained in detail in our response to query no. 4) which constitute privacy by design or privacy by default:

- Requirement of privacy policy;
- Collection of information for lawful purpose and with consent;
- Disclosure of information;
- Use of information for the purpose for which it was collected; and
- Retention of information only so long as that purpose gets fulfilled.

The PDP Bill mandates data fiduciaries to prepare a privacy by design containing the following:

- the managerial, organizational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
- the obligations of data fiduciaries;
- the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;
- the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;
- the protection of privacy throughout processing from the point of collection to deletion of personal data;
- the processing of personal data in a transparent manner; and
- the interest of the data principal is accounted for at every stage of processing of personal data.

Further, subject to the regulations which will be framed under the PDP Bill, the privacy by design policy may require certification from the DPA. The privacy by design policy certified by the DPA must be published on the website of the data fiduciary and the DPA.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Besides maintaining a privacy policy, data principal’s written consent and security practices and procedures (explained in our response to query no.4), the IT Act and the Privacy Rules do not require the personal data processors to maintain any internal records of their data processing activities.

However, the PDP Bill mandates significant data fiduciary to maintain accurate and up-to-date records of the following, in a prescribed form and manner:

- important operations in the data life-cycle including collection, transfers, and erasure of personal data;
- periodic review of security safeguards;
- data protection impact assessments; and
- any other aspect of processing as may be specified by regulations.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

The Indian Computer Emergency Response Team (CERT-In), established under the IT Act, is the national nodal agency for cybersecurity in India. The CERT-In Rules mandate the body corporates, service providers, intermediaries and data centres to report all cybersecurity incidents to CERT-In as early as possible. The format and procedure for reporting cybersecurity incidents are published on CERT-In’s website and are periodically updated. The RBI mandates reporting of cybersecurity breach incidents within 2 to 6 hours of incident.

The PDP Bill mandates every data fiduciary to inform the DPA about the breach of any personal data processed by the data fiduciary as soon as possible if such breach is likely to cause harm to any data principal.

12. Do the laws in your jurisdiction require or recommend conducting risk

assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The current Indian law does not prescribe any requirement to conduct risk assessments.

However, the PDP Bill mandates the "significant data fiduciary" (notified by the DPA) to undertake a data protection impact assessment before processing sensitive personal data in case it intends to involve new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals.

A data protection impact assessment must contain the following:

- detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;
- assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and
- measures for managing, minimising, mitigating or removing such risk of harm.

On completion of the data protection impact assessment, the data protection officer must review the assessment and submit the assessment to the DPA in the prescribed manner.

On the assessment's receipt and its review, in case the DPA has a reason to believe that such processing is likely to cause harm to the data principals, the DPA may either direct the data fiduciary to cease such processing or impose certain conditions on such processing as it deems fit.

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

The current Indian law does not prescribe for appointment of a data protection officer. However, the PDP Bill mandates every significant data fiduciary to appoint a data protection officer for carrying out the following functions:

- providing information and advice to the data fiduciary on matters relating to fulfilling its prescribed obligations;
- monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of the PDP Bill;
- providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review;
- providing advice to the data fiduciary on the development of internal mechanisms to satisfy the transparency principles prescribed under the PDP Bill;
- providing assistance to and co-operating with the DPA on matters of compliance of the data fiduciary with the provisions of the PDP Bill;
- act as the point of contact for the data principal for the purpose of grievances redressal; and
- maintaining an inventory of records to be maintained by the data fiduciary.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).

The Privacy Rules mandate that while collecting information, the body corporates must ensure that the information provider has the knowledge of the following:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information; and
- the name and address of the agency that is collecting the information, and the agency that will retain the information.

The Privacy Rules do not prescribe any format for notice.

The PDP Bill mandates data fiduciary to give notice to the data principal at the time of collection of personal data, containing the following information:

- the purposes for which the personal data is to be processed;
- the nature and categories of personal data being collected;
- the identity and contact details of the data fiduciary and the contact details of the data

protection officer, if applicable;
- the right of the data principal to withdraw the consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
- the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds under the PDP Bill;
- the source of such collection, if the personal data is not collected from the data principal;
- the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;
- information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
- the period for which the personal data shall be retained or where such period is not known, the criteria for determining such period;
- the existence of and procedure for the exercise of rights of data principal and any related contact details for the same;
- the procedure for grievance redressal;
- the existence of a right to file complaints to the DPA;
- where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary; and
- any other information as may be specified by the regulations.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The current Indian law does not distinguish between the data controllers/data fiduciaries and the data processors.

The PDP Bill defines the terms “data fiduciary” and “data processors” (as explained in our response to query no. 3). The data processors must be appointed by the data fiduciary under a contract, and the data processor must only process the personal data based on data fiduciary’s instructions and treat it confidential. The data fiduciaries and data processors are both responsible for undertaking the transparency measures and security safeguards for processing personal data, and for reporting personal data breach under the PDP Bill.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

The current Indian law does not prescribe the appointment of data processors. However, the PDP Bill mandates the appointment of data processor by a contract, and prescribes that the appointed data processor must not engage, appoint, use or involve another data processor for data processing on its behalf, except with the authorization of the data fiduciary and unless permitted in the contract. Further, the data processor must only process personal data based on data fiduciary’s instructions and treat it confidential.

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

The current Indian law does not address restrictions on or define the terms “monitoring”, “profiling”, “tracking technologies” or “cookies”. However, the PDP Bill defines the term “profiling” as any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal. The PDP Bill prohibits profiling, tracking or behaviourally monitoring, or targeting advertising directly at, children and undertaking any other processing of personal data that could cause significant harm to the child.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

The Telecom Commercial Communication Customer Preference Regulations, 2010 (TCCCPR) was issued by the TRAI under the TRAI Act, 1997 to address unregulated and endless telemarketing communications to customers.

The TCCCPR defines “commercial communication” as any voice call or message using telecommunication services, where the primary purpose is to inform about or advertise or solicit business for goods or services, a supplier or prospective supplier of offered goods or services, a business or investment opportunity, or a provider or prospective provider of such an opportunity.

The TCCCPR defines “promotional messages” as commercial communication message for which the sender has not taken any explicit consent from the intended recipient to send such messages.

The TCCCPR defines “unsolicited commercial communication (UCC)” as any commercial communication that is neither as per the consent nor as per registered preference(s) of recipient.

Any transactional/service message or transactional/service voice call transmitted on the directions of the Central/State Government or bodies established under the Indian Constitution and any message or voice calls transmitted by or on the direction of the TRAI or by its authorised agency does not constitute UCC in case such communication is in public interest.

A TCCCPR prescribes that a subscriber, who is not registered with any access provider for the purpose of sending commercial communications under the TCCCPR, cannot make UCC. Any subscriber sending commercial communication, telecom resources of the sender may be put under usage cap (i.e., a maximum of 20 outgoing voice calls per day and maximum 20 messages per day). Every access provider must ensure that no commercial communication is made to any recipient, except as per the preference(s) or digitally registered consent(s) in accordance with TCCCPR.

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The current Indian law does not have any provisions on privacy concerns relating to biometrics. The definition of “sensitive personal data” under the Privacy Rules includes biometric data, and the principles in the Privacy Rules (as elaborated in our response to query no. 4) applies to biometric data.

However, the PDP Bill defines “biometric data” as facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person.

The definition of “sensitive personal data” under the PDP Bill also includes biometric data. The PDP Bill requires the significant data fiduciary to undertake data protection impact assessment in case it involves processing of biometric data. The PDP Bill also prescribes that processing of certain biometric data (as may be notified by the Central Government) must be prohibited unless such it is permitted by law.

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form a regulator?)

The current Indian law does not prohibit the transfer of personal information outside India.

The Privacy Rules permit transfer of sensitive personal data outside India subject to the following restrictions:

- the recipient entity ensures adherence to the same level of data protection and that the transfer is necessary to comply with a lawful contract; or
- the data provider has given prior consent.

The PDP Bill permits transfer of sensitive personal data outside India on the following conditions:

- explicit consent is given by the data principal for such transfer; and
- the transfer is made pursuant to a contract or intra-group scheme approved by the DPA; or
- the Central Government, after consultation with the DPA, has allowed the cross-border transfer of sensitive personal data based on the fact that such sensitive personal data will be subject to an adequate level of protection and such transfer will not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction; or
- the DPA has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

The PDP Bill prescribes that “critical personal data” must be only processed in India.

The term "critical personal data" means such personal data as may be notified by the Central Government under the PDP Bill.

However, the critical personal data can be transferred outside India on the following conditions:

- the transfer is made to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action; or
- where the Central Government has deemed such transfer to be permissible and such transfer does not prejudicially affect the security and strategic interest of the State.

Any transfer of critical personal data must be notified to the DPA.

21. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The Privacy Rules prescribe that body corporates must implement reasonable security practices and procedures. The body corporates must have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures.

The IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one of the standards prescribed under the Privacy Rules. A body corporate which is following other than IS/ISO/IEC codes of best practices for data protection, must get its codes of best practices duly approved and notified by the Central Government for effective implementation.

The PDP Bill mandates data fiduciaries and data processors to implement necessary security safeguards including use of methods such as de-identification and encryption, steps necessary to protect the integrity of personal data and steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

The data fiduciaries and data processors must undertake a review of its security safeguards periodically in a prescribed manner and take appropriate measures accordingly.

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The CERT-In Rules defines "cyber security breach" as unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource.

The CERT-In Rules also define "cybersecurity incident" as any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, and information without authorization.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

- Banking Sector – The RBI's CSITE Cell periodically assess the implementation of cybersecurity framework by the banks and impose penalties on banks for non-compliance. The RBI's internal ombudsman scheme for commercial banks with more than ten branches is a redressal forum and has proposed to set up an online portal to investigate and address cybersecurity concerns and complaints. The RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways in March 2020 directs payment aggregators to implement data security standards (such as PCI-DSS, PA-DSS), incident reporting, cyber security audit and reports and framing IT policy.
- Insurance Sector – The IRDAI's guidelines on Information and Cyber Security for Insurers mandate the insurers to conduct assurance audit and security tests annually. The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, the IRDAI (Maintenance of Insurance Records) Regulations 2015, IRDAI (Health Insurance Regulations), 2016 and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, are some of the relevant regulations on data security.
- Telecom Sector – The Unified Access Service License regulates information security to telecom networks and third party operators.
- Security – SEBI has issued guidelines on cyber security and cyber resilience framework for

stock brokers, stock exchange and depositories.
- Health – The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 governs patient confidentiality, and the DISHA governs collection, storage, transmission and access of health data. The DISHA prescribes for the establishment of a National Digital Health Authority to enforce privacy and security measures for health data and to regulate storage and exchange of health records.

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

The current Indian law does not contain any statutory provision to notify the affected individuals or entities. However, the CERT-In Rules mandate the body corporates, data centres, service providers and intermediaries to report all cyber security incidents to CERT-In as soon as possible in a prescribed format. The RBI mandates banks to report cyber breach incidents within 2 or 6 hours of the incident.

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The Indian law does not define the term “cyber crime”. However, the IT Act and the Indian Penal Code, 1860 prescribe punishments for offences such as cyber terrorism, identity theft, cheating by using computer resource, publishing or transmitting obscene material, etc.

The term “cybercrime” is defined by the National Cyber Crime Reporting Portal, a government portal set up recently for reporting cybercrime, as any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime. Child pornography, cyber bullying, cyber stalking, cyber grooming, online job fraud, online sextortion, vishing, sexting, smshing, sim swap scam, debit/credit card fraud, impersonation and identity theft, phishing, spamming, ransomware, virus, worms and trojans, data breach, denial of services/distributed DOS, website defacement, cyber-squatting, pharming, crypto jacking, online drug trafficking and espionage constitute cybercrime. The Indian law does not prescribe any requirements such as payment of ransoms in ransomware attacks.

26. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

CERT-In is the national nodal agency for cybersecurity, to carry out the following functions:

- collection, analysis and dissemination of information on cyber-incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber-incidents response activities;
- issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and
- such other functions relating to cybersecurity as may be prescribed.

The CERT-In is responsible for responding to cybersecurity incidents and assist in implementing measures to reduce the risk of cybersecurity incidents. The CERT-IN has powers to issue directions to service providers, intermediaries, data centres, body corporates, etc., for enhancing cybersecurity infrastructure in India. The CERT-IN is also responsible to operate an incident response help desk on a 24-hour basis on all days including government and other public holidays to facilitate reporting of cyber-authority incidents.

As regards critical information, the National Critical Information Infrastructure Protection Centre (NCIIPC) is set up under the IT Act as the nodal agency to ensure a safe, secure and resilient information infrastructure for critical sectors in India.

27. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant

details.

The Privacy Rules prescribe right to the information provider to review, edit and update their personal data, and to withdraw their consent to personal data.

Whereas, the PDP Bill provides the following rights to the data principals:

- Right to confirmation and access – the data principal must have the right to obtain from the data fiduciary confirmation whether the data fiduciary is processing or has processed personal data of the data principal, the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof, and a brief summary of processing activities undertaken by the data fiduciary with respect to the data principal's personal data. The data principal must have the right to access in one place the identities of the data fiduciaries with whom the personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.
- Right to correction and erasure – the data principal must have the right to correct inaccurate or misleading personal data, to complete the personal data, to update the personal data, and to delete the personal data which is no longer necessary for the purpose for which it was processed. In case the data fiduciary does not agree with such correction, completion, updation or erasure of personal data for the purposes of processing, the data fiduciary must provide the data principal with adequate justification in writing for rejecting the data principal's request. If the data principal is not satisfied with the data fiduciary's justification, the data principal may require the data fiduciary to take reasonable steps to indicate the relevant entities that the same is disputed by the data principal.
- Right to data portability – the data principal must have the right to receive the following personal data in a structured, commonly used and machine-readable format:
    i. the personal data provided to the data fiduciary;
    ii. the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or
    iii. the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained

  The data principal must have the right to have the personal data transferred to any other data fiduciary. The right to data portability is not applicable in the following situations:

  i. the processing is necessary for functions of the State or in compliance of law or order of a court; and
  ii. the data portability would reveal a trade secret of any data fiduciary or would not be technically feasible.

- Right to be forgotten – the data principal must have the right to restrict or prevent the continuing disclosure of the personal data by a data fiduciary in the following situations:
    i. the disclosure has served the purpose for which it was collected or is no longer necessary for the purpose; and
    ii. the disclosure was made with the consent of the data principal and such consent has since been withdrawn; or was made contrary to the provisions of PDP Bill or any other law for the time being in force.

  The right to be forgotten may be

enforced only by the adjudicating officer's order based on an application filed by the data principal, in a prescribed manner.

28. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The IT Act prescribes appointment of an adjudicating officer in each State to conduct an inquiry for injury or damages for claims valued up to INR 50,000,000 (USD 670,439 approximately). The claims exceeding this amount must be filed before the competent civil court. The appeals from the adjudicating officer can be filed before the Appellate Tribunal and the second appeal can be filed before the High Court. India does not have a DPA as yet.

The PDP Bill prescribes that the data principal can exercise its rights (except the right to forgotten, which is enforced only on an order of the adjudicating officer, as explained in our response to the query no. 27), in the following manner:

- The data principal must make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to the identity, and the data fiduciary must acknowledge the receipt of such request within such period as may be specified by the PDP regulations.
- The data fiduciary must comply with the data principal's request and communicate it to the data principal, within such period as may be specified by PDP regulations.
- In case the data fiduciary refuse any request made by the data principal, it must provide the data principal the reasons in writing for such refusal and must inform the data principal regarding the right to file a complaint with the DPA against the refusal, within such period and in such manner as may be specified by PDP regulations. The data fiduciary is not obliged to comply with any request made by the data principal if such compliance will harm the rights of any other data principal.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

As the right to privacy in India is considered as a fundamental right under the Indian Constitution, the right to privacy can be enforced by filing writ petition in the competent High Court. The affected party can also claim monetary damages under the IT Act.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

The individuals are entitled to monetary damages on the personal data breach. The IT Act prescribes appointment of an adjudicating officer to conduct an inquiry for injury or damages for claims valued up to INR 50,000,000 (USD 670,439 approximately). The claims exceeding this amount must be filed before the competent civil court. The appeals from the adjudicating officer can be filed before the Appellate Tribunal and the second appeal can be filed before the High Court.

31. How are the laws governing privacy and data protection enforced?

The IT Act prescribes appointment of an adjudicating officer in each State to conduct an inquiry for injury or damages for claims valued up to INR 50,000,000 (USD 670,439 approximately). The claims exceeding this amount must be filed before the competent civil court. The appeals from the adjudicating officer can be filed before the Appellate Tribunal and the second appeal can be filed before the High Court. India does not have a DPA as yet.

32. What is the range of fines and penalties for violation of these laws?

The IT Act prescribes different penalties for different data breaches. Some of them are as follows:

- If a body corporate fails to protect sensitive personal data and is negligent in implementing reasonable security practices and procedures, such body corporate will be liable to pay damages by way of compensation to the person affected.
- The contravention of any rules or regulations under the IT Act for which no penalty is provided, will be liable to pay compensation of a maximum INR 25,000 (USD 340

approximately) to the affected person.
- Punishment for violation of privacy includes imprisonment up to 3 years or with fine no exceeding INR 200,000 (USD 2,700 approximately).

The PDP Bill prescribes a maximum penalty of INR150,000,000 (approximately USD2 million) or 4% of the data fiduciary's total global turnover in the preceding financial year, whichever is higher, for violation of PDP Bill. The PDP Bill also prescribes imprisonment of up to 3 years and/or a penalty of up to INR200,000 (approximately USD2,800) against any person who knowingly or intentionally, and without the consent of the data fiduciary, re-identify personal data which has been de-identified by a data fiduciary/data processor, or re-identify and process such personal data.

33. Can personal data or PII owners/controller appeal to the courts against orders of the regulators?

The IT Act prescribes an appeal can be filed before the Appellate Tribunal against the adjudicating officer's order. The second appeal can be filed before the High Court.

Contributors

Anoop Narayanan
Founding Partner

anoop@anaassociates.com

Ms. Rashi Chandhoke
Associate