DATA PROTECTION LAWS OF THE WORLD

India

INDIA

Last modified 5 January 2023

LAW

At present, the Information Technology Act, 2000 (the Act) and rules notified thereunder largely govern data protection in India.

On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in *Justice K.S.Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2019 (the PDP Bill). However, the PDP Bill was withdrawn in August 2022 considering a long list of recommendations for changes tabled by a Joint Parliamentary Committee that provided its report in December 2021. In its place, on November 18, 2022, the Ministry of Electronics and Information Technology (MeitY), Government of India, released a draft of the Digital Personal Data Protection Bill, 2022 (the DPDP Bill).[1]

The enactment of the PDP Bill will overhaul the personal data protection and regulatory regime in India. Until such time, the Act and rules provided therein govern data privacy in India. MeitY had invited comments on DPDP Bill till December 17, 2022. After this, the government may make changes to the current draft. The DPDP Bill is expected to be tabled before the Parliament and come into effect in early 2023.

India's IT Ministry, MeitY, adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), notified under the Act. The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal information, including sensitive personal information, to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider / organization providing services relating to the collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

As stated above, India is in the process of overhauling its personal data protection regime. While the PDP Bill and the report on non-personal data governance framework, which was released by a committee appointed by the Central Government to make recommendations on the regulation of non-personal data, had introduced provisions on protection of non-personal data, the DPDP Bill does not regulate non-personal data. Considering this, collection and handling of non-personal data is currently unregulated.

1: This Bill was published by MeitY on November 18, 2022, and people were permitted to comment on the same before December 17, 2022. The Bill has been drafted on the following principals:

a. Usage of personal data by organisation must be done in a manner that is lawful, fair to the individuals concerned and transparent to individuals;
b. Usage of personal data should be limited to the purpose for which it was collected;
c. Data minimisation should be followed where only those items of personal data required for attaining a specific purpose must be collected;
d. Accuracy of personal data whereby reasonable efforts should be made to ensure that the personal data of the individual is accurate and kept up to date;
e. Storage limitation whereby personal data should not be stored perpetually by default. Storage should be limited to such duration as is necessary for the stated purpose for which personal data was collected;
f. Reasonable safeguards are to be undertaken to ensure that there is no unauthorised collection or processing of personal data. This is intended to prevent personal data breach; and
g. The person who decides the purpose and means of processing of personal data should be accountable for such processing.

DEFINITIONS

Definition of personal data

The Privacy Rules define "personal information" as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Definition of sensitive personal data

The Privacy Rules define "sensitive personal data or information" to include the following information relating to:

- Passwords
- Financial information e.g. bank account / credit or debit card or other payment instrument details
- Physical, physiological and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information
- Any detail relating to the above clauses as provided to a corporate entity for providing services
- Any of the information received under the above clauses for storing or processing under lawful contract or otherwise

Biometrics means the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirement.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of the request or grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are there any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed.

COLLECTION & PROCESSING

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf that collects sensitive personal information must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 Press Note issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) that collects, receives, possess, stores, deals or handles information shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information, including sensitive personal information, and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

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

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required and should also ensure that the sensitive personal information is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (i.e. he / she will be able to withdraw his or her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

TRANSFER

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or to any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required by the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offense for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions:

- Entitling the data collector to distinguish between 'personal information' and 'sensitive personal information' that it wishes to collect / process; and

- Representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and outlining the liability of the third party.

Data Localization

India's central bank, the Reserve Bank of India (RBI) has made it mandatory from October 15, 2018, for all payment system providers and their service providers, intermediaries, third party vendors and other entities in the payment ecosystem to ensure that all data relating to payment systems operated by them are stored in a system only in India. Interestingly, by virtue of this regulation, RBI is seeking storage of all payment system data, which includes the entire payment processing cycle from request to final payout, such as customer data (name, mobile number, Aadhaar number, PAN number, etc.), payment sensitive data (customer and beneficiary account details), payment credentials (OTP, PIN, passwords, etc.), and transaction data (originating and destination information, transaction reference, timestamp, amount, etc.). However, for cross border transactions which consist of a foreign and domestic component, data pertaining to the foreign leg may be stored outside India. While data pertaining to the domestic leg should be stored in India, a copy may be stored abroad.

Separately, the Insurance Regulatory and Department Authority of India (Maintenance of Insurance Records) Regulations, 2015, require insurance providers to store data related to policies and claim records of insurers on systems in India (even if this data is held in an electronic form).

Additionally, while Section 128 of the Companies Act, 2013, requires every company prepare and store, at its registered office, books of account, other relevant books and papers and financial statements for every financial years, on August 5, 2022, the Ministry of Corporate Affairs amended this rule whereby all such relevant books and papers maintained in an electronic mode should remain accessible in India, at all times.

Further, the Ministry of Electronics and Information Technology's directions on information security practices, procedure, prevention, response and reporting of cyber incidents dated April 28, 2022 (in force since June 28, 2022), in particular the frequently asked questions released on these directions, require service providers offering services to users in the country to enable and maintain logs and records of financial transactions within India.

SECURITY

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement 'reasonable security practices and procedures' to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the federal government. Presently, no such codes of best practices have been approved by the federal government.

BREACH NOTIFICATION

The government of India has established and authorized the Indian Computer Emergency Response Team ("Cert-In") to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules") impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain cybersecurity incidents.

Cybersecurity incidents have been defined to mean any real or suspected adverse events, in relation to cybersecurity, that violate any explicitly or implicitly applicable security policy, resulting in:

- Unauthorized access, denial or disruption of service;
- Unauthorized use of a computer resource for processing or storage of information; and
- Changes to data or information without authorization.

Under the Directions, the occurrence of the following types of cybersecurity incidents are to be reported:

- Targeted scanning / probing of critical networks / systems;
- Compromise of critical systems / information;
- Unauthorized access of IT systems / data;
- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.;
- Malicious code attacks such as spreading virus / worm / trojan / bots / spyware / ransomware / cryptominers;
- Attack on servers such as databased, Mail and DNS and network devices such as routers;
- Identity theft, spoofing and phishing attacks;
- Denial of service and distributed denial of service attacks;
- Attacks on critical infrastructure, SCADA and operation technology systems and wireless networks;
- Attacks on applications such as e-governance, e-commerce, etc.;
- Data breach;
- Data leak;
- Attacks on internet of things devices and associated systems, networks, software and servers;
- Attacks or incident affects digital payment systems;
- Attacks through malicious mobile applications;
- Fake mobile applications;
- Unauthorized access to social media accounts;
- Attacks or malicious / suspicious activities affecting cloud computing systems / servers / software / applications;
- Attacks or malicious / suspicious activities affecting systems / servers / networks / software / applications related to Big Data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drones;
- Attacks or malicious / suspicious activities affecting systems / servers / software / applications related to artificial intelligence and machine learning.

These incidents can be reported to CERT-In, (i) via email (incident@cert-in.org.in), (ii) phone (1800-11-4949), or (iii) fax (1800-11-6969). The methods and formats of reporting are also available at www.cert-in.org.in and will be updated from time to time.

The compliance obligations under the Directions extend to all entities which have computer systems, networks and / or resources in India, irrespective of whether the entity is incorporated in or outside India.

ENFORCEMENT

Civil penalties of up to approximately €570,341.28 (as at December 21, 2022) for failure to protect data including sensitive

personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to three years of imprisonment or a fine up to approximately €5,704.34 (as at December 21, 2022), or both for unlawful disclosure of information.

Separately, the Directions have introduced penalty of a term of imprisonment extendable to 1 year or a fine up to approximately €1140.68 (as at December 21, 2022), or both, for failure to provide information to CERT-In or non-compliance with the Directions.

ELECTRONIC MARKETING

The Act does not refer to electronic marketing directly. Dishonestly receiving data, computer database or software is an offense. However, in a related development, the Food Safety and Standards Authority of India (FSSAI) has made it mandatory for E-commerce FBOs (Food Business Operators) to obtain a license from the Central Licensing Authority. E-commerce FBO means any Food Business Operator carrying out any of the activities in section 3(n) of Food Safety & Standards Act, 2006, through the medium of e-commerce. Interestingly, section 3(n) covers the entire food chain as it defines "food business" as any undertaking, whether for-profit or not, and whether public or private, carrying out any of the activities related to any stage of manufacture, processing, packaging, storage, transportation, distribution of food, import and includes food services, catering services, sale of food or food ingredients. Similarly, another set of legal Rules being referred as "E-commerce & the Legal Metrology (Packaged Commodities) Amendment Rules, 2017," effective from January 1, 2018, has made it mandatory for an e-commerce entity to ensure mandatory declarations about the commodity displayed on the digital and electronic network used for e-commerce transactions.

The consumer protection regime in India was recently overhauled by way of enactment of the Consumer Protection Act, 2019 (notified in July 2020) (CPA 2019). Under CPA 2019, sellers and service providers have the obligation to, among others, not engage in unfair trade practices including by way of misleading advertisements. Further, Consumer Protection (E-Commerce) Rules, 2020 (E-Commerce Rules) have been notified under the CPA to regulate e-commerce entities in India. An 'e-commerce entity' has been defined to mean any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity. E-commerce entities are required to set up a proper grievance redressal mechanism and consumer complaints should be acknowledged by the grievance officer within a stipulated timeline. E-commerce entities are further required to, among others, provide information in relation to refund, exchange, warranty, delivery, mode of payment, fees and charges, grievance process and other relevant information on their platform. The price (total and a break up) of goods or services should be mentioned clearly and misleading advertisements and misrepresentation are prohibited.

In June 2022, the Central Consumer Protection Authority (CCPA), issued Guidelines on Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (the Guidelines). The Guidelines lay down the conditions for non-misleading and valid advertisements and conditions for bait advertisements. The Guidelines prohibit surrogate advertising, and also lay down conditions for advertisements targeted at children. Moreover, the Guidelines also lay down duties of manufacturer, service provider, advertiser and advertising agency.

The Privacy Rules also provide the right to "opt out" of email marketing, and the company's privacy policy must address marketing and information collection practices. Further, the National Do Not Call (NDNC) Registry is effectively implemented by the Telecom Regulatory Authority of India (TRAI). TRAI has also established the Telecom Commercial Communication Customer Preference Portal, i.e. a national data base containing a list of the telephone numbers of all subscribers who have registered their preferences regarding the receipt of commercial communications. Telemarketing companies may lose their license for repeated violation of DNC norms.

ONLINE PRIVACY

There is no regulation of cookies, behavioural advertising or location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

However, the IT Act contains both civil and a criminal offenses for a variety of computer crimes:

- Any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to approximately €570,341.28 (as at December 21, 2022) (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed:
    - To modify, destroy, record, or transmit data or programs residing within a computer, computer system or computer network; or
    - By any means to usurp the normal operation of the computer, computer system or computer network;
- Any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to three years and a fine up to approximately € 1,140.68 (as at December 21, 2022).

KEY CONTACTS

J. Sagar Associates
www.jsalaw.com/

Sajai Singh
Partner
J. Sagar Associates
T +91 80 435 03627
sajai@jsalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.