COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

India

DATA PROTECTION & CYBERSECURITY

Contributor

ANA Law Group

Anoop Narayanan

Founding Partner | anoop@anaassociates.com

Priyanka Gupta

Senior Attorney | priyanka@anaassociates.com

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

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

INDIA
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity 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).

The Constitution of India guarantees the right to privacy to all citizens as part of the right to life and personal liberty under Articles 19 and 21, and as part of the freedoms guaranteed by Part III of the Constitution. This right was also upheld by the Supreme Court of India (SCI) in 2017 in its landmark judgment of Justice K S Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1 (the Privacy Judgment).

India does not currently have a comprehensive data privacy law. Personal and confidential information is protected under the Information Technology Act 2000 (ITA) and the IT Rules. India's central (federal) government has ratified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (DP Rules) under the ITA, to govern entities that collect and process sensitive personal information in India.

The DP Rules apply only to corporate entities and are restricted to sensitive personal data (SPD), which includes attributes such as sexual orientation, medical records and history, biometric information and passwords.

Pursuant to the Privacy Judgment, the Indian Ministry of Electronics and Information Technology (MeitY) had formed the Justice B N Srikrishna Committee (expert committee), to frame an all-encompassing data protection law in India. Consequently, the draft Personal Data Protection Bill 2019 was introduced. Thereafter, in December 2021, the Joint Parliamentary Committee (JPC) presented a revised version of the 2019 Bill, the Data Protection Bill, 2021 in the Parliament. The revised bill expanded the scope of the law to cover non-personal data, and introduced stringent data breach reporting requirements (within 72 hours), data localization requirements, regulation of hardware manufacturers and enabling a certification mechanism for all digital and IoT devices to mitigate data breaches, etc.

Finally, in November 2022, MeitY had introduced a further revised draft bill, Digital Personal Data Protection Bill, 2022 (the "DPDP Bill"), which adopts a more simplified approach to handling "personal data" in comparison to the previous versions. The DPDP Bill covers several key principles pertaining to lawful usage of personal data, limitation on collection of personal data, data minimisation, data storage and accountability of the person processing personal data. The DPDP Bill is applicable only to the processing of "digital personal data". Both non-personal data, and data in non-digital formats are excluded. Under the DPDP Bill, the role of the regulator is a reduced one, focused only on enforcement and adjudication.

India now awaits a robust data protection regime with the approval of the DPDP Bill.

Cybersecurity

India does not currently have a comprehensive cybersecurity law. Cybersecurity, data breach notification and incident response are governed under the ITA. The ITA defines "cybersecurity" as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction".

Under the ITA, the Indian government has established the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency for cybersecurity, to carry out functions including 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, and

issue of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the "CERT-In Rules") prescribe that CERT-In will be responsible for responding to cybersecurity incidents and will assist cyber-users in the country in implementing measures to reduce the risk of cybersecurity incidents. CERT-In also has powers to issue directions to service providers, intermediaries, data centres, body corporates, etc, for enhancing cybersecurity infrastructure in the country.

Earlier, the service providers, intermediaries, data centres and body corporates handling sensitive personal data (SPD) had to mandatorily report all cybersecurity incidents to CERT-In "as early as possible". In April 2022, the CERT-In issued a new directive modifying obligations under the 2013 Cert-In Rules, including requirements to report cybersecurity incidents within six hours, syncing system clocks to the time provided by government servers, maintaining security logs in India, and storing additional customer information. CERT-In has also set up sectoral CERTs to implement cybersecurity measures at a sectoral level. The details regarding the methods and formats for reporting cybersecurity accidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cybersecurity are published on CERT-In's website and are updated from time to time.

For critical sectors, the government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) under the ITA, as the nodal agency, and has framed the NCIIPC Rules and guidelines to protect the nation's critical information infrastructure (CII) from unauthorised access, modification, use, disclosure and disruption to ensure a safe, secure and resilient information infrastructure for critical sectors in the country.

Other relevant rules framed under the IT Act include the following.

- The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, which prescribe security measures for protected systems, as defined under the IT Act. Under the IT Act, the government may notify any computer resource that affects the facility of CII to be a "protected system".
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 require intermediaries to implement reasonable security practices and procedures to secure their computer resources and information, maintaining safe harbour protections. Intermediaries are also mandated to report cybersecurity incidents to CERT-In.

Other laws that contain cybersecurity-related provisions include the Indian Penal Code 1860, which deals in criminal offences, including those committed in cyberspace, and the Companies Act 2013, which requires the companies to implement security systems to ensure that electronic records are secured from unauthorised access.

The ITA prescribes that any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for by CERT-In or comply with CERT-In's direction will be punishable with imprisonment for a term which may extend to one year or a fine which may extend to INR100,000 or both.

The ITA also prescribes deterrence in terms of compensations, penalties and punishments for offences such as damage to computer system, failure to protect data, computer-related offences, theft of computer resource or device, SPD leak, identity theft, cheating by impersonation, violation of privacy, cyberterrorism, online pornography (including child pornography), breach of confidentiality and privacy, and breach of contract.

Regulators

In addition to the MeitY and NCIIPC, the government has established the National Security Council Secretariat (NSCS) as the central co-ordinating body for cybersecurity and internet governance. NSCS has developed a draft cybersecurity strategy to address the issue of security of national cyberspace, but currently there is no implementation date for this strategy.

The Ministry of Home Affairs has set up the Cyber and Information Security Division (C&IS) to deal with matters relating to cybersecurity, cybercrime, the National Information Security Policy & Guidelines (NISPG) and its implementation. C&IS comprises of a cybercrime wing, cybersecurity wing, information security wing, and a monitoring unit.

Further, the Home Ministry has established the Indian Cybercrime Co-ordination Centre (I4C) which is a nodal point in the fight against cybercrime and co-ordinates implementation of mutual legal assistance treaties (MLAT) with other countries.

The government has also set up the National Technical Research Organisation (NTRO) as a technical intelligence agency under the National Security Advisor in the Prime Minister's office. Its primary role is to develop technology capabilities in aviation and remote sensing, data gathering and processing, cybersecurity, strategic hardware and strategic monitoring. NCIIPC comes within NTRO's ambit.

The ITA mandates the central government to appoint an adjudicating officer to conduct inquiries, and adjudicate matters (ie, contravention of any of the provisions of the ITA or of any rule, regulation, direction or order made thereunder, including non-compliance of CERT-In's direction), with claims for injury or damages valued up to INR50 million. Claims that exceed this amount must be filed before the competent civil court. Where more than one adjudicating officer is appointed, the ITA mandates the central government to specify the matters and places of jurisdiction of each adjudicating officer.

The first appeal from the adjudicating officer's decisions can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court.

The DPDP Bill prescribes filing the complaint before the data protection officer, which can be appealed before the adjudicating officer of the DPB, who will have the authority to impose penalties on the data fiduciary. The maximum penalty for violation of the DPDP Bill's provisions by an individual is INR5 billion (USD60 million approx.), if the non-compliance is regarded as significant by the DPB. The DPDP Bill also prescribes specific penalties of INR500 million to INR2.5 billion (USD6 million to 30 million approx.) for failure to take reasonable security safeguards to prevent personal data breach; failure to notify the Board and affected data principals of data breaches; and non-compliance with additional obligations. The aforesaid offences under DPDP Bill are cognisable (ie, the police have the power to arrest the offender without a court warrant) and non-bailable.

The DPDP Bill proposes that the central government establish an appellate tribunal to adjudicate on appeals from the orders of the DPA, and the SCI as the final appellate authority for all purposes under the DPDP Bill.

Sector-specific regulators

Banking sector

The Reserve Bank of India (RBI) governs both public and private sector banks. The RBI's guidelines prescribe that the RBI can request an inspection any time of any of the banks' cyber-resilience. The RBI has set up a Cyber Security and Information Technology Examination (CSITE) cell under the Department of Banking Supervision, to periodically assess the progress made by banks in the implementation of the cybersecurity framework (CSF), and other regulatory instructions and advisories through on-site examinations and off-site submissions. The RBI has an internal ombudsman scheme for commercial banks with more than ten branches as a redressal forum, and has also issued guidelines on information security, electronic banking, technology risk management and cyber frauds. CERT-In and the RBI jointly carry out a cybersecurity awareness campaign on "Beware and be aware of financial frauds" through the Digital India Platform.

RBI also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways, directing the payment aggregators to put in place adequate information and data security infrastructure and systems for prevention and detection of frauds, and has specifically recommended implementation of data security standards and best practices such as PCI-DSS, PA-DSS, the latest encryption standards and transport channel security. Payment aggregators must establish a mechanism for monitoring, handling and follow-up of cybersecurity incidents and breaches, and mandatorily report incidents to RBI and CERT-In.

RBI regularly conducts audits and enquiries into the banks' security frameworks, and imposes penalties on the banks for non-compliance of RBI's cybersecurity framework for banks. RBI has also formulated an integrated scheme, The Reserve Bank – Integrated Ombudsman Scheme, 2021 (the "RB-IOS, 2021") to simplify the grievance redress process at RBI by enabling the customers of all regulated entities to register their complaints at one centralised reference point. Through this portal RBI also spreads cyber-crime awareness including frauds using mobile apps/UPI/QR codes, etc.

With regard to data leaks, the RBI's guidelines restrict payment aggregators and merchants from storing card and card-related data, and all such data previously stored to be deleted.

The RBI has provided tokenisation of card data as a solution to comply with the card storage restrictions. The RBI has widened the existing limited device-based tokenisation framework to all devices and also permitted card-on-file tokenisation.

The RBI has also issued a first-of-its-kind framework to enable digital payments with poor or no internet connectivity in offline mode.

Recently, in April 2023, the RBI had issued the Master

Direction on Outsourcing of Information Technology Services ("Outsourcing Directions") to bring IT service providers under additional level of compliance, audit and oversight, data storage norms and cyber security incident reporting.

Insurance sector

The Insurance Regulatory and Development Authority (IRDA) is the nodal agency for governance and regulation of the insurance sector in India. The IRDA conducts regular on-site and off-site inspections of insurers to ensure compliance with the legal and regulatory framework. The IRDA also has guidelines on Information and Cyber Security for Insurers (IRDA Cyber Security Policy), requiring vulnerability assessment and penetration testing annually and closing any identified gaps within a month. Some other relevant guidelines issued by IRDA are: IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017; IRDAI (Maintenance of Insurance Records) Regulations, 2015; and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, which contain a number of provisions and regulations on data security. Additionally, IRDAI has recently issued guidelines to insurers on structuring cyber-insurance for individuals and identifying gaps that need to be filled. As per the guidelines, cyber-insurance should provide cover against theft of funds and identity, unauthorised online transactions, email spoofing, etc.

Telecom sector

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).

TRAI has released its recommendations on cloud services in relation to creation of a regulatory framework for cloud services, and constituting an industry-led body of all cloud service providers (CSP).

DoT regularly conducts cybersecurity workshops and cyber drills for better awareness.

Securities

The Securities Exchange Board of India (SEBI) has issued detailed guidelines to market infrastructure institutions (MIIs) to set up their respective Cyber Security Operation Centre (C-SOC) and to oversee their operations through dedicated security analysts. The cyber-resilience framework also extends to stockbrokers and depository participants.

Recently, in February 2023, SEBI has issued guidelines based on Financial Computer Security Incident Response Team's (CSIRT-Fin) recommendations to enhance the cybersecurity and data privacy measures for the financial institutions and to curb the increasing cybersecurity threat to the securities market.

Health sector

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.

The Ministry of Health and Family Welfare had approved a Health Data Management Policy (the "HDM Policy") largely based on the DPDP Bill to govern data in the National Digital Health Ecosystem. The HDM Policy recognises entities such as data fiduciaries and data processors similar to the DPDP Bill, and establishes a consent-based data-sharing framework.

Other Regulators

There are CERTs established under the Ministry of Power to mitigate cybersecurity threats in power systems, and four sub-CERTs for transmission, thermal, hydro and distribution to co-ordinate with power utilities. The amended Intermediaries Guidelines of 2022 under the ITA impose various obligations on the intermediaries including reporting cyber incidents to the CERT-In.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

India may see its first comprehensive, general data protection law introduced this year through notification of the DPDP Bill.

The Indian government is working towards updating its National Cybersecurity Strategy in order to improve its position in cyberspace. The updated National Cybersecurity Policy may be issued this year.

The validity of the Cert-In Directions has been challenged by several entities across Indian courts alleging that certain provisions of the Cert-In Directions are ultra vires. Reportedly, one of the provisions challenged includes collection of details like name, IP address, address, contact information, and the purpose of using VPN and keeping it for five years even after the user's relationship with the VPN service provider has ended. Although the Cert-In Directions are currently in force, the court's approach on the pending cases will be noteworthy.

The government will soon be releasing the draft e-commerce policy that proposes to set up an e-commerce regulator with broad powers over e-commerce entities and platforms. The draft policy contains proposals on sharing source codes, algorithms and other data with the government, use of non-personal data of consumers, anti-piracy, cross-border data transfers, etc. This is an important development and it will be interesting to monitor the final policy in view of the provisions under the pending DPDP Bill, and, thereafter, the policy's feasibility and enforceability.

3. 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 is no registration or licensing requirement 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.

4. 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 DP 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 DPDP Bill only includes the definition of "personal data", which means any data about an individual who is identifiable by or in relation to such data.

Additionally, the DPDP Bill also defines

- Personal Data Breach – means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
- Data Fiduciary – means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- Data Processor – means any person who processes personal data on behalf of a Data Fiduciary.

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The principles for processing sensitive personal data prescribed under the DP 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 and procedures. The body corporate 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.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

The DP 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 SPD. The DP Rules do not mandate consent for collection of personal data. Further, the DP Rules do not prescribe any consent form.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The DP Rules provide that the body corporate must obtain a written consent (through letter, fax or e-mail) from the information provider, and 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.

Besides the foregoing, there is no prescribed format or content for the consent. The consent can be incorporated into a broader document or bundled with other matters.

8. 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 or disclosure?

The DP Rules 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 and 5.

9. How do the laws in your jurisdiction address children's personal data?

Current Indian data privacy law does not address privacy issues specifically relating to children. Under India's contract law, a contract executed by a minor (below 18 years) is invalid, and parental or legal guardian consent must be obtained for all online contracts.

However, the DPDP Bill has introduced additional obligations for processing of children's personal data, such as obtaining prior verifiable parental consent, not undertake processing that is likely to cause harm to a child, and not undertaking tracking or behavioural monitoring of children or targeted advertising directed at children.

10. How do the laws in your jurisdiction address health data?

Health data is protected as SPD under the DP Rules.

Besides this, 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 2020, the Ministry of Health and Family Welfare had issued the Health Data Management Policy (HDM Policy) for the protection of individuals'/data principal's personal digital health data privacy. The HDM Policy is largely based on the DPDP Bill to govern data in the National Digital Health Ecosystem, and also recognises entities such as data fiduciaries and data processors similar to the DPDP Bill, and establishes a consent-based data-sharing framework.

11. Do the laws include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The ITA 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 ITA.

Note: The ITA 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.

12. 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 concepts of "privacy by design" and "privacy by default" are not defined under current Indian data protection law. However, these concepts are reflected in the ITA and the DP Rules, as they incorporate provisions such as:

- provision of a privacy policy and disclosure of information;
- collection of information for lawful purposes with a data provider's consent;
- use of information for the purpose for which it was collected; and

- retention of information only so long as that purpose gets fulfilled.

Further, the telecom regulator, TRAI recommends that privacy by design along with data minimisation should apply to all entities in the digital ecosystem.

Under the DPDP Bill, the central government has proposed to establish the Data Protection Board of India. The allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions of the Board shall be digital by design.

13. Are owners/controllers 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 providing a privacy policy, data principal's written consent and security practices and procedures (explained in our response to query no.5), the ITA and the DP Rules do not require the personal data processors to maintain any internal records of their data processing activities.

However, CERT-In new directives require all service providers, intermediaries, data centres, body corporate, virtual private server (VPS) providers, cloud service providers, VPN service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations to maintain security logs in India and store certain additional customer information as prescribed under the directive.

14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The DP Rules provide that the body corporate must not retain the information longer than is required for the purpose for which it was collected. No specific duration has been specified.

MeitY notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 replacing the Information Technology (Intermediaries guidelines) Rules, 2011. The new intermediary rules provide an obligation for internet intermediaries to retain users' information collected upon registration for 180 days even after any cancellation or withdrawal of such registration.

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

The CERT-In Rules mandate the body corporates, service providers, intermediaries and data centres to report all cybersecurity incidents to CERT-In within six hours, and also provide a point of contact. The format and procedure for reporting cybersecurity incidents are published on CERT-In's website and are periodically updated.

Besides the foregoing, there is no statutory requirement under the current Indian law.

16. 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 DP Rules do not prescribe conducting internal risk assessments, vulnerability scanning, penetration tests, etc. The RBI mandates banks to have periodical vulnerability assessment and penetration testing exercises for all critical systems. The IRDA also has a cybersecurity policy that recognises the need for testing programmes, vulnerability assessments and penetration tests. For instance, in October 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' security concerns, which aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement strong and robust business continuity.

Further, the DPDP Bill requires the significant fiduciaries to undertake measures including data protection impact assessment and periodic audit. The "Data Protection Impact Assessment" is defined as a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed. Unlike the previous versions, this proposed law does not provide any details on how to carry out the assessment, which would be notified by the government

in due course.

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

The DP Rules do not prescribe for appointment of a data protection officer. However, they provide for the appointment of a grievance officer to redress the information provider's grievances.

Further, the NCIIPC guidelines recommend that all CIIs have an information security department headed by a CISO. The RBI's Cyber Security Guidelines mandate the appointment of a chief information security officer (CISO), along with a security steering committee in public/private sector banks, who must report any incident directly to the bank's head of risk management. The IRDA also requires the appointment of a CISO for implementing a cybersecurity framework. Cert-In's new directives require the service providers, intermediaries, data centres, corporate bodies and government organisations to designate a "Point of Contact" to interface with CERT-In.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There is no such statutory requirement.

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

The DP Rules mandate that while collecting personal 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 DP Rules do not prescribe any format for notice.

20. 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? (For example, 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.

21. 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 any provisions governing the appointment of data processors.

22. Please describe any restrictions on monitoring, automated decision-making 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 specify any restrictions on or define the terms "monitoring", "profiling", "tracking technologies" or "cookies".

The proposed law, DPDP Bill defines "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 DPDP Bill provides that its provisions shall also apply to processing of digital personal data outside India, if such processing is in connection with any profiling of, or activity of offering goods or services to data principals within India.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

There is no specific provision under the DP Rules. However, the proposed DPDP Bill prohibits tracking or behavioural monitoring of children or targeted advertising directed at children by the data fiduciaries.

Further, 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. TCCCPR restricts sending of unsolicited commercial communication to any subscriber, who is not registered with any access provider.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or related terms defined, and what restrictions are imposed, if any?

There is no such statutory provision to address sale of personal data.

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

TCCCPR address unregulated and endless telemarketing communications to customers in India.

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.

26. 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?

There are no specific provisions under Indian data privacy or sectoral laws to address the privacy concerns arising from facial recognition technology. Some of the large amount of emotional and factual data collected from facial recognition technology can be regarded as SPD.

Biometric data is categorised as SPD under the DP Rules, and its collection, processing and transfer is subject to the prescribed statutory restrictions.

India's central government enacted the Aadhaar Act for the targeted delivery of financial benefits and subsidies to the underprivileged. The Aadhaar Act establishes an authority, the UIDAI, responsible for the administration of the Aadhaar Act. It also establishes a Central Identities Data Repository (CIDR), which is a database holding Aadhaar numbers and corresponding demographic and biometric information. Aadhaar is currently the largest database of biometrics globally.

27. 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 a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from 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.

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

The DP 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.

Further, companies must ensure that electronic records and security systems are protected against unauthorised access and tampering, in accordance with the Companies

(Management and Administration) Rules 2014, which was created under the Companies Act,

2013. In case of any information security breach, such corporations are required to show to the authorities that the prescribed security control measures had been implemented. Any lapse on the part of such bodies corporate shall attract charges under Section 43A of the IT Act and they will be required to compensate all those affected as a result of such breach.

India's Whistle Blowers Protection Act, 2011 (the "Whistle Blower Act") establishes a mechanism to receive complaints relating to allegations of corruption or wilful misuse of power against any public servant, and to provide adequate safeguards against the victimisation of a whistle-blower. However, a major shortfall is that a whistle-blower must disclose their identity in the complaint.

Further, the Companies Act, 2013, mandates that certain publicly listed companies establish a vigil mechanism and an exclusive hotline for directors and employees to report their genuine concerns about unethical behaviour or misconduct, actual or suspended frauds, and violations of the code of conduct.

Additionally, SEBI's Listing Agreement's Clause 49 under the Principles of Corporate Governance requires that companies establish a whistle-blower policy to safeguard the identity of an employee who reports instances to the management.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define "security breach"?

The CERT-In Rules define a cyber-incident as "any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality integrity, or availability, of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative impact on the national economy, or diminishes the security posture of the nation".

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 authorisation".

A cybersecurity breach is also defined under the CERT-In Rules 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".

Cybersecurity incidents prescribed under the CERT-In Rules must be reported, including:

- targeted scanning/probing of critical networks/system;
- compromise of critical systems/information;
- unauthorised access of IT systems/data;
- defacement of a website or intrusion into a website and unauthorised changes, such as inserting malicious code, links to external websites, etc;
- malicious code attacks, such as the spreading of viruses, worms, Trojans, botnets and spyware;
- attacks on servers, such as databases, email and DNS and network devices, such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) and distributed denial of service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications, such as e-governance, e-commerce.

The data to be provided while incident reporting includes the sector details, location of the system, date and time of the occurrence, criticality, affected system/network, symptoms observed, and the relevant technical information such as type of incident, number of hosts affected, security systems deployed and actions to mitigate the damage.

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

The relevant laws in India that govern network monitoring and cybersecurity defensive measures are:

- the ITA;
- the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the "Interception Rules");
- the DP Rules;
- the CERT-In Rules and the new directives issued thereunder in April 2022;
- the NCIIPC Rules; and
- the Sectoral Cyber Security Framework Policies.

The ITA provides a legal framework to address hacking and security breaches of IT infrastructure and prescribes penalties for negligently handling SPD. Furthermore, to the extent that the data intercepted and monitored by a body corporate includes the SPD of its customers or employees, the body corporate must comply with the DP Rules.

The Interception Rules prescribe that no person shall carry out any interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, unless authorised by India's central or state governments. There is a lack of clarity on whether a company's interception and monitoring of its internal servers will conflict with the above restriction.

The sectoral cybersecurity policies for banks, insurance companies, telecom companies and CII permit body corporates, including banks, to monitor the secure status of each system and network, mobile and home-working procedures, and critical systems. These may include third-party providers. The UASL obliges telecom companies to monitor all intrusions, attacks and fraudulent activity on its technical facilities and report to the DoT.

Key legislations that address data protection in the finance sector include the Credit Information Companies (Regulation) Act 2005 (CIC Act), the Credit Information Companies Regulations 2006 (CIC Regulations) and circulars issued by the RBI.

The CIC Act and CIC Regulations primarily apply to credit information companies; recognise them as data collectors; require that they ensure data security and secrecy; and require that they adhere to privacy principles in respect of data collection, use, disclosure, accuracy and protection against loss or unauthorised use, access and disclosure.

The RBI's guidelines on data localisation of payment system data in India will also, to an extent, help protect financial data.

Data protection laws in respect to health data are inadequate in India. The Health Ministry has proposed the DISH Act to ensure electronic health data privacy, security and standardisation in the healthcare sector. The DISH Act is pending government approval and is expected to be notified soon.

Although there are multiple telecoms laws, data protection norms in the telecoms sector are primarily governed by the UASL issued to telecoms service providers (TSPs) by the DoT. A TSP has an obligation to take necessary steps to safeguard the privacy and

confidentiality of users' information. Furthermore, customer information can be disclosed only after obtaining the individual's consent and if the disclosure is in accordance with the terms of such consent.

Artificial intelligence (AI) is not dealt with under the current data privacy regime. However, reliance on AI is increasing significantly among organisations wishing to secure their networks and their data.

MEITY has constituted four committees for promoting AI initiatives and developing a policy framework. The committees have submitted their first reports on platforms and data on AI; leveraging AI for identifying national missions in key sectors; mapping technological capabilities; key policy enablers required across sectors; and on cybersecurity, safety, legal and ethical issues.

31. 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?

There is no statutory provision mandating the sharing of cybersecurity information with the government, although the breach must be reported to Cert-In.

Incidents specified under the CERT-In Rules must be reported to CERT-In within six hours in the prescribed format. Data breaches in certain specific sectors such as finance, insurance and securities must be reported to the respective regulators. Cybersecurity incidents must be reported to the CISO.

There is no statutory requirement to report a cybersecurity incident to other companies or organisations. Contractually, a body corporate may require the vendor or service provider to promptly report any incident to the company.

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

Currently, there are no regulations restricting payment of ransomware. However, legal experts have been advising companies against making payments for ransomware, as the remittance is likely to trigger implications under the foreign exchange and money laundering laws.

33. 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, NCIIPC is set up under the ITA as the nodal agency to ensure a safe, secure and resilient information infrastructure for critical sectors in India.

34. 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.

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

Individual data privacy rights are exercisable and enforced through the judicial system in India, as there is no central data privacy authority.

36. 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 ITA.

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

The individuals are entitled to monetary damages on the personal data breach. The ITA prescribes appointment of an adjudicating officer to conduct an inquiry for injury or damages for claims valued up to INR 50,000,000 (USD 600,000 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.

38. How are data protection, privacy and cybersecurity laws enforced?

The ITA 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 600,000 approximately). The claims exceeding this amount must be filed before the competent civil court. A written complaint can be made to the adjudicating officer based on the location of the computer system or the computer network, together with a fee based on the damages claimed as compensation. The adjudicating officer thereafter issues a notice to the parties notifying the date and time for further proceedings and, based on the parties' evidence, decides whether to pass orders (if the respondent pleads guilty) or to carry out an investigation. If the officer is convinced that the scope of the case extends to the offence instead of contravention, and entails punishment greater than a mere financial penalty, the officer will transfer the case to the magistrate having jurisdiction.

The first appeal from the adjudicating officer's decisions can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court. India does not have a DPA as yet.

The DPDP Bill prescribes filing the complaint before the data protection officer, which can be appealed before the adjudicating officer of the DPB, who will have the authority to impose penalties on the data fiduciary.

The DPDP Bill proposes that the central government establish an appellate tribunal to adjudicate on appeals from the orders of the DPA, and the SCI as the final appellate authority for all purposes under the DPDP Bill.

As regards cybersecurity, the Indian government has established the CERT-In under the ITA as the national nodal agency for cybersecurity. CERT-In has also set up sectoral CERTs to implement cybersecurity measures at a sectoral level. The details regarding the methods and formats for reporting cybersecurity accidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cybersecurity are published on CERT-In's website and are updated from time to time.

For critical sectors, the government has set up the NCIIPC under the ITA, as the nodal agency,

In addition to ITA, cybersecurity-related provisions are included in the Indian Penal Code 1860, which deals in criminal offences, including those committed in cyberspace, and the Companies Act 2013, which requires the companies to implement security systems to ensure that electronic records are secured from unauthorised access.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

The ITA prescribes that any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for by CERT-In or comply with CERT-In's direction will be punishable with imprisonment for a term which may extend to one year or a fine which may extend to INR100,000 or both.

The ITA also prescribes deterrence in terms of compensations, penalties and punishments for offences

such as damage to computer system, failure to protect data, computer-related offences, theft of computer resource or device, SPD leak, identity theft, cheating by impersonation, violation of privacy, cyberterrorism, online pornography (including child pornography), breach of confidentiality and privacy, and breach of contract.

The proposed DPDP Bill prescribes the maximum penalty for violation of its provisions by an individual as INR5 billion (USD60 million approx.), if the non-compliance is regarded as significant by the DPB. The DPDP Bill also prescribes specific penalties of INR500 million to INR2.5 billion (USD6 million to 30 million approx.) for failure to take reasonable security safeguards to prevent personal data breach; failure to notify the Board and affected data principals of data breaches; and non-compliance with additional obligations. The aforesaid offences under DPDP Bill are cognisable (ie, the police have the power to arrest the offender without a court warrant) and non-bailable.

40. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

There are no rules or guidelines published regarding calculation of fines or thresholds for the imposition of sanctions.

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

Yes, the first appeal from the adjudicating officer's decisions can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court.

The DPDP Bill prescribes filing the complaint before the data protection officer, which can be appealed before the adjudicating officer of the DPB, who will have the authority to impose penalties on the data fiduciary.

The DPDP Bill proposes that the central government establish an appellate tribunal to adjudicate on appeals from the orders of the DPA, and the SCI as the final appellate authority for all purposes under the DPDP Bill.

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

There are no applicable legal standards. Instances of cybersecurity breach are adjudicated on a case-by-case basis.

India saw a rising trend of writ petitions being filed across various High Courts seeking the right to be forgotten and right to erasure. In December 2022, the Kerala High Court disposed of a series of writ petitions filed by various petitioners. A mother and daughter had filed a petition to remove the daughter's name and details from an Indian legal database and also Google's search engine. The daughter was wrongfully detained when she was a medical student, and later released based on the habeas corpus petition. Similarly, some petitioners who were allegedly involved in criminal activities and were later bailed or were acquitted had sought removal of their names and details from the online records. The court had observed that a claim for the protection of personal information based on the right to privacy cannot co-exist in an open court justice system. Further, the court observed that it was for the Legislature to fix grounds for the invocation of such a right, and the Court is entitled only in appropriate cases to invoke principles related to the right to erasure to allow a party to erase and delete personal data available online.

In all the petitions where the petitioners were involved in any kind of criminal activities, although granted bail or acquitted at a later state, the court had refused removal of such cases from the public domain or redaction of names and details from the legal database or Google search engines. However, in the petitions that involved family matters including matrimony, divorce, custody of child, etc, the court had allowed the right of privacy and had directed removal of the aggrieved persons' details from online records.

SC passed a significant judgment in October 2021 in the Pegasus spyware issue, recognising the need to assess the impact of the Pegasus spyware on the right to privacy and freedom of speech. The court formed a three-member committee to make recommendations on enactment or amendment of the existing surveillance laws to ensure an improved right to privacy and cybersecurity and threat assessment measures.

The committee has not as yet submitted its recommendations.

In a landmark case involving collection and transfer of citizens' personal data for COVID-19 tracking purposes by the government of Kerala (a southern Indian state) to a US-based data analysis company, the Kerala High Court had restricted the government from sharing citizens' sensitive personal data, unless the data was anonymised. The court had also recognised the

importance of the data subject's informed consent prior to collecting their personal data and the safeguards to ensure confidentiality of the data collected.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

India may see its first comprehensive, general data protection law introduced this year through notification of the DPDP Bill.

The Indian government is working towards updating its National Cybersecurity Strategy in order to improve its position in cyberspace. The updated National Cybersecurity Policy may be issued this year.

The validity of the Cert-In Directions has been challenged by several entities across Indian courts alleging that certain provisions of the Cert-In Directions are ultra vires. Reportedly, one of the provisions challenged includes collection of details like name, IP address, address, contact information, and the purpose of using VPN and keeping it for five years even after the user's relationship with the VPN service provider has ended. Although the Cert-In Directions are currently in force, the court's approach on the pending cases will be noteworthy.

The government will soon be releasing the draft e-commerce policy that proposes to set up an e-commerce regulator with broad powers over e-commerce entities and platforms. The draft policy contains proposals on sharing source codes, algorithms and other data with the government, use of non-personal data of consumers, anti-piracy, cross-border data transfers, etc. This is an important development and it will be interesting to monitor the final policy in view of the provisions under the pending DPDP Bill, and, thereafter, the policy's feasibility and enforceability.

Contributors

Anoop Narayanan
Founding Partner
anoop@anaassociates.com

Priyanka Gupta
Senior Attorney
priyanka@anaassociates.com