Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE NEW DELHI MUNICH / AMSTERDAM NEW YORK GIFT CITY

Research / Dossier

Privacy and Data Protection in India

June 2023

Research / Dossier

Privacy and Data Protection in India

June 2023

concierge@nishithdesai.com

FT INNOVATIVE LAWYERS 2019
FINANCIAL TIMES
ASIA-PACIFIC WINNER

Ranked as the 'Most Innovative Indian Law Firm' in the prestigious FT Innovative Lawyers Asia Pacific Awards for multiple years. Also ranked amongst the 'Most Innovative Asia Pacific Law Firm' in these elite Financial Times Innovation rankings.

Chambers AND PARTNERS

IFLR1000

The LEGAL 500

BENCHMARK LITIGATION

asialaw

WWL

ASIAN LEGAL BUSINESS

INDIA BUSINESS LAW JOURNAL

INDIA BUSINESS LAW JOURNAL THE LIST 2022 2023 LAW ASIA

Mergermarket An Acuris company

ITR WORLD TAX

ILA IDEX LEGAL AWARDS

LEGAL ERA BY THE PEOPLE. FOR THE PEOPLE. OF THE PEOPLE

concierge@nishithdesai.com

Disclaimer

Contact

For any help or assistance please email us on:
concierge@nishithdesai.com or **privacy.nda@nishithdesai.com**

or visit us at **www.nishithdesai.com**.

Acknowledgements

Aaron Kamath
aaron.kamath@nishithdesai.com

Purushotham Kittane
purushotham.kittane@nishithdesai.com

Aniruddha Majumdar
aniruddha.majumdar@nishithdesai.com

Varsha Rajesh
varsha.rajesh@nishithdesai.com

Akhileshwari Anand
akhileshwari.a@nishithdesai.com

Contents

Summary and Chronology of Significant Privacy Developments in India

I. Information Technology Act, 2000

The *Information Technology Act, 2000* (**"IT Act"**) was the first law enacted in India which contained provisions on confidentiality, privacy and security for information stored in a computer resource. In 2011, the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (**"Data Protection Rules"**) were issued under the IT Act to protect sensitive personal data and information collected from individuals by body corporates.[1] These rules make up the existing general data protection framework in India. In addition to the Data Protection Rules, the *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* and the directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet (issued in April 2022), which are administered by the Indian Computer Emergency Response Team (CERT-In) form the general cyber security framework in India.

II. Supreme Court Recognizes a Fundamental Right to Privacy

The Supreme Court in the landmark decision of *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors.*[2] affirmed that a fundamental right to privacy exists under the Constitution that is enforceable against the State even though it was not explicitly worded. This decision overruled previous Supreme Court decisions where the court held that there was no fundamental right to privacy. Further, the Court also asked for a data protection law to be framed to protect individual's rights against privacy parties.

III. Courts Divided on the Right to be Forgotten in India

The first case in India to deal with the concept of the right to be forgotten was heard in the Gujarat High Court, where the petitioner prayed for the removal of a published judgment in which he had been acquitted. The Court did not per se recognize the 'right to be forgotten' and disposed of the case as the petitioner had not been able to point out specific provisions of law that had been violated.[3]

The Karnataka High Court has also made references to the *"trend in the Western countries"* where they follow the *"right to be forgotten"* in sensitive cases.[4]

The Odisha High Court in the case of *Subhranshu Rout @ Gugul v. State of Odisha*[5] observed in its order on November 23, 2020 the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The case involved objectionable content regarding a woman that was posted online.

1 'Body corporates' includes any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities, as per Section 43A of the IT Act.

2 Supreme Court, Writ Petition (Civil) No 494 Of 2012.

3 *Dharmaraj Bhanushankar Dave v. State of Gujarat*, Special Civil Application No. 1854 of 2015.

4 *[Name Redacted] v. The Registrar, Karnataka High Court*, Writ Petition No.62038 Of 2016.

5 BLAPL No. 4592 of 2020.

The court encouraged the victim to seek appropriate orders for the protection of her fundamental right to privacy even in the absence of an explicit right to be forgotten. It noted that the right to be forgotten would be recognized by the proposed draft data protection bill.[6]

Distinguishing from the above decisions, the Madras High Court, on August 3, 2021, dismissed a petitioner seeking to have his name redacted from court orders by exercise of his right to be forgotten.[7] The petitioner was acquitted in certain criminal proceedings by the Madras High Court and prayed for his name to be redacted from the judgment of the Madras High Court. Without a precise framework or objective criteria for redaction of the name of an accused in India's criminal justice system, the court held that it would be more appropriate to await the enactment of India's new data protection law to exercise such rights and thus dismissed the petition.

In December 2022, a batch of petitions were filed before the Kerala High Court by multiple individuals who had sought deletion of judicial orders[8] published by Indian Kanoon and indexed by Google's search engine with their details included. The High Court held that the claim to have personal information erased or redacted based on informational privacy and the right to be forgotten cannot be relied on to prevent the uploading of judgments in the Court Information System for criminal matters. However, it also held that courts may allow a party to de-index and remove their personal information from search engines in certain circumstances on a case-to-case basis, and in cases where the law does not require an open court system, such as in family and matrimonial cases.

In the same case, a review petition was filed before the High Court of Kerala by one of the respondents, Google LLC. In its order dated March 30, 2023,[9] the court reiterated that the right to be forgotten cannot be claimed in relation to records of recent origin. The court also recognized the right to be forgotten as a fundamental right.

In another case in July 2022, a petition was filed before the Supreme Court submitting that the display of the petitioner's name in the public domain with respect to offences committed on the modesty of woman and involving Sexually Transmitted Diseases (STD) caused immense loss by way of social stigma and infringement of her personal privacy. The petitioner pleaded the 'right to be forgotten' and 'right of erasure' being part of the right to privacy, and prayed for the name of the petitioner as well as the respondent be removed/masked along with the address, identification details and case numbers to the extent that the same are not visible for search engines. The Supreme Court issued an order directing the registry to "examine the issue and to work out how the name of both the petitioner and respondent No. 1 along with address details can be masked so that they do not appear visible for any search engine."[10]

6 Please see our detailed update on this matter.http://nishithdesai.com/Content/pdf/210208_A_India__Individuals_Right_to_be_Forgotten_emphasised_by_HC.pdf, last accessed May 17, 2023.

7 *Karthick Theodre v. The Registrar General, Madras High Court* (W.P.(MD) No.12015 of 2021 and WMP(MD).No.9466 of 2021); available at: https://www.mhc.tn.gov.in/judis/index.php/casestatus/viewpdf/783065, last accessed April 14, 2023.

8 W.P.(C).Nos. 26500/2020, 6687/2017, 20387/2018, 7642/2020, 8174/2020, 21917/2020, 2604/2021, 12699/2021 & 29448/2021 decided on December 22, 2022 before the High Court of Kerala; available at: https://hckinfo.kerala.gov.in/digicourt/orders/2020/215700265002020_2.pdf, last accessed April 14, 2023.

9 RP No.107/2023 in W.P.(C).No.6687/2017, RP No.108/2023 in W.P.(C).No.2604/2021, RP No.109/2023 in W.P.(C).No.7642/2020, RP No.112/2023 in W.P.(C).No.20387/2018, RP No.113/2023 in W.P.(C).No.12699/2021, RP No.114/2023 in W.P.(C).No.21917/2020, RP No.116/2023 in W.P.(C).No.29448/2021, RP No.118/2023 in W.P.(C).No.8174/2020, RP No.120/2023 in W.P.(C).No.26500/2020, order dated March 30, 2023 before the High Court of Kerala; available at: https://hckinfo.kerala.gov.in/digicourt/orders/2020/215700265002020_2.pdf, last accessed May 18, 2023.

10 *XXXX v. YYYY*, Misc. App. 875/2022, SLP(Cr) 3211/2022.

IV. Committee to Examine Non-Personal Data Constituted

MeitY, in September 2019 had constituted a special committee (**"NPD Committee"**) to explore the governance of 'non-personal data' (**NPD**). The NPD Committee released a report on the Non-Personal Data Governance Framework in July 2020,[11] including a revised version in December 2020.[12] Although, not much traction on this report observed thereafter, it was reported that non-personal data could be included in the widened ambit of the draft data protection bill itself.[13]

V. Bureau of Indian Standards Publishes Data Privacy Standards

The Bureau of Indian Standards made available to the public its new standards for data privacy assurance i.e., the IS 17428 which was notified in the official Gazette on December 21, 2020.[14] The standard seeks to provide a privacy assurance framework for organizations to establish, implement, maintain and continually improve their data privacy management system. It comprises two parts – one being the prescriptive part where the requirements are to be mandatorily implemented by anyone applying the standard and the other part being the suggestive part with detailed best practices to aid in implementing the requirements of the prescriptive part.

VI. Supreme Court Forms Committee to Review Surveillance Laws

The Supreme Court of India heard a petition on October 27, 2021 following certain reports of a spyware called '*Pegasus*' (developed by an Israeli security firm i.e. the NSO Group) being deployed as a surveillance tool on Indian citizens.[15] The petitions prayed for an independent investigation to be conducted into the alleged deployment of Pegasus by certain foreign governments and Indian government agencies.

The Supreme Court noted that the impact of the alleged use of Pegasus on the right to privacy and freedom of speech need to be examined, while forming the three-member expert technical committee. The committee is directed to make recommendations on enactment or amendment to existing surveillance laws to ensure an "improved" right to privacy, improved cyber security and threat assessment measures. The committee had submitted an interim report in February 2022[16] and had sought public responses on the issues referred to it by the Supreme Court. The case is pending before the Supreme Court.

11 Available at: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf, last accessed February 25, 2023.

12 Available at: https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf, last accessed February 25, 2023.

13 Available at: https://indianexpress.com/article/business/looking-at-bigger-umbrella-pdp-bill-likely-to-include-non-personal-data-7552240/, last accessed February 25, 2023.

14 Available at: https://egazette.nic.in/WriteReadData/2020/223869.pdf, last accessed February 25, 2023.

15 *Manohar Lal Sharma v. UOI* (WP (Crl) 314 of 2021); available at: https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf, last accessed February 25, 2023.

16 Available at: https://indianexpress.com/article/india/pegasus-panel-to-probe-spying-charges-submits-its-report-to-sc-7784559/, last accessed February 25, 2023.

VII. MeitY Publishes a Policy for Use of Public Sector Data

MeitY also published an India Data Accessibility and Use Policy on February 21, 2022.[17] This policy seeks to establish a public access and data sharing framework of all public sector data i.e. data created, generated, collected or archived by the Indian Government or its agencies. Following the India Data Accessibility & Use Policy, MeitY also published a Draft National Data Governance Framework Policy which also focuses on use of Government data, particularly on its data collection and management processes and systems.[18] This draft policy purportedly replaces the India Data Accessibility & Use Policy and envisions the setting up of an India Data Management Office (IDMO) instead to issue rules and guidelines instead of the India Data Office. It proposes an India Datasets program consisting of non-personal and anonymized datasets obtained from Government ministries/departments. This data would be collected from Indian citizens or those in India.

Private entities are also encouraged to share non-personal data in a non-mandatory manner. The IDMO is charged with various enforcement functions such as publishing anonymization, meta data, data quality and sharing standards, rules regarding data requests, usage rights, disclosure norms, ethical and fair use of data, etc. While the power to license and monetize certain datasets by the Government in the earlier draft was subject to some criticism,[19] this policy does away with pricing models. However, pricing models for such datasets are again being contemplated under the newly proposed overarching digital law in India (*Please see Section VII above on the proposed Digital India Act*).

VIII. CERT-In Issues Directions for Cyber Security Incident Response

The CERT-in, is the agency appointed under the Information Technology Act, 2000 for dealing with cyber security incidents. It issued certain directions on April 28, 2022 under Section 70B(6) of the Information Act, 2000.[20] These directions provide a list of cyber security incidents that must be mandatorily reported by service provider, intermediary, data centre, body corporate and Government organisation within 6 hours of noticing such incidents or being brought to notice about such incidents. When CERT-In issues any order/ directions to a service provider/intermediary/data centre/body corporate, such entities must mandatorily take action or provide information or any such assistance to CERT-In.

Service providers, intermediaries, data centres, body corporate and Government organisations are required to undertake synchronisation of all their ICT systems clocks, designate a point of contact, enable logs of all ICT systems for a rolling period of 180 days within India. Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers are required to maintain certain prescribed information for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration. Virtual asset service providers, virtual asset exchange providers and custodian wallet providers (to be defined by Ministry of Finance) are required to maintain KYC information for 5 years.

The Government also issued a set of FAQs[21] to provide clarifications to certain aspects of the directions, in addition to certain oral clarifications during meetings with stakeholders.

17 Available at: https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022, last accessed April 14, 2023.

18 Available at: https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf, last accessed April 14, 2023.

19 Available at: https://www.medianama.com/2022/04/223-summary-iff-feedback-draft-data-access-policy/, last accessed April 14, 2023.

20 Available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf, last accessed April 14, 2023.

21 Available at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf, last accessed May 15, 2023.

IX. Draft Digital Personal Data Protection Bill, 2022

In pursuance of the developments in Court towards recognizing privacy as fundamental right, the Indian Government has been in the process of introducing an extensive data protection law since 2018.

Four drafts of a proposed standalone data privacy legislation has been released by the Government. The current and the latest draft of the proposed framework- draft Digital Personal Data Protection Bill, 2022[22] was released on November 18, 2022 for public consultation inviting comments for stakeholder and general public until January 2023.

The proposed law prescribes compliances for collection, storage, handling and transfers of personal data. It applies to the processing of digital personal data in India, where the personal data is (i) collected from the data principal online; and (ii) collected offline and subsequently digitized. It also imposes a soft data localization requirement for all personal data. It was reported that the Central Government is likely to notify a negative list of countries to which data pertaining to Indian users cannot be transferred.[23] The draft bill is expected to be tabled in the Monsoon Session of the Indian Parliament in July 2023.[24]

X. Proposed Digital India Act

A new law- the Digital India Act ("**Proposed DIA**") is proposed to overhaul the existing IT Act. In March 2023, the MeitY organized a consultation with experts, the general public, industry, academic, media, etc. to seek feedback on the broad framework of the Proposed DIA.[25] Reportedly, once the Proposed DIA is enacted, a new set of rules under the Proposed DIA may be introduced under this framework for sharing of non-personal data. These rules could include pricing for sharing anonymized data sets and provisions for free government access to boost efficiency of the government's welfare schemes.[26]

XI. Data Embassies

In the Budget for financial year 2023-24, it was announced that data embassies would be permitted to be established in India.[27] Data embassies are servers and technology infrastructures of countries owned and hosted by their governments outside of the territorial jurisdiction. Data embassies enjoy diplomatic immunity from local laws.

Reportedly, the MeitY plans to draft a separate policy for enabling data embassies which are likely to allow them to store only non-personal datasets.[28]

---

22 Available at: https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill,%202022.pdf, last accessed February 25, 2023.

23 Available at: https://economictimes.indiatimes.com/tech/technology/india-may-blacklist-some-nations-to-stop-data-flow-mos-it/articleshow/98829328.cms?from=mdr, last accessed April 17, 2023.

24 Available at: https://www.thehindu.com/news/national/new-data-protection-bill-likely-to-be-introduced-in-monsoon-session-in-parliament-centre-to-supreme-court/article66723887.ece, last accessed April 17, 2023.

25 Available at: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf, last accessed May 19, 2023.

26 Available at: https://www.hindustantimes.com/india-news/govt-may-frame-rules-for-the-sharing-of-non-personal-data-under-digital-india-law-101677355138634.html, last accessed May 19, 2023.

27 Available at: https://www.indiabudget.gov.in/doc/budget_speech.pdf, last accessed May 19, 2023.

28 Available at: https://www.business-standard.com/article/technology/data-embassies-may-only-be-allowed-to-store-non-personal-information-123021200403_1.html, last accessed May 19, 2023.

Right to Privacy — Now a Fundamental Right of Citizens

I. Judicial Precedents: Right to Privacy

- **First Supreme Court decision to deal with the fundamental right to privacy – March 1953**

  In a case where search warrants issued by judicial authorities were challenged on a fundamental rights violation, the Supreme Court held that no fundamental right to privacy existed under the *Constitution of India* (**"Constitution"**).[1]

- **The Supreme Court recognized the right to privacy albeit in a minority opinion – December 1962**

  In a case where regulations that allowed surveillance by the police were challenged; the Supreme Court, in its majority opinion rejected the idea of a fundamental right to privacy and permitted such surveillance, but the minority opinion held that privacy was protected as a fundamental right under the Constitution.[2] Given that this was a minority opinion, it was not binding.

- **Supreme Court recognizes privacy as a common-law right – March 1975**

  The Supreme Court for the first time recognized a common law right[3] to privacy, i.e. even though it was not guaranteed by the constitution and thus not a fundamental right, the Court recognized the existence of this right. This was a similar case filed to challenge the validity of police regulations which allowed police surveillance.[4]

- **Supreme Court links the right to privacy with Right to Life guaranteed under the Constitution – October 1994**

  In a case where a famous criminal opposed the publication of his autobiography by a news magazine on the ground that it violated his right to privacy, the Supreme Court for the first time linked the right to privacy to the right to life and personal liberty guaranteed under Article 21 of the Constitution, but also noted in the same breath that it was not an absolute right.[5]

II. Landmark Supreme Court Verdict on Privacy as Fundamental Right

The Supreme Court on August 24, 2017 passed the landmark judgment of *Justice K.S Puttaswamy (Retd.) v. Union of India and Ors.*[6] (**"Puttaswamy Case"**) wherein Article 21 of the Constitution was expanded by judicial reading to recognize privacy as a fundamental right, which can be claimed by individuals in India.[7]

1 *MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors,* 1954 AIR 300, 1954 SCR 1077.

2 *Kharak Singh v. State of Uttar Pradesh,* 1963 AIR 1295, 1964 SCR (1) 332.

3 A common-law right is one that has been created by judicial precedent, as opposed to a statutory/constitutional right that has been provided for in a statute.

4 *Govind Singh v. State of M.P.* 1975 AIR 1378, 1975 SCR (3) 946.

5 *R. Rajagopal v. State of Tamil Nadu,* 1995 AIR 264, 1994 SCC (6) 632.

6 WP (C) 494 of 2012.

7 This is as Article 21 is available to 'persons' and not only citizens.

The question of the right to privacy as a fundamental right has come up before the judiciary multiple times, but was never declared as a fundamental right available to citizens against the State before the Puttaswamy Case.

III. Impact of the Judgment

The impact of recognizing privacy as a fundamental right, as opposed to a statutory or a common-law right, is that it is an inviolable right – these fundamental rights cannot be given or taken away by law, all laws and executive actions must abide by them, and an individual cannot part with these rights. The judgment recognized that the right to privacy was now a fundamental right under Articles 19[8] and 21[9] of the Constitution. To clarify, these fundamental rights are enforceable only against the State or instrumentalities of the State and not against non-State parties. The Court, however, highlighted the need for a data protection law to confer rights on individuals and enforce such rights against non-State parties as well.

IV. Reasonable Restrictions

The Supreme Court has, clarified that like most other fundamental rights, the right to privacy is not an "absolute right", and is subject to the satisfaction of certain tests and reasonable restrictions. Therefore, a person's right to privacy could be overridden by competing state and individual interests. In the Supreme Court's view, the fundamental right to privacy cannot be read in isolation and that the infringement of any of the fundamental rights will have to pass the basic tests under Articles 14[10] and 21 of the Constitution as mentioned below:

- existence of law to justify an encroachment on privacy;
- the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action;

The judgment itself lays down some examples of what the legitimate aim of the state would be, i.e. protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits); the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law.

8 Article 19(1) states that: *"All citizens shall have the right— (a) to freedom of speech and expression; (b) to assemble peaceably and without arms; (c) to form associations or unions; (d) to move freely throughout the territory of India; (e) to reside and settle in any part of the territory of India; (g) to practice any profession, or to carry on any occupation, trade or business".* These rights are subject to reasonable restrictions.

9 Article 21 states that: *"No person shall be deprived of his life or personal liberty except according to procedure established by law".*

10 Article 14 states that: *"the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India".*

Further, the Court acknowledged that the principles set out in this judgment should be followed in the drafting of the new data protection law.

Post August 2017, the Puttaswamy Case has been upheld by the Delhi High Court in the case of Sangamitra *Acharya and Ors. v State (NCT of Delhi) and Ors.*[11] and in the Kerala High Court case of *Oommen Chandy v. State of Kerala*,[12] and both cases observed that the right to privacy lay against both State and non-State actors. Further, the Kerala High Court has applied the Puttaswamy Case where the determination of the privacy of an individual's bank account information was in question,[13] and where the right to access the internet was determined to constitute the right to privacy and education under the Constitution of India.[14]

11 250(2018)DLT36; In this case, the petitioner was an adult female who was forcibly taken away from the residence of her music teacher with whom she had been residing since the age of 18 by her parents, brother and police. The Court observed that the fundamental right to privacy applies against both State and non-State actors.

12 2018(2)KLT748; In this case, a committee consisting of a retired Judge relied on and published a letter containing sexual allegations against the Petitioner. The Court held that the right to privacy lies both against State action as well as private citizens like the press or media.

13 *Raju Sebastian v. Union of India*; Kerala High Court, WA. No.2112 OF 2018.

14 *Faheema Shirin v. State of Kerala*; Kerala High Court; WP(C). No.19716 OF 2019(L).

Existing Legal Framework on Data Protection

I. General Data Protection Law

In India, data protection viz. private parties is currently governed by the *Information Technology Act, 2000* (as amended) (**"IT Act"**) and more specifically, the rules issued under Section 43A of the IT Act: *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (**"Data Protection Rules"**). There are two categories of information covered under the IT Act, which need to be considered with respect to data protection:

a. **Personal information** (**"PI"**) which is defined as 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; and

b. **Sensitive personal data or information** (**"SPDI"**) which is defined to mean such personal information which consists of information relating to:

   i. passwords;

   ii. financial information such as bank account or credit card or debit card or other payment instrument details;

   iii. physical, physiological and mental health condition;

   iv. sexual orientation;

   v. medical records and history;

   vi. biometric information.[1]

I. Applicability

The Data Protection Rules are applicable to a body corporate that is engaged in the collection, receiving, possessing, storing, dealing or handling of SPDI using an electronic medium and sets out compliances for protection of SPDI by such body corporate. Thus, the Data Protection Rules do not apply to (i) natural persons who collect SPDI, or (ii) to standalone PI, or (iii) to information purely in the physical domain.

Further, the Data Protection Rules are applicable only to body corporates located within India. Therefore, if SPDI of any individual is collected, received, processed, stored, dealt with and handled outside India, the Data Protection Rules may not be applicable. The IT Act however, is applicable to an offence committed outside India if the act involves a computer, computer system or computer network located in India. However, the local data protection laws of the relevant countries may apply in relation to such data.

1 Further, as per Rule 3 of the Data Protection Rules, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force will not be regarded as sensitive personal data or information for the purposes of the Data Protection Rules.

Processing Data under a Contractual Obligation As we have discussed below, the draft Personal Data Protection Bill, 2018 introduces the concept of a 'Data Fiduciary' and a 'Data Processor' – wherein the Data Processor processes data on behalf of the Data Fiduciary and is subject to fewer compliance requirements as compared to the Data Fiduciary who remains primarily responsible. However, no such distinction existed in the Data Protection Rules.

However, the Department of Information Technology issued a Clarification on the Data Protection Rules in 2011 (**"2011 Clarification"**). It was clarified that:

The rules governing the collection and disclosure of SPDI,[2] will not apply to any body corporate providing services relating to collection, storage, dealing or handling of SPDI under a contractual obligation with any legal entity located within or outside India. The rules will, however apply to a body corporate, providing services to the provider of information under a contractual obligation directly with them. This clarification thus brought in a lower compliance requirement for 'Data Processors', as have come to be known under the DPB. This clarification was essentially introduced for the IT/Business Process Outsourcing (BPO) industry – where data is usually processed on the basis of contracts between the outsourcing entity and the entity who does the actual processing.

II. Compliance Requirements

The existing compliance requirements for the body corporates (company, firm, sole proprietorship, or other association of individuals) who possess, or handle SPDI under the Data Protection Rules are as follows:

a. Provide the individual with the option to either not provide the SPDI to the body corporate or to withdraw his/her consent (withdrawal of consent must be given in writing) given previously for the collection of SPDI.

b. Ensure that the SPDI is collected for a lawful purpose connected with the activity of the body corporate, and that the collection of the SPDI is considered necessary for the purpose.

c. Obtain specific consent of the individual, in writing (or any mode of electronic communication) regarding the purpose of use of the SPDI.

d. Provide a privacy policy for the handling of or dealing in SPDI, and ensure that such privacy policy is available on its websites and for view by individual.

e. Ensure that SPDI is not retained for longer than is required for the purpose for which the SPDI is collected.

f. Ensure that the SPDI is used for the purpose for which it has been collected.

g. Permit the individual to review the SPDI provided and have any inaccurate or deficient SPDI corrected or amended as feasible.

h. Ensure that a grievance officer is appointed, whose name and contact details are published on the website of the body corporate.

2 Rules 5 and 6.

i. Ensure that to the extent any SPDI is transferred to any third party (within or outside of India), specific permission has been obtained for such transfer, and that the transferee provides the same level of data protection as adhered to by the transferor as required under the Indian data protection laws.

j. Implement reasonable security practices and procedures such as the International Standard IS / ISO / IEC 27001, or any security practices and procedures that may be agreed to between the individual and the body corporate.

k. Maintain comprehensive documented security policies.

III. Penalties

i. Personal Information

Whilst there is no specific compliance set out in the IT Act or the Data Protection Rules with respect to PI, the IT Act provides for a penalty for offenders who, while providing services under a contract, have accessed PI, and with wrongful intent, discloses the PI, knowing that such disclosure would cause harm without authorization.[3]

This section prescribes a penalty of imprisonment up to three years and/ or a fine up to INR 5,00,000 (approx. USD 6,530).

ii. SPDI

As per the IT Act, where a body corporate, possessing, dealing or handling any SPDI is negligent in implementing security measures, and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the affected person.[4] There is no cap prescribed under the IT Act on the compensation payable to the person so affected.

Since the IT Act has extra-territorial jurisdiction, the above penalties may be applicable to parties outside India, subject to meeting certain nexus requirements to India.[5]

II. Industry Specific Regulations

I. Telecommunications Law

The *Indian Telegraph Act, 1885*[6] and the *Indian Telegraph Rules, 1951*[7] provide for certain directions issued by the Central/State Government for the interception of messages in situations of public emergencies, or in the interest of public safety. The Central/State Government may in specified instances, issue directions for such interception.

3 Section 72A, IT Act.
4 Section 43A, IT Act.
5 Section 75, IT Act.
6 Section 5 of the Indian Telegraph Act, 1885.
7 Rule 419A of the Indian Telegraph Rules, 1951.

From a regulatory perspective, it would be pertinent to note certain obligations of telecom service providers (**"TSP"**) under the Unified License (**"UL"**)[8] issued to the TSP by the Department of Telecom (**"DoT"**). We have listed below some privacy specific requirements to be complied with under the UL:

- TSPs cannot employ 'bulk encryption' equipment in its network. However, it has to ensure the privacy of any message transmitted over the network and prevent unauthorized authorization of any message'. This condition extends to those third parties who render services to the TSP.
- TSPs have to permit the government agencies to inspect 'wired or wireless equipment, hardware/ software, memories in semiconductor, magnetic or optical varieties', etc.
- TSPs have to procure 'trusted' telecom equipment from designated 'trusted sources' and where necessary, ensure that such equipment is tested and resolved for risks and vulnerabilities. TSPs have to ensure that this equipment provides for lawful interception and monitoring from a centralized location.
- TSPs are required to maintain Call Detail Record (CDR)/ IP Detail Record (IPDR) and Exchange Detail Record (EDR) with regard to communications exchanged over the TSP network. This data needs to be maintained for a period of two years.
- The TSP is not permitted to export out of India, accounting information of Indian telecom users (with the exception of international roaming subscribers) or user information of Indian telecom users (with the exception of foreign subscribers using Indian TSP's network while roaming and International Private Leased Circuit customers).
- TSPs are not permitted to use remote access facilities for content monitoring. Where remote access is otherwise provided (such as lawful monitoring by the government under the Indian Telegraph Act, 1885) from foreign locations, such locations must be approved by the government.
- TSPs have to maintain Call Detail Records/IP Detail Record for internet services including for internet telephony rendered for a minimum period of two years. Parameters of IP Detail Records that need to be maintained as per the directions/instructions issued by the government to TSPs.
- TSPs have to maintain log-in/log-out details of all subscribers for services provided such as internet access, e-mail, Internet Telephony, IPTV etc. These logs are required to be maintained for a minimum period of two years.
- A penalty of up to INR 500,000,000 (approx. USD 6,097,110) may be imposed by the government in the event of any security breaches on the TSPs networks which are caused due to inadequate precautions at the end of the TSP.

II. Banking Laws

Apart from the IT Act and Data Protection Rules, banks and financial institutions in India are governed and regulated by various regulations and guidelines (**"Banking Laws"**) issued by the Reserve Bank of India ("**RBI**"), the apex bank in India. There is no specific definition of 'sensitive data' or its equivalent under the banking laws. However, different Banking Laws, based on their subject matter seek to protect such kind of information.

8 Available at: https://dot.gov.in/sites/default/files/UL%20AGREEMENT%20with%20Audiotex%20M2M%20without%20INSAT%20MSSR%2017012022.pdf?download=1, last accessed February 25, 2023.

Certain Banking Laws such as the *Reserve Bank of India Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006*[9] and *Reserve Bank of India Master Direction on Outsourcing of Information Technology Services, 2023*[10] impose obligations on banks, which include that when engaging third party vendors / service providers / consultants / sub-contractors, to contractually impose certain obligations on such third parties. Few key obligations include:

- The third-party service provider would be required to report cyber incidents to the bank without undue delay;
- The service provider would be required to store bank-related data only in India, in line with data localization requirements;
- Banks would be required to have controls in the agreement with the service provider, for maintaining confidentiality of customers data. The service provider would be liable to the bank in the event of any security breach and leakage of such information;
- The agreement between the bank and service provider would include the types of data/information that the service provider is permitted to share with the bank's customers and/or any other party, and a non-disclosure clause or agreement with respect to the information retained by the service provider in relation to the outsourced activity;
- In case of cross-border outsourcing wherein the service provider is based out of India, the banks should closely and continuously monitor the policies of the service provider's jurisdiction, set up mitigation measures based on the country's risk, and ensure banks and the RBI have the right to audit the service providers, even in case of liquidation of the service providers; and
- Banks should also ensure that access to customer information by staff of the service provider is on a 'need to know' basis, and each bank's customer information, documents, records, and assets should be isolated and clearly identifiable to the respective bank with the service provider.

Some of the major laws in the BFSI sector which have privacy and security related provisions include the *Payment and Settlement Systems Act, 2007, RBI Circular on a Cyber Security Framework for Banks,*[11] *RBI Directions on Information Technology Framework for the NBFC Sector,*[12] *RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds,*[13] *RBI Report on Information Systems Security Guidelines for the Banking and Financial Sector,*[14] *RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks,*[15] *RBI Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligation of banks and financial institutions under PMLA, 2002,*[16] *RBI's Master Circular on Customer Service in Banks, 2014,*[17] *RBI's circular on Storage of Payment System Data, 2018,*[18] *RBI's Master Direction on Credit Card and Debit Card – Issuance and Conduct Directions,*

9 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=3148&Mode=0, last accessed April 17, 2023.

10 Available at: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486, last accessed April 17, 2023.

11 Available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF, last accessed February 25, 2023.

12 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10999&Mode=0, last accessed February 25, 2023.

13 Available at: https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf, last accessed February 25, 2023.

14 Available at: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=275, last accessed February 25, 2023.

15 Available at: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=3148&Mode=0, last accessed February 25, 2023.

16 Available at: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566 aspx?id=9848, last accessed February 25, 2023.

17 Available at: https://www.rbi.org.in/scripts/bs_viewmascirculardetails.aspx?id=9008, last accessed February 25, 2023.

18 Available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244, last accessed April 17, 2023.

2022,[19] *RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways,*[20] *and RBI's Guidelines on Digital Lending, 2022*[21].

Importantly, the RBI released the *Storage of Payment System Data Directive, 2018*[22] ("**Data Storage Circular**") in April 2018 which mandated the entire data relating to payment systems operated by system providers to be stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. This Data Storage Circular exempts data corresponding to the foreign leg of a transaction from this requirement. The deadline to comply with this mandate was on October 15, 2018.

The RBI then released clarifications in the form of FAQs on the circular in June 2019[23] The FAQs clarified that the directive is applicable to all Payment System providers authorised / approved by the RBI to set up and operate a payment system in India. It was also clarified that the end to end payments data is to be stored in India. The FAQs also addressed cross-border data flows, where it clarified that for processing of payment transaction is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier.

The *RBI's Guidelines on Digital Lending, 2022* lays down certain data-related compliances for regulated entities such as banks to ensure that the lending service providers ("**LSP**") and the digital lending apps of the LSPs/ banks ("**DLA**") adhere to. This includes ensuring that:

- any collection of data by LSPs'/banks' DLAs is need-based and with prior and explicit consent of the borrower with an audit trail,
- DLAs desist from accessing mobile phone resources like file and media, contact list, call logs, telephony function, etc. of the borrower (with one-time exceptions permitted for camera, location, microphone, etc., required for KYC and on-boarding requirements),
- the borrower is provided the option to give or deny consent for use of specific data, for data disclosure and retention, etc.,
- LSPs/DLAs engaged by the banks do not store personal information of borrowers except some basic data required for operations, i.e. name, address, contact details of the customer, etc., and
- no biometric data is stored/ collected in the systems associated with the DLA of banks/LSPs, unless allowed under extant statutory guidelines.

III. Capital Market and Financial Services

The Capital Markets and Financial Services industry is primarily regulated in India by the Securities and Exchange Board of India (**"SEBI"**). SEBI came out with a framework for *cyber security for some regulated entities called the Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories,*

19 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12300&Mode=0 aspx?id=7338, last accessed February 25, 2023.

20 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0, last accessed February 25, 2023.

21 Available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF, last accessed April 17, 2023.

22 Available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0, last accessed February 25, 2023.

23 Available at: https://www.rbi.org.in/Scripts/FAQView.aspx?Id=130, last accessed February 25, 2023.

and similar such circulars for other securities-market related entities (**"SEBI Circulars"**).[24] The SEBI Circular is applicable to Clearing Corporations, Depositories, Stock Exchanges, Mutual Fund Asset Management Companies, Stock Brokers, Derivative Exchanges, and Share Transfer Agents (**"MIIs"**).

The SEBI Circulars extensively cover the obligations of the MIIs as far as maintaining their IT infrastructure is concerned, such as the need to establish a Cyber Security and Cyber Resilience Policy, appointment of a designated officer for identifying cyber security risks, constitution of an internal technology committee with experts to review the policy, along with confidentiality and privacy requirements to be followed by MIIs. MIIs are also mandated to conduct comprehensive cyber audits at least twice in a financial year.

All cyber-attacks and cyber-incidents experienced by MIIs must be reported to SEBI within 6 hours of detecting such incidents or being brought to notice about such incidents, and to CERT-In in accordance with the relevant guidelines. Additionally, the SEBI issued an advisory for SEBI regulated entities outlining cybersecurity best practices in 2023,[25] prescribing additional responsibilities for the designated officer and specific measures against phishing attacks.

In 2020, SEBI issued the *Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solution, 2020* ("**Data Advisory**")[26] (accessible here) which is applicable to (i) stock brokers through exchanges; (ii) all depository participants through depositories; (iii) all merchant bankers (iv) all registrar to an issue and share transfer agent; (v) all debenture trustee (vi) all credit rating agencies (vii) all bankers to an issue (viii) all STP service providers, and (ix) all approved intermediaries.

Among other compliances, the Data Advisory requires 'critical data' to be stored in systems in India. The items of critical data is elaborated in Annexure to the Data Advisory. For background, this Annexure is the CERT-In *Advisory for Financial Sector Organizations- SEBI and RBI* issued by the Indian Computer Emergency Response Team (CERT-In) – the nodal agency for cybersecurity in India. Accordingly, critical data may include- *credit risk data, liquidity risk data, market risk data, system and sub-system information, internal and partner IP schema, network topography and design, audit/internal audit data, system configuration data, system vulnerability information, risk exception information, supplier information and its dependencies information.* Each of these items of critical data are not specifically defined.

More recently in 2023, SEBI issued the *Framework for Adoption of Cloud Services by SEBI Regulated Entities, 2023*[27] which applies to Stock Exchanges, Clearing Corporations, Depositories, Stock Brokers through Exchanges, Depository Participants through Depositories, Asset Management Companies/Mutual Funds, Qualified Registrars to an Issue, Share Transfer Agents, and KYC Registration Agencies. It sets out the baseline standards for security and regulatory compliances for implementing/adopting cloud computing tools including mitigating critical risks associated with cloud computing and to establish mandatory control measures.

---

24 Available at: https://www.sebi.gov.in/legal/circulars/jan-2019/cyber-security-and-cyber-resilience-framework-for-mutual-funds-asset-management-companies-amcs-_41589.html; https://www.sebi.gov.in/legal/circulars/oct-2019/cyber-security-and-cyber-resilience-framework-for-qualified-registrars-to-an-issue-share-transfer-agents_44660.html; https://www.sebi.gov.in/legal/circulars/jul-2015/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporation-and-depositories_30221.html; https://www.sebi.gov.in/legal/circulars/mar-2016/cyber-security-and-cyber-resilience-framework-of-national-commodity-derivatives-exchanges_32150.html; https://www.sebi.gov.in/legal/circulars/sep-2017/cyber-security-and-cyber-resilience-framework-for-registrars-to-an-issue-share-transfer-agents_35890.html; https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html; and https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html, last accessed April 17, 2023.

25 Available at: https://www.sebi.gov.in/legal/circulars/feb-2023/advisory-for-sebi-regulated-entities-res-regarding-cybersecurity-best-practices_68334.html, last accessed April 17, 2023.

26 Available at: https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html, last accessed February 25, 2023.

27 Available at: https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html?utm_medium=email&_hsmi=252016588&_hsenc=p2ANqtz-9S3NOYw198GD2rKqZzR3EwuLIqmvfqhFI9XNap4DmX-GZ4M0vaQcQaktiRp0p7_ESgVeZ_0YKvRzmQNn2uGBY1moqxEjPH8wfksJ6aZM9wUt530AI&utm_content=252016588&utm_source=hs_email, last accessed April 17, 2023.

This framework extends to all services deployed through the public, community and hybrid cloud. However, in terms of implementation, the above-mentioned regulated entites are required to adopt appropriate security, risk mitigation and due-diligence measures commensurate with the criticality and sensitivity of the systems, data/operations on the cloud.

IV. Insurance

The insurance regulator, the Insurance Regulatory and Development Authority of India (**"IRDAI"**) has in place a number of regulations and guidelines which contain provisions on data security. Examples are the *'IRDAI Information and Cyber Security Guidelines, 2023'* **("Insurer Guidelines"),**[28] *IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017,*[29] *IRDAI (Maintenance of Insurance Records) Regulations, 2015,*[30] *and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017.*[31] The above guidelines and regulations broadly provide for the following:

- Policies to be framed by the Insurer for information security
- Requirement to establish an Information Security Committee and its duties
- Requirement to appoint a Chief Information Security Officer and his duties
- Information Security Risk Management
- Data Security
- Platform, Application and Infrastructure Security
- Cyber Security

The Insurer Guidelines are a comprehensive set of guidelines prescribe compliances with respect to information systems, data security, network security, monitoring mechanisms, change control, could systems and security, service providers etc. The Insurer Guidelines are applicable to all insurance intermediaries (including brokers, corporate agents, web aggregators, corporate surveyors, insurance self-networking platforms and insurance repositories, motor insurance service provider, common service centres, insurance information bureau, insurance marketing firms). The Insurer Guidelines were made applicable to all insurance intermediaries (including brokers, corporate agents, web aggregators, corporate surveyors, insurance self-networking platforms and insurance repositories) as of 2022.[32]

Via the Insurer Guidelines, the IRDAI has recognized the immense growth in the information technology space, the varied applications of these developments on the insurance sector and the critical need to protect sensitive customer data, especially health data. Further, the *IRDAI (Maintenance of Insurance Records) Regulations, 2015* contain a data localization requirement, where records pertaining to all the policies issued and all claims made in India, are to be stored in data centers located and maintained only in India.[33]

28 Available at: https://irdai.gov.in/document-detail?documentId=3314780, last accessed February 25, 2023.

29 Available at: https://irdai.gov.in/document-detail?documentId=604638, last accessed February 25, 2023.

30 Available at: https://irdai.gov.in/document-detail?documentId=604674, last accessed February 25, 2023.

31 Available at: https://irdai.gov.in/document-detail?documentId=385593, last accessed February 25, 2023.

32 IRDAI circular on 'Implementation of Information and Cyber Security Guidelines', available at: https://irdai.gov.in/document-detail?documentId=385593, last accessed April 17, 2023.

33 Available at: https://irdai.gov.in/document-detail?documentId=604674, last accessed February 25, 2023.

V. Healthcare

Under the Ayushman Bharat Digital Mission ("**ABDM**"), the Ministry of Health and Family Welfare had announced the National Digital Health Mission. As part of this mission, the Health Data Management Policy ("**HDM Policy**") has been introduced [34] to govern health data under the ABDM Digital Health Ecosystem,[35] The HDM Policy recognises entities in the data processing space, i.e. data fiduciaries (similar to data controllers under GDPR) and data processors similar to the draft Indian data protection bill, and establishes a consent framework for processing personal data. It also lays down the framework for security by design for the digital health ecosystem under ABDM. As per the HDM, three separate Health IDs-for patients (Health ID), medical practitioners (Health Practitioner ID) and clinical establishments (Health Facility ID) will be created. Each ID comes with its sets of data access rights and privileges. The HDM Policy also gives the patient complete ownership over the health data and lays down a framework for how this data may be utilized. Once fully functional, the ABDM will link all patient data with a single Health ID making it easier for both patients and healthcare practitioners to access their medical history when making clinical decisions. The data may also be utilized in an anonymized form to better understand trends in public health and assist the government in making data-driven policy decisions in the healthcare space.

The National Health Authority invited comments from public on its Consultation Paper on proposed Health Data Retention Policy (**"Consultation Paper"**) released on November 23, 2021.[36] It proposes the health data retention framework for the ABDM architecture. The Consultation Paper also considers the applicability of the proposed health data retention policy to the entire healthcare system. The passage of a health data retention policy would create uniform principles for the retention, use, storage and accessibility of health data in line with international best practices.

VI. Geospatial Data Regulation and National Geospatial Policy

The Department of Science and Technology of the Government of India issued "*Guidelines for acquiring and producing geospatial data and geospatial data services including Maps*"[37] on February 15, 2021. Under these guidelines and as opposed to the previous legal regime, there is no restriction, nor requirement of any approval, clearance, license, etc. on the collection, generation, preparation, dissemination, storage, publication, updating and/or digitisation of geospatial data and maps within the territory of India, subject to a negative list of attributes for which there are restrictions. The guidelines also restrict foreign entities from creating and/or owning, or hosting geospatial data finer than certain prescribed threshold values. They are also restricted from conducting terrestrial mobile mapping surveys, street view surveys and surveying in Indian territorial waters. Our analysis of the new geospatial data and maps guidelines are available here.

34 Available at: https://abdm.gov.in/assets/uploads/consultation_papersDocs/Draft_HDM_Policy_April2022.pdf, last accessed February 25, 2023.

35 Available at: https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf, last accessed February 25, 2023.

36 Available at: https://abdm.gov.in:8081/uploads/Consultation_Paper_on_Health_Data_Retention_Policy_21_28557f9a6a.pdf, last accessed February 25, 2023.

37 Available at: https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf, last accessed February 25, 2023.

It was reported in December 2022 that the Union Cabinet has approved the National Geospatial Policy ("NGP")[38] which was initially released as a draft in 2021.[39] The NGP proposes a new body called the Geospatial Data Promotion and Development Committee ("GDPDC") which will take over the duties of the National Data Spatial Committee that governs utilization of spatial data and also establish a structure of practices and relationships among data producers and users that facilitates data sharing and use.

The NGP envisages private enterprises to play a significant role in the geospatial sector both independently and through collaborations with the Government and various Government agencies. While the NGP makes a reference to a "well-defined custodianship model and data supply chain" and "cross sector and multi-disciplinary collaboration involving all stakeholders", it does not expressly provide for any mandatory compliance requirements for private entities.

38 Available at: https://www.livemint.com/technology/tech-news/govt-introduces-national-geospatial-policy-to-promote-startups-advanced-tech-11672376526352.html, last accessed December 30, 2022.

39 Available at: https://dst.gov.in/sites/default/files/Draft%20NGP%2C%202021.pdf, last accessed December 30, 2022.

India: The Draft Digital Personal Data Protection Bill

Closer to a Reality in 2023

Authored by Aaron Kamath and Varsha Rajesh

As published in (February 2022)

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE

The Ministry of Electronics and Information Technology of the Government of India ('MeitY') published the draft Digital Personal Data Protection Bill, 2022 ('the Draft Bill') on 18 November 2022 for public consultation, which was open until 2 January 2023. Aaron Kamath and Varsha Rajesh, from Nishith Desai Associates, discuss the content of the Draft Bill and its potential impact on businesses.

The Indian Government has been working towards introducing a comprehensive standalone data protection legislation since 2018, and this is the fourth bill to be floated on the subject. The draft Bill is a much simpler version compared to the previous drafts and relaxes multiple compliance requirements previously proposed.

Once the draft Bill is deliberated and enacted by the Parliament; it will overhaul the current law, i.e. the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 issued under the Information Technology Act, 2000. The draft Bill also provides for different dates that may be appointed for different provisions, and hence there may be a transitional period for implementation.

Applicability of the Proposed Law

'Personal data' has been broadly defined as 'any data about an individual who is identifiable by or in relation to such data'. The draft Bill is proposed to apply to: (i) processing of digital personal data within the territory of India where the personal data which is collected from the data principal online and also to data which is collected offline and subsequently digitised; and (ii) processing of personal data outside India if in connection with any profiling, or activity of offering goods or services to data principals located within India.

The draft Bill does not apply to personal data processed by an individual for any personal or domestic purpose and, interestingly, data sets which have been in existence for at least 100 years.

The Data Protection Board of India

The Data Protection Board of India ('the Board') is proposed to be established under the draft Bill. The Board will function as an independent body and will function digitally, however, the exact composition and other aspects of the Board are to be further elaborated and prescribed by the Central Government.

The functions of the Board would include determination of non-compliance; imposition of penalties; and directing adoption of urgent remedial measures in cases of personal data breaches. Orders from the Board will be deemed to be decrees made by a civil court and may be appealed to the High Courts.

In a first, the draft Bill proposes an alternate dispute resolution mechanism. If the Board is of the opinion that any complaint may more be appropriately resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation.

In the event the Board determines on conclusion of an inquiry that a non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose a financial penalty of up to INR 5 billion (approx. ₹56.7 million).

Types of Regulated Entities

In increasing order of compliance obligations, there are three broad categories of regulated entities:

- data processors i.e. which process data on behalf of a data fiduciary;
- data fiduciaries akin to 'data controllers' which determine the purpose and means for processing of personal data; and
- significant data fiduciaries ('SDFs') which are a subset of data fiduciaries which are notified by the Central Government based on the volume and sensitivity of the data processed by them.

Notice and Consent

The draft Bill permits processing of personal data for a lawful purpose, with consent from the data principal. The data fiduciary is required to provide an itemised notice to the data principal, prior to or upon collection of personal data, in clear and plain language containing a description of personal data sought to be collected and the purpose of processing of such personal data. For consent given prior to enactment of the new law, such notice should be given to the data principal, as soon as reasonably practicable. Additionally, free, specific, informed, and unambiguous consent by clear affirmative action must be sought from the data principal for the collection and processing of their personal data. The consent may subsequently be withdrawn at the discretion of the data principal.

The draft Bill also specifies the role of 'consent manager', which are data fiduciaries that enables a data principal to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform.

Given that the current law prescribes notice and consent requirements only for the collection of sensitive personal data or information, businesses will now have to gear up to implement the notice and consent requirements for all personal data.

Deemed Consent

The draft Bill introduces the concept of 'deemed consent' as well as sets out scenarios and illustrations wherein consent is required. Essentially, a data fiduciary should not be required to provide consent for the collection and processing of data for the following purposes:

- where the data principal voluntarily provides personal data to the data fiduciary and it is reasonably expected that such personal data may be provided;
- for the performance of any function under any law, or the provision of any service or benefit to the data principal, or the issuance of any certificate, license, or permit for any action or activity of the data principal, by the State or any instrumentality of the State;
- for compliance with any judgment or order issued under any law;
- for responding to a medical emergency involving a threat to the life or immediate threat to the health of the data principal or any other individual;
- in case of taking measures to provide medical treatment or health services to any individual during an epidemic or outbreak of diseases etc.;
- for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order;
- for purposes related to employment including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a data principal who is an employee, and verification of attendance and assessment of performance;
- in public interest, which includes purposes such as prevention and detection of fraud, credit scoring, recovery of debt, mergers and acquisitions, network and information security, processing of publicly available personal data, operation of search engines, processing of publicly available personal data, and recovery of debt; and
- for fair and reasonable purpose as may be prescribed by the Central Government, including based on legitimate interests of the data fiduciary, and reasonable expectation of processing of personal data.

Deemed consent is similar to 'alternate grounds of processing of data' which is seen in privacy legislation in other jurisdictions. However, unlike the concept of alternate grounds of processing, deemed consent is not an alternate to consent based processing, instead, the data principal maybe deemed to have given their consent for processing only under the above-mentioned grounds. Hence, all rights applicable to consent-based processing (including withdrawal of consent) should apply here.

Data Principal Rights and Duties

The data principals may exercise certain rights with respect to their personal data:

- right to information about personal data including information regarding status of processing, summary of processing activities, and identities of all the data fiduciaries with whom the personal data has been shared along with the categories of personal data so shared;
- correction and erasure of personal data;

- right to grievance redressal; and
- right to nominate any other individual to exercise the above-mentioned rights under the draft Bill in the event of data principal's death or incapacity.

To protect businesses, the draft Bill imposes certain duties upon data principals, including prohibiting them from registering a false or frivolous grievance or complaint with a data fiduciary and from providing false information or suppressing material information. A penalty of up to INR 10,000 (approx. ₹110) may be levied on data principals for the failure to comply with their duties.

Compliances

Broadly, the compliances to be undertaken by data fiduciaries are as follows:

- comply with the draft Bill (irrespective of whether processing is undertaken by a processor/data fiduciary on its behalf or if the data principal is non-compliant with their duties;
- undertake reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete if the personal data is likely to be used by the data fiduciary to make a decision that affects the data principal or if the personal data is likely to be disclosed another data fiduciary;
- implement appropriate technical and organisational measures;
- protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach;
- notify the Board and each affected data principal in the event of a personal data breach;
- publish, in such manner as may be prescribed, the business contact information of a data protection officer ('DPO'), if applicable, or a person who is able to answer on behalf of the data fiduciary, the data principal's questions about the processing of their personal data; and
- share, transfer, or transmit the personal data to any data fiduciary or data processor with consent of the data principal.

Additionally, SDFs are required, among other obligations, to implement independent data audits, appoint a DPO, and carry out Data Protection Impact Assessments ('DPIAs'). Non-compliance with these additional obligations may attract a penalty of up to INR 1.5 billion (approx. ₹17 million).

Retention Period

While there are no specific retention periods prescribed, personal data is only permitted to be retained for as long as necessary for legal or business purposes. Further, personal data is not permitted to be retained if the purpose for which such personal data was collected is no longer being served by its retention.

Cross-border Transfers of Data

Personal data can be transferred to only those countries which are notified by the Central Government in accordance with terms and conditions as may be prescribed. At present, there is no foreseeability on the factors basis which countries may be notified.

For personal data, while the draft Bill does not expressly allow transfer of personal data outside India, it provides that the Central Government may whitelist certain countries or territories outside India. The draft Bill draft itself does not throw light on the factors based on which countries or territories will be whitelisted, nor the types of personal data that may be allowed/restricted to be transferred. The MeitY has also remarked that data localisation is intended to be the norm and cross-border transfer of personal data may only be allowed as an exception through 'corridors of trust' where established with such countries or territories.

Children's Data

The draft Bill mandates 'verifiable' parental/guardian consent for processing of children's data (those below age of eighteen). There is no exemption carved out for children who are between the ages 13 and 18 years old. Profiling, tracking, behavioural monitoring, and targeted advertising aimed at children and any other processing of personal data that can lead to harm to the child is also prohibited.

The primary issue with the requirement of 'verifiable parental consent' is that businesses will need to obtain consent of parents if children are accessing their services. This is applicable in instances of minor users availing services on the internet such as browsing videos, shopping online, and educational services which may involve the collection of personal data of children. This form of compliance could disincentivise businesses from offering services to children, including those which are useful. Further, there is a blanket ban on tracking and behavioural monitoring of children. There is no exemption carved out for activities which may be carried out to benefit children, such as preventing harm and ensuring the safety of children online.

The prohibition on targeted advertising directed at children overlaps with the prohibition on children targeted advertisements provided in the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 issued under the Consumer Protection Act, 2019. Currently there is no sight on how the two laws may interplay once the draft Bill is in force. The draft Bill proposes a high penalty which may extend up to INR 2 billion (approx. ₹22.6 million) for non-compliance with this children-data related obligations.

Data Breach Reporting

The draft Bill defines 'personal data breach' as 'any unauthorized 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'.

The draft Bill obligates the data fiduciary or the data processor to notify the Board and the affected data principals in the event of a personal data breach. The obligation to notify data principals does not exist under Indian law currently. The data fiduciary and the processor may contractually determine who is responsible for undertaking the reporting obligation. Further, the draft Bill proposes a penalty which may extend up to INR 2 billion for non-compliance with this requirement.

Exemptions

By way of notification, the applicability of provisions in the draft Bill may be exempted for any instrumentality of the state in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, and maintenance of public order. No specific exemptions have been specified for private bodies.

Conclusion

A revamp of the general data protection law has been in the works since 2017 when the Supreme Court of India delivered the landmark judgement in *Justice K S Puttaswamy and Anr v. Union of India and Ors* [Writ Petition (Civil) No. 494 of 2012] recognising the right to privacy as a 'fundamental right'. The draft Bill is a fresh and minimalistic take on reinventing the general data protection in law in India. Though covering a variety of aspects at a conceptual level, the draft Bill delegates to the Central Government a host of important matters, including the data breach notification requirements, compliances of a data fiduciary, classes of regulated entities, the exercise of a data principal's rights, and cross-border transfer of personal data.

Further, an interesting feature of the draft Bill is that it is not intended to overhaul the entire gamut of data protection regulations in India. Data privacy and security related obligations under sectoral laws currently, such as the banking regulations, insurance and health regulations, and securities regulations, will continue to apply in parallel. Therefore, businesses will continue to have to evaluate the applicability of sectoral laws to them or their products even after the draft Bill becomes law.

As with every new law, the draft Bill brings with it its own unique set of challenges and implementation hurdles. The draft Bill raises questions regarding: the regulation of personal data in the absence of sensitivity-based classification; the lack of foresight on how comprehensive the rules and regulations subsequently introduced will look like; the lack of clarity with respect to exemptions listed under deemed consent; and the broad powers vested with the Board. The draft Bill also misses out in clarifying several provisions and has left much to the discretion of the Central Government to frame rules and regulations. Aspects such as: the manner of personal data breach notifications; registration and functions of consent manager; parental consent for processing of personal data of children; the composition of the Board; conducting DPIAs; and audits, will be further elaborated by way of rules and regulations introduced by the Central Government. The indirect data localisation in the form of introducing requirement of approving only specific jurisdictions is also a cause of concern in the absence of clarity of how countries or territories maybe whitelisted.

Post the Government's receipt of public comments and feedback, it is expected that the draft Bill will be tabled before Parliament in 2023 and is expected to become law in 2023.

DMS - 21736.1

concierge@nishithdesai.com

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm — and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly — the VISION — to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech and Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times–RSG award 4 times in a row, (2014-2017) as the Most Innovative Indian Law Firm.

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

Research@NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our NDA Labs dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research papers and disseminate them through our website. Our ThinkTank discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. Imaginarium AliGunjan is a platform for creative thinking; an apolitical ecosystem that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness — that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have on our research publications. Please feel free to contact us at **research@nishithdesai.com**.

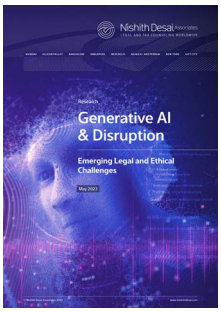
Recent Research Papers

Extensive knowledge gained through our original research is a source of our expertise.

May 2023

Sovereign Wealth Funds & Pension Funds: Investments into India

Regulatory, Legal and Tax Overview



May 2023

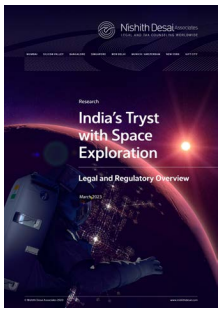
Generative AI & Disruption

Emerging Legal and Ethical Challenges

May 2023

M&A Lab

Adani's Hostile Takeover of NDTV



May 2023

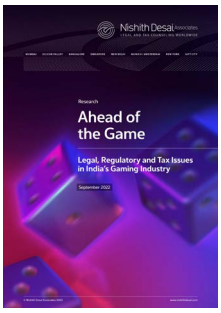
India's Tryst with Space Exploration

Legal and Regulatory Overview

January 2023

Doing Business in India

The Guide for US Businesses and Organizations Entering and Expanding into India



September 2022

Ahead of the Game

Legal, Regulatory and Tax Issues in India's Gaming Industry

For more research papers **click here**.

concierge@nishithdesai.com

Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

Tel +91 22 6669 5000

SILICON VALLEY

220 S California Ave., Suite 201
Palo Alto, California 94306, USA

Tel +1 650 325 7100

BENGALURU

Prestige Loka, G01, 7/1 Brunton Rd
Bengaluru 560 025, India

Tel +91 80 6693 5000

SINGAPORE

Level 24, CapitaGreen
138 Market St
Singapore 048 946

Tel +65 6550 9855

MUMBAI BKC

3, North Avenue, Maker Maxity
Bandra–Kurla Complex
Mumbai 400 051, India

Tel +91 22 6159 5000

NEW DELHI

13-H, Hansalaya Building, 15
Barakhamba Road, Connaught Place
New Delhi 110 001, India

Tel +91 11 4906 5000

MUNICH / AMSTERDAM

Maximilianstraße 13
80539 Munich, Germany

Tel +49 89 203 006 268

NEW YORK

1185 6th Avenue, Suite 326
New York, NY 10036, USA

Tel +1 212 464 7050

GIFT CITY

408, 4th Floor, Pragya Towers
GIFT City, Gandhinagar
Gujarat 382 355, India

Privacy and Data Protection in India

concierge@nishithdesai.com