Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE MUMBAI BKC NEW DELHI MUNICH NEW YORK GIFT CITY

Research

Privacy & Data in India: Fostering the World's Digital, Innovation and Outsourcing Destination

Legal, Ethical and Tax Considerations & Comparative Notes to the GDPR

May 2022

Research

Privacy & Data in India: Fostering the World's Digital, Innovation and Outsourcing Destination

Legal, Ethical and Tax Considerations & Comparative Notes to the GDPR

May 2022

concierge@nishithdesai.com

About NDA

We are an India Centric Global law firm (www.nishithdesai.com) with four offices in India and the only law firm with license to practice Indian law from our Munich, Singapore, Palo Alto and New York offices. We are a firm of specialists and the go-to firm for companies that want to conduct business in India, navigate its complex business regulations and grow. Over 70% of our clients are foreign multinationals and over 84.5% are repeat clients. Our reputation is well regarded for handling complex high value transactions and cross border litigation; that prestige extends to engaging and mentoring the start-up community that we passionately support and encourage. We also enjoy global recognition for our research with an ability to anticipate and address challenges from a strategic, legal and tax perspective in an integrated way. In fact, the framework and standards for the Asset Management industry within India was pioneered by us in the early 1990s, and we continue remain respected industry experts. We are a research based law firm and have just set up a first-of-its kind IOT-driven Blue Sky Thinking & Research Campus named Imaginarium AliGunjan (near Mumbai, India), dedicated to exploring the future of law & society. We are consistently ranked at the top as Asia's most innovative law practice by Financial Times. NDA is renowned for its advanced predictive legal practice and constantly conducts original research into emerging areas of the law such as Blockchain, Artificial Intelligence, Designer Babies, Flying Cars, Autonomous vehicles, IOT, AI & Robotics, Medical Devices, Genetic Engineering amongst others and enjoy high credibility in respect of our independent research and assist number of ministries in their policy and regulatory work. The safety and security of our client's information and confidentiality is of paramount importance to us. To this end, we are hugely invested in the latest security systems and technology of military grade. We are a socially conscious law firm and do extensive pro-bono and public policy work. We have significant diversity with female employees in the range of about 49% and many in leadership positions.

Asia-Pacific:
Most Innovative Law Firm, 2016
Second Most Innovative Firm, 2019

Most Innovative Indian Law Firm, 2019, 2017, 2016, 2015, 2014

Asia Pacific:
Band 1 for Employment, Lifesciences, Tax, TMT,
2021, 2020, 2019, 2018, 2017, 2016, 2015

Tier 1 for Private Equity, Project Development: Telecommunications Networks,
2020, 2019, 2018, 2017, 2014

Deal of the Year: Private Equity, 2020

Asia-Pacific:
Tier 1 for Dispute, Tax, Investment Funds, Labour & Employment, TMT, Corporate M&A, 2021, 2020, 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012

Asia-Pacific:
Tier 1 for Government & Regulatory, Tax, 2020, 2019, 2018.

Ranked
'Outstanding' for Technology, Labour & Employment, Private Equity, Regulatory, Tax,
2021, 2020, 2019.

Global Though Leader — Vikram Shroff
Thought Leaders-India — Nishith Desai, Vaibhav Parikh, Dr. Milind Antani
Arbitration Guide, 2021 — Vyapak Desai, Sahil Kanuga

Fastest growing M&A Law Firm, 2018

Asia Mena Counsel: In-House Community Firms Survey:
Only Indian Firm for Life Science Practice Sector, 2018

Please see the last page of this paper for the most recent research papers by our experts.

Disclaimer

Contact

For any help or assistance please email us on **concierge@nishithdesai.com**
or visit us at **www.nishithdesai.com**

Acknowledgements

Huzefa Tavawalla
huzefa.tavawalla@nishithdesai.com

Aaron Kamath
aaron.kamath@nishithdesai.com

Meyyappan Nagappan
meyyappan.n@nishithdesai.com

Purushotham Kittane
purushotham.kittane@nishithdesai.com

Contents

Prologue

There have been a plethora of developments in the privacy and data protection space in India. Data, off late, has been looked at by many very differently today in terms of value and treatment. There appears to be some rationale in the new saying that 'data is the new oil'. Uses of data for businesses today is vital for businesses to survive and lucrative if used efficiently. Data is the key for innovation, desirable customer experience and driver for competition. Without data, organizations would struggle to innovate or offer memorable experiences to consumers, both affecting technological developments and consumer choices and variety.

Globalization and technology have made cross border data flows ubiquitous and an essential phenomenon for global economic activity. As on April 2022, the World Bank estimates the digital economy to be equivalent to 15.5% of global GDP, growing two and a half times faster than global GDP over the past 15 years.[1]

India, now the largest consumer of mobile data in the world, has woken up and acknowledged the importance of data, its uses and security. Following the steps of global heavyweights and pushed against the wall in light of multiple data breaches in recent times, the Government and judiciary have been taking a more pro-active stance on protecting consumer rights and balancing organizations' interest when it comes to the fight (and freedom) for data.

India's apex court in 2018 declared the right to privacy as a fundamental right guaranteed under the Constitution of India. Thereafter, in December 2019, the Indian Government introduced in the lower house of Parliament – the **Personal Data Protection Bill, 2019** (**"PDP Bill"**). The PDP Billreferred to a joint parliamentary committee, was expanded into the draft **Data Protection Bill, 2021** (**"DPB"**) currently under Indian Government consideration. One cannot deny that India has also looked over its shoulder at the EU and the GDPR. Whist implementation and enforcement of the GDPR largely remains untested, certain concepts have been contemplated by the law framers in introducing the new law in India. Many companies, including Indian companies, are now GDPR compliant, and are looking at complying with the DPB. Hence, there may be certain deviations and incremental changes at an organizational and technological level to implement the DPB, due to the similarities between the laws. It is also pertinent to note at this juncture that India already has a basic regime in place, compliance of which cannot be boasted of. The Government has already in fact mandated localization requirements in certain sectors, reflecting its mindset that data in regulated and sensitive sectors should reside in India for ease of Government access if required, among other reasons.

Apart from the DPB, a committee within the Ministry of Electronics and Information Technology (**"MeitY"**) had also released a report on the Non-Personal Data Governance Framework,[2] including a revised version. On February 21, 2022, MeitY also published a draft India Data Accessibility and Use Policy to harness the potential of public sector non-personal data.[3] The interplay between the draft DPB and these regimes is yet to be thrashed out.

There are interesting and exciting times ahead as further developments unfold. We hope you enjoy this academic and industry-focused paper first taking us through how privacy has developed and evolved over the years in India, whilst we analyze the existing framework (general and industry-wise) and proposed framework, how it compares to the GDPR, tax considerations and what we can expect in the foreseeable future.

1. Overview of Digital Development, available at https://www.worldbank.org/en/topic/digitaldevelopment/overview#1 (last accessed May 3, 2022).
2. https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf (Last accessed May 3, 2022).
3. https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf (Last accessed May 3, 2022).

1. Summary and Chronology of Privacy Developments in India

I. Information Technology Act, 2000 Enacted

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 enacted under the IT Act to protect sensitive personal data and information collected from individuals by body corporates.[4] These rules make up the existing general data protection framework in India.

II. High 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 didn't 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.[5]

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.[6]

The Odisha High Court in the case of **Subhranshu Rout @ Gugul v. State of Odisha**[7] 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. 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. Please see our detailed update on this matter.[8]

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.[9] 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.

4. '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.
5. Dharmaraj Bhanushankar Dave v. State of Gujarat, Special Civil Application No. 1854 of 2015.
6. [Name Redacted] v. The Registrar, Karnataka High Court, Writ Petition No.62038 Of 2016.
7. BLAPL No. 4592 of 2020.
8. http://nishithdesai.com/Content/pdf/210208_A_India__Individuals_Right_to_be_Forgotten_emphasised_by_HC.pdf (last accessed May 3,2022).
9. 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 May 3, 2022).

III. 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.**[10] 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.

IV. Data Localization Mandate issued by the Reserve Bank of India

The Reserve Bank of India (**"RBI"**) released a notification on the storage of payment system data,[11] which mandated that the entire data relating to payment systems operated by entities licensed / directly regulated by the RBI must be stored in a system only in India and provided a deadline of October 15, 2018 for all entities to comply with this requirement. This notification provided an exemption for data pertaining to foreign leg of transactions. The RBI subsequently issued FAQs on the data localization requirement, which clarifies certain aspects of the circular, and provides context on instances wherein payment systems data may be processed outside India.

V. Government Issues Draft National E-Commerce Policy

The Department for Promotion of Industry and Internal Trade (**"DPIIT"**) released a Draft National E-Commerce Policy titled 'India's Data for India's Development'. A renewed draft of the e-commerce policy was reportedly leaked in July 2020. This policy proposed to set up an e-commerce regulator with wide-ranging powers over e-commerce entities and platforms. It also had proposals on sharing data with the Government such as algorithms and source codes, processing of non-personal data of consumers, anti-piracy, cross-border data transfers, etc. It was reported in March 2022 that this policy was being deliberated and would be published publicly after discussions.[12]

VI. RBI restricts card data storage

The Reserve Bank of India (**"RBI"**) has established a renewed regulatory framework for storage of payment instrument data by stakeholders for processing recurring payments.[13] A customer's card data cannot be stored by any entity in the payment transaction / payment chain other than card issuers and card networks. However, the last 4 digits of the actual card number and card issuer's name can be stored for transaction tracking and reconciliation purposes. Merchants and payment aggregators are prohibited from storing customer's actual card data and are required to purge existing data from their systems by 30th June 2022.[14] As an alternative, the RBI

10. Supreme Court, Writ Petition (Civil) No 494 Of 2012.
11. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244 ((last accessed May 3, 2022).
12. https://www.business-standard.com/article/economy-policy/centre-deliberating-on-e-commerce-policy-draft-says-cait-122032101012_1.html. (last accessed May 3, 2022).
13. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11668&Mode=0 (last accessed May 3, 2022).
14. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12211&Mode=0 (last accessed May 3, 2022).

has also prescribed workable solutions such as device-based tokenization and card-on-file tokenization as per prescribed framework. For recurring payments, merchants and payment aggregators have been working together with card issuers and card networks to implement these tokenization solutions to ensure continuity in online checkouts and payments as well as seamless recurring payments.[15]

VII. Kerala High Court lays down guidelines for sharing of data with 3rd parties by Government

The Kerala High Court in the case of **Balu Gopalakrishnan v. State of Kerala**[16] passed an interim order on April 24, 2020 on the export of COVID-19 related data by the State Government of Kerala to a US-based entity, Sprinklr, for data analytics. The High Court held that certain measures were to be implemented by the State Government before granting Sprinklr access to the data. These measures include anonymizing the data, obtaining specific consent from citizens, and ensuring the return of data once contractual obligations end. The High Court also barred advertisements and the commercial exploitation of the data by Sprinklr. This judgment sets an important benchmark for all public-private partnerships in the post COVID-19 era in the field of data protection and emphasizes the accountability of the State in handling data of its citizens. Our detailed update on this matter is available here.

VIII. 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,[17] including a revised version in December 2020.[18] 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.[19]

IX. 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.[20] 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.

15. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0 (last accessed May 3, 2022).
16. WP (C) 9498/2020.
17. https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf (last accessed May 03, 2022).
18. https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf (last accessed May 3, 2022).
19. https://indianexpress.com/article/business/looking-at-bigger-umbrella-pdp-bill-likely-to-include-non-personal-data-7552240/ (last accessed May 3, 2022).
20. See https://egazette.nic.in/WriteReadData/2020/223869.pdf (last accessed May 03, 2022).

X. Large messaging apps mandated to introduce traceability features

MeitY notified the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**[21] on February 25, 2021 replacing the **Information Technology (Intermediaries guidelines) Rules, 2011.** The new intermediary rules provide for certain due diligence requirements to be followed by internet 'intermediaries'. The rules also provides for recognition of certain intermediaries as 'significant social media intermediaries' if the number of registered users cross a certain threshold (subsequently notified as 50,00,000 registered users[22]). One of the additional due diligence requirements to be complied with by significant social media intermediaries which provide messaging services primarily is to enable the identification of the first originator of the any information that is transmitted through such intermediary, if required to do so by a court or a government direction to intercept, monitor or decrypt the information. The new intermediary rules provide that the significant social media intermediary is required to disclose only the identification of the first originator of a message and not the contents of any electronic message or any information related to the first originator or other users.

This traceability requirement under the new intermediary rules has been challenged by WhatsApp before the Delhi High Court[23] on the grounds of unconstitutionality and violation of the fundamental rights to privacy and freedom of speech and expression of an individual. The case is pending before the Delhi High Court.

XI. Bill regulating DNA technology being considered

During the 2021 monsoon session of the Parliament, the **DNA Technology (Use and Application) Regulation Bill, 2019**[24] was listed for consideration and passing before the lower house. This bill seeks to regulate the use of DNA technology for identifying persons for specific purposes such as solving crimes, among others. It also prescribes DNA collection procedures, establishment of DNA data banks, a regulatory board, accreditation mechanisms, etc. The bill was however not taken up in the Lok Sabha.

XII. 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.[25] 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

21. Available at https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (last accessed May 03, 2022).
22. See https://egazette.nic.in/WriteReadData/2021/225497.pdf (last accessed May 03, 2022).
23. WhatsApp v. Union of India (W.P. (C) 7284/2021).
24. Available at http://164.100.47.4/billstexts/lsbilltexts/asintroduced/128_%202019_LS_eng.pdf (last accessed May 03, 2022).
25. 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 May 03, 2022).

submitted an interim report in February 2022[26] and had sought public responses on the issues referred to it by the Supreme Court. The case is pending before the Supreme Court.

XIII. Data Protection Bill 2021

In December 2017, a Government appointed data protection committee chaired by Justice Srikrishna released an extensive white paper on data protection. Through this white paper, the committee released principles that should form the bedrock of the data protection law and sought comments from stakeholders as well as the public, to arrive at a draft of the law.[27] In July 2018, the committee released the draft Personal Data Protection Bill, 2018. Pursuant to further revisions in the bill, the draft Personal Data Protection Bill, 2019 was introduced in the lower house of Parliament. This draft bill was referred to a joint parliamentary committee for further debate and examination (**"Parliamentary Committee"**). The Parliamentary Committee on December 16, 2021 presented its report on the proposed data protection law, along with a revised version of the bill, the **Data Protection Bill, 2021** (**"DPB"**) in the Parliament.[28] The draft bill is yet to be tabled as a draft law for consideration and passing by the Parliament. Subsequent to the draft bill being made public, there have also been calls from the industry for a fresh consultation since many of the provisions deviate from the previous version published two years ago. It is reported that the Indian Government 'hopes' get the DPB passed in the Indian Parliament latest by the monsoon session of 2022, which typically is scheduled in July – August. Please refer to Chapter IV for our detailed analysis of the DPB.

XIV. Department of Science and Technology issues geospatial data guidelines

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"**[29] 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.

XV. MeitY publishes a policy for use of public sector data

MeitY also published an India Data Accessibility and Use Policy on February 21, 2022.[30] 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. In March 2022, the State of Tamil Nadu also published a 'Tamil Nadu Data Policy' along similar lines to leverage public sector data.[31]

---

26. https://indianexpress.com/article/india/pegasus-panel-to-probe-spying-charges-submits-its-report-to-sc-7784559/ (last accessed May 3, 2022).
27. https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf. (last accessed May 03, 2022).
28. Available at http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf (last accessed May 3, 2022).
29. Available at https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf (last accessed December 31, 2021).
30. https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022 (last accessed May 3, 2022).
31. http://cms.tn.gov.in/sites/default/files/go/it_e_16_2022_Ms.pdf (last accessed May 3, 2022).

XVI. The Criminal Procedure (Identification) Act, 2022 receives presidential assent

The Criminal Procedure (Identification) Act, 2022 received presidential asset and was published in the official gazette on April 18, 2022.[32] This act repeals the Identification of Prisoners Act, 1920. The act allows police officers or prison officers to collect biometric information such as fingerprints, iris and retina scans, photos, etc. and behavioral attributes including signatures and handwriting of persons arrested or convicted of offences punishable with imprisonment for a period of at least 7 years or offences committed against a woman or a child, and be retained in digital or electronic form for a period of 75 years. However, all biometric information and behavioral attributes are required to be destroyed from records (unless specifically directed by a court) if a person is released without trial or discharged or acquitted by the court, after exhausting all legal remedies.

XVII. Health Data Management Policy approved

On April 23, 2022, the Ministry of Health and Family Welfare released a draft Health Data Management Policy[33] to govern data under in the proposed National Digital Health Ecosystem,[34] which allows for interoperability of digital health systems at the patient, hospital, and ancillary healthcare provider level. The draft Health Data Management Policy also recognizes stakeholders such as data fiduciaries (similar to data controllers under GDPR) and data processors similar to the draft Indian data protection bill. It establishes compliances requirements for these stakeholders while recognising individual rights.

XVIII. CERT-In issues directions for cyber security incident response

The Indian Computer Emergency Response Team (CERT-In) which is the agency appointed under the Information Technology Act, 2000 for dealing with cyber security incidents has issued certain directions on April 28, 2022.[35] The 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. MeitY has also published FAQs on these directions on May 18, 2022.[36]

32. https://egazette.nic.in/WriteReadData/2022/235184.pdf (last accessed May 3, 2022).
33. Available at https://abdm.gov.in/assets/uploads/consultation_papersDocs/Draft_HDM_Policy_April2022.pdf (Last accessed on May 03, 2022).
34. https://economictimes.indiatimes.com/tech/technology/budget-2022-23-fm-announces-open-platform-for-national-digital-health-ecosystem-under-abdm/articleshow/89272174.cms (last accessed May 3, 2022).
35. https://www.cert-in.org.in/Directions70B.jsp (last accessed May 03, 2022).
36. https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf (last accessed May 18, 2022).

2. 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")**.[37]

- **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.[38] 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[39] 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.[40]

- **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.[41]

II. Nine-Judge Bench Judgment of the Supreme Court in the Puttaswamy Case

The Supreme Court on August 24, 2017 passed the landmark judgment of **Justice K.S Puttaswamy (Retd.) v. Union of India and Ors.**[42] **("Puttaswamy Case")** wherein Article 21 of the Constitution was expanded by judicial

37. MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors., 1954 AIR 300, 1954 SCR 1077.
38. Kharak Singh v. State of Uttar Pradesh, 1963 AIR 1295, 1964 SCR (1) 332.
39. 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.
40. Govind Singh v. State of M.P. 1975 AIR 1378, 1975 SCR (3) 946.
41. R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264, 1994 SCC (6) 632.
42. WP (C) 494 of 2012.

reading to recognize privacy as a fundamental right, which can be claimed by individuals in India.[43] 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[44] and 21[45] 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[46] 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.

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.**[47] and in the Kerala High Court case of **Oommen Chandy v.**

43. This is as Article 21 is available to 'persons' and not only citizens.
44. 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.
45. Article 21 states that: "No person shall be deprived of his life or personal liberty except according to procedure established by law".
46. 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".
47. 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.

State of Kerala,[48] 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,[49] and where the right to access the internet was determined to constitute the right to privacy and education under the Constitution of India.[50]

48. 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.

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

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

3. 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.[51]

A. 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.

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

51. 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.

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,[52] 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.

B. 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:

i. 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.

ii. 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.

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

iv. 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.

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

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

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

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

ix. 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.

x. 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.

xi. Maintain comprehensive documented security policies.

52. Rules 5 and 6 in particular.

C. 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.[53]

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. SDPI

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.[54] 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.[55]

II. Industry Specific Regulations

A. Telecommunications Law

The **Indian Telegraph Act, 1885**[56] and **the Indian Telegraph Rules, 1951**[57] 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.

From a regulatory perspective, it would be pertinent to note certain obligations of telecom service providers (**"TSP"**) under the Unified License (**"UL"**)[58] 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 have to permit the government agencies to inspect 'wired or wireless equipment, hardware/ software, memories in semiconductor, magnetic or optical varieties' etc.

  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 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 one year.

53. Section 72A, IT Act.
54. Section 43A, IT Act.
55. Section 75, IT Act.
56. Section 5 of the Indian Telegraph Act, 1885.
57. Rule 419A of the Indian Telegraph Rules, 1951.
58. https://dot.gov.in/sites/default/files/UL%20AGREEMENT%20with%20Audiotex%20M2M%20without%20INSAT%20MSSR%2017012022.pdf?download=1 (last accessed May 03, 2022).

- 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 international roaming subscribers using Indian TSP's network while roaming and International Private Leased Circuit customers).

- TSPs have to maintain Call Detail Records/IP Detail Record for internet services rendered for a minimum period of one year. Parameters of IP Detail Records that need to be maintained as per the directions/ instructions issued by the government to the telecom operators.

- 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 one year.

- A penalty of up to INR 500,000,000 (approx. USD 6,531,000) 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.

B. 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 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. Further, certain Banking Laws 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.

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,[59] RBI Directions on Information Technology Framework for the NBFC Sector,[60] RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds,[61] RBI Report on Information Systems Security Guidelines for the Banking and Financial Sector,[62] RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks,[63] 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,[64] RBI's Master Circular on Customer Service in Banks, 2014,[65] RBI's Master Direction on Credit Card and Debit Card – Issuance and Conduct Directions, 2022,[66] and RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways.[67]**

Importantly, RBI released the Storage of Payment System Data Directive, 2018[68] 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 Circular exempts data corresponding to the foreign leg of a transaction

59. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF. (last accessed May 03, 2022).
60. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10999&Mode=0 (last accessed May 03, 2022).
61. https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F. pdf. (last accessed May 03, 2022).
62. https://www.rbi.org.in/Scripts/PublicationReportDetails. aspx?ID=275. (last accessed May 03, 2022).
63. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=3148&Mode=0. (last accessed May 03, 2022).
64. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566 aspx?id=9848. (last accessed May 03, 2022).
65. https://www.rbi.org.in/scripts/bs_viewmascirculardetails. aspx?id=9008. (last accessed May 03, 2022).
66. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12300&Mode=0 aspx?id=7338. (last accessed May 03, 2022).
67. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0 (last accessed May 03, 2022).
68. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. (last accessed May 03, 2022).

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[69] The FAQs clarified that the directive is applicable to all Payment System providers authorised / approved by the Reserve Bank of India (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.

C. 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** (**"SEBI Circular"**).[70] The SEBI Circular is only applicable to Clearing Corporations, Depositories and Stock Exchanges (**"MIIs"**).

The SEBI Circular extensively covers 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, along with confidentiality and privacy requirements to be followed by MMIs.

D. 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 'Guidelines on Information and Cyber Security for Insurers' (**"Insurer Guidelines"**),[71] **IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017,**[72] **IRDAI (Maintenance of Insurance Records) Regulations, 2015,**[73] **and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017.**[74] 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.

69. https://www.rbi.org.in/Scripts/FAQView.aspx?Id=130. (last accessed May 03, 2022).
70. http://www.sebi.gov.in/sebi_data/attachdocs/1436179654531. pdf. (last accessed May 03, 2022).
71. https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20Information%20and%20Cyber%20Security%20for%20insurers.pdf. (last accessed May 03, 2022).
72. https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1. (last accessed May 03, 2022).
73. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo2604&flag=1. (last accessed May 03, 2022).
74. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3191&flag=1. (last accessed May 03, 2022).

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.[75]

E. Healthcare

Under the Ayushman Bharat Digital Misson, the Ministry of Health and Family Welfare had announced the National Digital Health Mission. As part of this mission, a draft Health Data Management Policy (**"draft HDM Policy"**) has been released[76] to govern health data under in the proposed National Digital Health Ecosystem,[77] The draft 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 provides for rights to individuals, establishes an identification framework for stakeholders and mandates certain compliance requirements on data fiduciaries.

F. Geospatial Data Regulation

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"**[78] 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.

75. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1(last accessed May 03, 2022).
76. Available at https://abdm.gov.in/assets/uploads/consultation_papersDocs/Draft_HDM_Policy_April2022.pdf (last accessed May 03, 2022).
77. https://economictimes.indiatimes.com/tech/technology/budget-2022-23-fm-announces-open-platform-for-national-digital-health-ecosystem-under-abdm/articleshow/89272174.cms (last accessed May 03, 2022).
78. Available at https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf (last accessed May 03, 2022).

4. New Data Protection Law Proposed in India

I. Background

The DPB is an omnibus, cross-sector privacy law, with similarities to the E.U. General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. It is a substantially revised version of the PDP Bill and the draft Personal Data Protection Bill, 2018, of which the latter was proposed in July 2018 by a Committee of Experts set up by the Government, chaired by retired Supreme Court judge, Justice Srikrishna (**"Committee"**).

On December 12, 2019, the PDP Bill was referred to a Joint Parliamentary Committee for further debate and examination (**"Parliamentary Committee"**). Initially expected to be presented in early 2020, the Parliamentary Committee presented its report on the PDP Bill in the Parliament on December 16, 2021 (**"Report"**). While the Report has been adopted by the members of the Parliamentary Committee, eight members have submitted dissent notes on certain aspects of law.

The Report recommends several amendments to the PDP Bill, including a change in title i.e., renaming the draft law to Data Protection Bill, 2021, since the law now proposes to regulate the collection and processing of both personal data and non-personal data (**"NPD"**). At this stage, the DPB is merely a draft law, and is yet to be tabled as a Bill for the consideration of the Parliament. Notably, the recommendations of the Parliamentary Committee are not binding upon the Government. The DPB may be tabled in Parliament in its current form, or undergo change. Nonetheless, the legislative process is likely to entail the following steps prior to law enactment:

- The DPB could be accepted as it is, or amended further by MeitY.
- The MeitY is then expected to seek Cabinet approval prior to the introduction of the revised DPB on the floor of the Parliament.
- The draft DPB, as will be introduced in the Parliament, will be debated and passed by both Houses of the Parliament.
- The version of the DPB passed by both Houses of the Parliament (including further amendments suggested by the Parliament, if any) would then require Presidential assent.
- Subsequent to obtaining Presidential assent, enactment of the law entails its publication in the Official Gazette.

However, since the DPB does not have any transitional provisions (such as the GDPR or the California law), businesses should strongly consider beginning preparation for its implementation. The implementation of various provisions is dependent on the Government notifying such provisions into law. The Report suggests that the Act would be made effective not later than 24 months from the date of notification although this remains a matter of discretion and we would suggest that a transition period is provided for in the text of the DPB.

II. Highlights of the DPB and What It Means for You

1.	**Major overhaul of current data protection law in India:**	The erstwhile data protection regime under the Information Technology Act, 2000, was limited in scope to electronic information, largely concentrating on sensitive personal data and information. It was a notice-and-consent-based regime, with minimal compliances. The DPB is far more complex and far-reaching than the current law and extends to all forms of personal data.
2.	**Extra-territorial application**	It applies to all entities outside India if they process personal data in connection with a business in India, or systematically offers goods / services to data principals in India or undertake profiling of data principals in India. While the intent behind the incorporation of the terms ``business connection", "systematic activity" and "profiling" have not been discussed in the Report, further guidance on the interpretation of these terms could be derived from supplementary sources such as taxation laws, and prior reports on the subject, including the Report of the Justice B. N. Srikrishna Committee on data protection.
3.	**New data regulator (the Data Protection Authority, the "DPA"), adjudicating officers, and appellate tribunal**	Currently, MeitY oversees data protection issues as part of its larger functions. The DPA will be the first cross-sector dedicated data protection regulator in India (governing both personal and NPD) vested with significant regulation-making powers. The DPA is however required to consult with other sectoral regulators, and the Central Government, for the discharge of certain functions. The DPA will contain an independent adjudicatory wing, consisting of adjudicating officers tasked with adjudicating contraventions of the law, determining penalties, and other matters such as determining the enforceability of a "right to be forgotten" request. Appeals against orders of the DPA will lie before the Appellate Tribunal established under the DPB.
4.	**Subordinate legislation**	The DPB delegates a host of important matters, including the specification of types of data, classes of regulated entities, and codes of practice to the Central Government and the DPA. A true compliance picture will form only when these rules and regulations are framed.
5.	**Wider categories of data protected**	The proposed DPB will apply to all 'personal data'[79], SPD,'[80] CPD,[81] as well as NPD,[82] including anonymised personal data9. Higher benchmarks of compliance are prescribed for SPD and CPD (which are subsets of 'personal data').
6.	**Data localization for sensitive data**	A copy of all SPD must be stored in India but may be transferred outside India subject to obtaining explicit consent of the data principal, and compliance with the terms of DPA-approved contracts or intra-group schemes. CPD (which will be defined by the Central Government through Rules) must be processed only in India, with the exception of transfers required for prompt action in terms of delivering health or emergency services, and transfers permitted by the Central Government in accordance with the DPB. Organizations processing SPD should prepare their infrastructure for data localization.

79. Personal data is defined in the DPB as "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling".

80. Sensitive personal data is defined in the DPB as "such personal data, which may, reveal, be related to, or constitute - (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (iv) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15. Explanation.- For the purposes of this clause, the expressions,- (a) "intersex status" means the condition of a data principal who is- (i) a combination of female or male; (ii) neither wholly female nor wholly male; or (iii) neither female nor male; (b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure".

81. Critical personal data is explained in the DPB as any personal data that is notified by the Government as critical personal data.

82. Non-personal data is defined in the DPB as "data other than personal data".

4. New Data Protection Law Proposed in India

7.	**Cross-border transfer restrictions**	Personal data (that does not qualify as SPD or CPD) has been exempted from cross-border transfer restrictions. SPD may be transferred outside India if there is: a. Explicit consent of the individual, and b. Either: i. A regulator-approved contract or intra-group scheme for the transfer; or ii. A regulator-approved transferee entity or country. Data notified as CPD may be transferred outside India with the permission of the Central Government, on certain narrow grounds. These include transfers required for prompt action in relation to the provision of health and emergency services, and transfers to countries or international organisations, specifically greenlit by the Central Government, in line with strategic interests of the State.
8.	**Privacy principles**	The principles underlying the DPB are largely in line with global regulation, and include consent (with exceptions), purpose limitation, storage limitation and data minimization.
9.	**Rights-based law**	The rights conferred on individuals include: ■ The right to confirmation and access; ■ the rights to correction, and erasure; ■ the right to data portability; and ■ the right to be forgotten; Data fiduciaries (those that determine the purpose and means for processing) will need to implement processes to honor these rights when exercised by individuals.
10.	**Consent managers**	A new concept of registered 'consent managers' who liaise between individuals and data fiduciaries, including for the exercise of the above rights, has been introduced. The idea of 'consent managers' is innovative but relatively untested in practice. Similar frameworks have been explored by the RBI in the financial sector through the "Account Aggregator'' model, which enables consumers to manage consent across a variety of financial accounts and products. The underlying intention appears to be mitigation of 'consent fatigue' and providing greater awareness to the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on the implementation of the consent manager framework.
11.	**Three types of regulated entities**	In increasing order of compliance obligations, these are: a. Data processor (akin to the eponymous GDPR concept); b. Data fiduciary (akin to the GDPR 'data controller'); and c. Significant data fiduciary (a subset of data fiduciary). Significant data fiduciaries (**"SDFs"**) are treated as full-fledged regulated entities and are required to implement independent data audits, appoint a data protection officer, and carry out data protection impact assessments prior to carrying out any processing with a risk of significant harm, among other obligations. SDFs include 'social media platforms' with over a certain number of users and whose actions are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, and security of the State. Data fiduciaries processing children's personal data, or involved in the provision of services to children, have also been included within the scope of SDF.

12.	**Personal data breach notifications**	Personal data breaches (including breaches of SPD and CPD) must be reported to the DPA, who may upon evaluation of the impact of the breach, require that the breach be reported to affected individuals and that remedial action be taken.
13.	**Special provisions concerning children's data**	The DPB mandates age verification, and parental consent. No exemptions have been provided for the requirement of obtaining parental consent. The DPB prohibits the profiling, tracking, or behavioral monitoring or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child.
14.	**Innovation sandbox for artificial intelligence and emerging technology**	The innovation sandbox instituted by data fiduciaries and start-ups is supervised by the regulator, and eligible data fiduciaries can avail of relaxations from certain obligations of the DPB up to a maximum period of 3 years
15.	**Government requests for anonymized and NPD**	The Central Government has been given the power to direct that anonymized / NPD be shared by any entity with the Central Government, in certain circumstances. The Central Government has also been given the policy space to frame a policy on the regulation of NPD including anonymized data.
16.	**GDPR-like penalties**	The DPB provides for civil compensation; financial penalties such as fines (up to 4% of global turnover); and criminal penalties in the limited case of unauthorized de-identification of data.
17.	**Phased Implementation**	The DPB provides that it will come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of the law.

III. Detailed Analysis of the DPB

The key points to note in the DPB are as follows:

A. Amendments to Current Law

The DPB, when enacted, will replace Section 43A[83] of the Information Technology Act, 2000 and the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** (Current Law) which currently, in tandem with sectoral laws, provide for the data protection framework in India.

B. Applicability

The DPB applies to the processing of personal data of natural persons, of which SPD and CPD are subsets. The natural person whose data is being processed is referred to as a **"Data Principal".** Further, the proposed law applies to both automated and non automated processing, as further elaborated in Section XVIII.

i. Retrospective Applicability

The DPB is silent about retrospective applicability, i.e. applicability to data collected before the law comes into effect. However, the report issued along with the PDP Bill stated that the law will apply to any ongoing processing once introduced. While this has not been addressed in the Report, the same understanding ought to continue.

83. Section 43A: Compensation for failure to protect data
"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008) Explanation: For the purposes of this section (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. (iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

Sans any such current legal requirement, it is likely that prior to the enactment of the DPB substantial amounts of personal data would have been obtained with consent. Thus, data fiduciaries will need to obtain necessary consents for the continued processing of such personal data.

Similarly, data fiduciaries may have to delete all such personal data which was obtained by them without specific consents, unless specific consent is obtained for continued processing of such personal data, in accordance with the DPB.

ii. Definitions

Several definitions in the DPB are open-ended. This could create uncertainties in the manner in which the DPB will be interpreted, implemented and enforced.

For instance, the definition of harm includes references to **"any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled", "any observation or surveillance that is not reasonably expected by the data principal" and "psychological manipulation which impairs the autonomy of the individual",** all of which are ambiguous and open-ended. The updated definition of "harm" also includes any other harm as may be prescribed by the Central Government. Thus, raising concerns of untested inclusions to the definition of "harm" by the Central Government from time to time.

iii. Personal Data

Personal data has been defined as data about, or relating to, a natural person who is directly or indirectly identifiable, having regard to any (or combinations of) characteristic, trait, attribute or any other feature of the identity of such natural person, and includes any inference drawn from such data for the purpose of profiling.

The definition of personal data is extremely wide in comparison to the Current Law. While the Parliamentary Committee noted stakeholders' suggestion of excluding 'inferences drawn from profiling' from the definition of personal data, the same has not been reflected in the definition incorporated under the DPB.

With the exception a few specifically identified provisions,[84] and other exemptions which may be granted (such as an exemption from complying with requests for enforcing Data Principals' rights), the provisions of the DPB are equally applicable to non-automated (manual) processing of personal data, Thus, several non-digital businesses, which manually collect and process personal data (not qualifying as SPD or CPD), will be expected to comply with consent requirements, and demands for enforcement of the right to confirmation and access, and the right to correction and erasure, unless the DPA provides exemptions.

iv. Sensitive Personal Data

SPD is a subset of personal data and consists of specified types of data, such as financial data, health data, official identifier, sex life, sexual orientation, biometric data,[85] genetic data, transgender status, intersex status, caste or tribe, religious or political belief, etc. The DPA has the power to declare further categories of data as SPD. The DBP also bars the processing of certain forms of biometric data as may be prescribed, unless it is permitted by law.

84. As per Section 39 of the DPB, the provisions that are not applicable to non-automated processing by small entities are Section 7, 8, 9, 17(1)(c), and Sections 19 -32.

85. The DPB specifically bars the processing of biometric data, unless such processing is "permitted by law". Notably, the provision is quite wide and the scope of which biometric data may not be processed seems to be unclear.

Several stakeholders had urged the Parliamentary Committee to adopt an exhaustive definition of SPD, as opposed to an open-ended and inclusive definition. However, it did not adopt this recommendation.

There are certain additional compliance requirements for SPD, such as the data localization and restrictions on processing. We have covered these below. As a result of these additional compliance requirements, the BFSI and Pharmaceutical industries are likely to get affected as both 'financial data' and 'biometric/health data' have been retained as categories of SPD. Our specific observations are below:

- **Financial data:** The definition of financial data ought to have been restricted to 'authentication information' for financial instruments alone. Information such as a bank account number, on its own, and in the absence of other information relevant to authentication and access to financial accounts and information, is unlikely to cause harm to the Data Principal. For example, with the advent of the usage of mobile phone numbers as primary means to enable digital payments, they are often used in lieu of bank account numbers as the identifiers for mobile wallets.

- **Biometric data:** In addition to fingerprints, iris scans, facial images, biometric data has been defined to include 'behavioral characteristics'. The said term is not defined. Prima facie, it could impact voice activated assistants and assistive technologies which are used by people with disabilities. Further, the Central Government has the overarching power of carving out certain kinds of biometric data from processing, as it may deem fit, resulting in further uncertainty over the legality of incorporating security and access control hardware in various devices.

- **Religious or political beliefs/ caste or tribe:** Interestingly, the DPB also includes religious or political beliefs / caste or tribe within the realm of SPD. However, in the Indian context, the inclusion of these items does not appear to be entirely relevant as they might be disclosed via individuals' surnames.

- **Official identifiers:** Official identifiers have been defined to include any number, code or other identifier, assigned to a Data Principal under a provision of law for the purpose of verifying the identity. While Aadhaar UIDs have been removed from the illustrative list of official identifiers, the inclusive definition is still broad enough to include Aadhaar UIDs, since it includes any number or identifiers used for the purpose of verifying the identity of a Data Principal. Given that some official identifiers may be asked for verification by various government as well as non-governmental bodies, it will burden many organizations with compliance requirements by virtue of just collecting such data in electronic form.

v. Processing

Processing has been defined very broadly to include an operation or set of operations performed on personal data, and may include operations such as collection, organization, storage, alteration, retrieval, use, alignment or combination, indexing, disclosure, etc.

vi. Data Fiduciaries and Data Processors

Entities processing personal data, may be either **"Data Fiduciaries"** (the entity that determines the purpose and means for processing) or **"Data Processors"** (the entity that processes personal data on behalf of a Data Fiduciary). These 'entities' may be the State, a company, a non-government organization, a juristic entity or any individual. While most obligations under the DPB are applicable to data fiduciaries, limited obligations have also been imposed upon data processors, such as the necessity to implement security safeguards.

vii. Non-personal / Anonymized Data

NPD (Including anonymized data (i.e. data which cannot identify a Data Principal)) has been defined as **"data other than personal data"** and has now been included within the scope of the DPB.

The extent to which large datasets can be truly anonymized (an irreversible process) is still a matter of global debate, as there may always be identifiers from which it may be re-identified as personal data. However, for the purposes of the DPB, anonymization is presumed to be possible, and the discussion here is on that basis.

The Central Government may direct any data fiduciary or data processor to provide any anonymized personal data or other NPD in order to enable **better targeting of service delivery** or to **aid evidence-based policy making** in a manner as may be prescribed. This obligation to share anonymized data is applicable to data fiduciaries and data processors alike. It must be kept in mind that it may not be practical for data processors to share data without instruction from data fiduciaries. It is unclear whether this data would have to be provided only to the State or to private parties as well; In addition, terms of the provision of such data, such as fair compensation, have not yet been specified. The DPB also reserves the power of the Central Government to frame policies for the promotion of the digital economy including for the handling of NPD including anonymized data.

Separate to the developments on the DPB, Ministry of Electronics and Information Technology has published an India Data Accessibility and Use Policy on February 21, 2022.[86] This policy seeks to address NPD that is available in the public sector and establish an access and sharing framework for such NPD which would include data created, generated, collected or archived by the Indian Government or its agencies.

viii. Extra Territorial Application

In addition to being applicable to the processing of personal data collected within the territory of India and collected by Indian citizens/companies; the DPB is designed to have extra territorial application.

Applicability of the DPB		**Processing**		**Data Principal (only Natural Persons)**	
		In India	Overseas	Located in India	Located overseas
Data Fiduciary / Processor	Located in India	✓	✓	✓	✓ Unless specifically exempted, such as in the case of outsourcing contracts.
	Located overseas	✓	✓ If in connection with any business carried on in India, or any systematic activity of offering goods or services to Data Principals within India; or in connection with any activity which involves profiling of Data Principals within India.	✓	X

86. https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022 (last accessed May 03, 2022).

The DPB does not define what would amount to 'carrying on business in India'. For reference, the Australian Privacy Principles without defining 'carrying on business' have interpreted it to generally involve conducting some form of commercial enterprise, 'systematically and regularly with a view to profit'; or to embrace 'activities undertaken as a commercial enterprise in the nature of an ongoing concern, i.e., activities engaged in for the purpose of profit on a continuous and repetitive basis'. While the Report of the Parliamentary Committee acknowledges suggestions to clarify this point, guidance on the interpretation of the phrase has not been included in the DPB.

The DPB has tried to ensure a balance between seeking to ensure the applicability of the DPB to the personal data of foreign residents processed in India, and at the same time has provided for exemptions, where necessary to promote data processing activities in India.

Section 2 of the DPB which sets out the applicability of the law, prescribes a territorial nexus with India for establishing jurisdiction for the purposes of the DPB - this could be on the basis of residence of the Data Principal, or the residence of the data fiduciary. If the data is processed by any person or entity within India, then the provisions of the DPB will apply. This could possibly go on to show that India is seeking to provide an equivalent level of data protection to the data of foreigners, hence increasing the chances of gaining 'data adequacy' status from jurisdictions such as the EU.

However, in view of the fact that India has a well-developed domestic data processing industry the Central Government has been given the power to exempt the processing of personal data of Data Principals located outside India by Indian data processors, if pursuant to a contract executed with a person outside the territory of India.

C. Major Obligations

i. Notice

The data fiduciary is obligated to provide a Data Principal with adequate notice prior to collection of personal data, either at the time of collection, or as soon as reasonably practicable (if the personal data is not directly collected from the Data Principal) (**"Notice"**). To fulfill the Notice requirement, certain key information is required to be provided to the Data Principal by the data fiduciary, such as:

- The purposes for which the data is to be processed;
- The nature and categories of personal data being collected;
- The right of the Data Principal to withdraw their consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; and
- information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable.

This Notice should be clear, concise and comprehensible and it is also specified that a Notice may be issued in multiple languages whenever necessary. However, the DPB is not clear as to when such multilingual notices may be necessary, and this may be specified through Codes of Practice.

From a practical implementation perspective, we note that the information required to be shared in a Notice is extensive, detailed and fairly granular. Some practical issues that are likely to arise are:

- Details about individuals and entities with whom such personal data may be shared is required to be provided upfront in the Notice itself. It is not clear whether the names of such entities are required to be disclosed or only the categories. We believe that the final law should clarify that broad categories should be sufficient as at the time of collection of the personal data the data fiduciary is unlikely to have access to the names of all entities who may process such personal data.
- The source from where such personal data is collected, is also required to be disclosed. Ascertaining the source in a complex data sharing architecture may get very difficult, especially where multiple group companies or related entities may be involved. Further, it may also result in notice fatigue amongst Data Principals, due to the multiplicity of Notice(s) that may need to be sent out by data fiduciaries.
- The DPA has been empowered to add to the list of items to be disclosed in the Notice. The DPA should exercise this power cautiously so as to ensure that the Notice does not contain granular details, so as to render the Notice too cumbersome, thereby compromising clarity and conciseness as required under the DPB.

ii. Purpose and Collection Limitation

Data fiduciaries processing personal data, are required to do so in a fair and reasonable manner so as to ensure the privacy of the Data Principal.

Data fiduciaries are permitted to collect only such personal data from that is necessary for the purposes of processing. Personal data may be may be processed only for (a) the purposes specified to the Data Principal under the consent Notice; or (b) any other incidental purpose that the Data Principal would reasonably expect the personal data to be used for, given the context and circumstances in which such personal data was collected, or (c) the purposes listed under the exceptions to consent in Clause 12 of the DPB. Therefore, using previously collected personal data for new (or previously unspecified) purposes would require additional consents from Data Principals.

iii. Storage Limitation

Personal data may be retained only until the purpose of collection is completed. Data fiduciaries should consider developing data retention policies, outlining the length of time they will hold on to the personal information of its users, as there is a positive obligation to delete such data in certain situations.

Data principals have the right to request the deletion of their personal data at any time. Compliance with such requests, require the data fiduciary to confirm the removal of such personal data from both its own systems, and those of any other companies who were processing the same data on its behalf. It must be noted that in a digital ecosystem, the feasibility of accurately confirming the complete deletion of data to the exclusion of any and all digital footprints, remains questionable.

iv. Transparency of Processing.

The DPB requires data fiduciaries to implement measures which facilitate and demonstrate transparency and accountability measures. These measures are intended to provide adequate information to Data Principals on the manner in which their data is being processed and also provide notification on data breaches.

The DPB requires data fiduciaries to provide the following information relating to their processing of personal data, in the manner as may be specified by regulations:

- Categories of personal data being collected.

- The purpose for which such personal data is being processed.
- Categories of data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm (as defined under the DPB).
- The existence of, and the procedures for the exercise of Data Principals' rights.
- Information relating to cross border transactions generally carried out by the data fiduciary.
- The Data Trust Score of the data fiduciary (wherever applicable).

The above list is not exhaustive, since the DPB also reserves the provision to add **'any other information as may be specified by regulations'.**

In addition to the above, the data fiduciary is also required to inform the Data Principal of 'important operations' in the processing of personal data. However, what constitutes 'important' has not been defined under the DPB and has instead been left to be specified through regulations.

D. Grounds for Processing PD and SPD

The DPB requires all personal data to be processed on the basis of consent obtained in accordance with Clause 11 of the DPB, with the exception of certain limited circumstances where personal data may be processed without consent.

i. Processing on the basis of consent

- The DPB lays down the test for 'valid consent' for personal data, i.e. consent which is free (as per the Indian Contract Act), informed (considering whether the information required under the notice provision has been provided), specific (considering whether the Data Principal can determine the scope of consent for the purpose), clear (indicated through affirmative action in a meaningful way) and capable of being withdrawn (considering the ease of withdrawal of such consent compared to the ease with which consent was granted).

  The consent requirements under the DPB would also require data fiduciaries to enable Data Principals to withdraw consent and request correction or erasure of the data.

- "Explicit consent" remains the only permissible ground for processing and transfer of SPD. "Explicit consent" has been defined as consent that is obtained in clear and specific terms without recourse to inference from conduct or context, and after informing the Data Principal of the purposes of processing activities which likely to cause significant harm, and providing the Data Principal with options to separately consent to the purposes of, operations in, and use of different categories of SPD. Obtaining explicit consent can prove to be impracticable or inappropriate in certain situations, such as in the case of processing SPD of employees, capture of biometric data such as video feed from security cameras – or in situations where such data is processed for fraud-detection, or for the purposes of complying with regulatory reporting requirements or court orders.

- In an attempt to make consent more meaningful and prevent its abuse, the DPB also provides that data fiduciaries cannot make the provision of their services / goods conditional on the consent of the Data Principal to collect and process personal data that is not necessary for the provision of the services / goods by the data fiduciary, and cannot be denied based on exercise of choice. Accordingly, in situations where such processing of personal data is necessary for the provision of services, a data fiduciary may require the provision of services to be premised upon obtaining the consent of the Data Principal. Considering the

increasingly complex nature of personalized services derived from processing of multiple fields of personal data, the determination of whether some personal data is necessary for the particular of specific services could become a complicated exercise based on the unique circumstances of each product or service in consideration.

- The DPB places the burden on the data fiduciary to demonstrate that consents obtained by it, adhere to the elements specified above. Under the current scheme of the DPB, discharging this burden will require a data fiduciary to prove the absence of coercion in obtaining consent. This goes against the basic principles of burden of proof.

Consent Manager:

The DPB has introduced the concept of 'consent managers', identified as data fiduciaries who will enable Data Principals to gain, withdraw, review and manage consent through "accessible, transparent and interoperable" platforms. These consent managers are to be registered with the DPA and will be subject to certain regulations as the DPA may specify.

The idea of 'consent managers' is innovative but relatively untested in practice for personal data, though to a certain extent, the "Account Aggregator" framework prescribed by the Reserve Bank of India (RBI), contemplates a similar role for Account Aggregators, requiring them to develop platforms that enable customers to manage consent and information across financial accounts and products. The underlying intention appears to be mitigation of 'consent fatigue' and providing greater awareness to the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on the implementation of the consent manager framework.

It appears from the role of the consent manager that they are supposed to be acting as a service provider to Data Principals to manage their consent. If that were the case, consent managers should not be categorized as data fiduciaries, or a separate category of data processors who may be subject to limited compliances. In order to qualify as data fiduciaries under the DPB, consent managers would have to determine the purpose and means for processing of data.

ii. Processing on grounds other than consent

Personal data may be processed without consent for specified grounds including:

- if processing is "necessary" for: (a) the performance of certain State functions (i.e., the provision of any service or benefit to Data Principal, or the issuance of any certificate, license or permit); or (b) "under any law" that is made by Parliament or a State legislature;
- for prevention, investigation or prosecution of any offence or any other contravention of any law;
- for compliance with court orders;
- in connection with legal proceedings;
- in connection with disasters or medical emergencies;
- for employment-related purposes (where the Data Principal is an employee of the Data Fiduciary);
- for journalistic purposes;
- for personal or domestic purposes;

- for classes of research, archiving or statistical purposes specified by the DPA; and,
- for reasonable purposes as specified by regulations issued by the DPA.

"Reasonable purposes" may include prevention of unlawful activity, credit scoring, recovery of debt, network and information security, among other items. These reasonable purposes may be specified after taking into consideration factors such as the legitimate interest of the data fiduciary in processing for that purpose, whether it is reasonably expected and practicable for consent to be taken, the degree of adverse effect of the processing activity on the rights of the Data Principal, and the reasonable expectations of the Data Principal having regard to the context of processing.

Although further clarity would be appreciated, a plain reading of section 12 indicates that SPD may be processed without consent on all the grounds specified above except employment-related purposes. The DPA is given the power to specify additional safeguards for the purposes of "repeated, continuous or systematic collection" of SPD for profiling.

With respect to the State's processing of personal data, the DPB grants fairly wide leeway to the State (see (i) and (ii) above). Ideally, State and non-State actors could have been treated at par in the DPB, to the extent that such treatment did not impede compelling State interests.

From the perspective of businesses, it is a welcome move that consent has been made a prominent ground for the processing of personal data and SPD. This has been done in spite of voices to the contrary suggesting the exclusion of consent as a ground altogether. The 'reasonable purposes' provision leaves discretion with the DPA to notify additional purposes for which consent may not be required to process personal data. However, contracts between parties has not been specifically identified as a ground for processing without express consent. As these grounds are to be specified by the DPA, there may be an opportunity for industries to make representations for additional grounds to be added.

E. Personal and Sensitive Personal Data of Children

Age of consent: The DPB mandates that parental consent will be necessary for the processing of personal data of children (i.e., persons below the age of eighteen years).

Obligations of Data Fiduciaries: Data fiduciaries are to verify the age of children and seek parental consent before processing their personal data.[87] Thus, the obligation to ensure age gating / verification and the necessary tools will have to be implemented by businesses. Age verification mechanisms are to be specified by regulations.

Bar on profiling/tracking children: Data fiduciaries are barred from undertaking activities such as profiling, tracking, behavioral monitoring, targeting advertising directed at children, or any form of processing that could cause significant harm to children.

This provision triggers when there is significant harm caused to children. While significant harm is defined, the interpretation of what encapsulates significant harm and who determines it is debatable.

These provisions may lead to practical implementation issues for the following reasons:

The DPB removes the concept of a "guardian data fiduciary" from the previous version and classifies all data fiduciaries processing children's personal data as SDFs. Additionally, the exemption from consent granted to counseling and child protection services from the previous version has been removed.

87. The only entities exempted from the parental consent requirement are those guardian data fiduciaries who provide exclusive counseling or child protection services.

There are certain platforms which are targeted / focused on young adults aged 14-18 such as casual gaming, education, or even specific video platforms. Seeking parental consent in each of these cases would not only be difficult but also impractical. While the Parliamentary Committee noted that stakeholders suggested that the age of children should be 13/14/16 years for the purpose of the definition, it did not adopt this recommendation.

Businesses catering to those below 18 might be affected. Education focused startups, who rely on targeted advertisements for example, may suffer due to the bar on processing of personal data of children. Similarly, audio / video streaming platforms may not be able to offer suggestions based on individual preferences. Importantly, emerging technologies such as AI, which are used as teaching aids may not be able to function as the profiling, tracking and behavioral monitoring of children will now not be allowed minus any exceptions to profiling or processing of data. Blanket restrictions such as this are likely to hinder effective service delivery to children, such as for educational purposes.

F. Rights of Data Principals: Right to Confirmation and Access / Right to Correction

The DPB provides detailed rights to the Data Principal to access and correct their data.

With regards to a right of review, the DPB grants rights to: (a) a confirmation about the fact of processing; (b) a brief summary of the personal data being processed; and (c) a brief summary of processing activities. Similarly, the right of correction has been developed in the DPB into a detailed step-wise process for how correction, completion or updating of the personal data should be done. The DPB also grants the right to request for erasure of personal data which is no longer necessary for the purpose for which it was processed.

In addition, the DPB also grants Data Principals, the right to access in one place and in a manner as may be prescribed via any regulations (a) the identities of all the Data Fiduciaries with whom their personal data has been shared; and (b) details as to the categories of their personal data which has been shared with such Data Fiduciaries, which seems quite onerous.

The DPB requires businesses to provide the Data Principal with summaries of the personal data being processed rather than the entire data dump. This may require some effort on the part of Data Fiduciaries.

G. Data Portability

In an attempt to grant users more control over their data, the DPB introduces a provision with respect to data portability, whereby Data Principals may seek from the Data Fiduciary, their personal data in a 'structured, commonly used and machine-readable format'. The DPB however does not specify the technical specifications of such a format, or what would be threshold for 'common use'.

The personal data to be provided to the Data Principal would consist of: (i) data already provided by the Data Principal to the Data fiduciary; (ii) data which has been generated by the Data fiduciary in its provision of services or use of goods; (iii) data which forms part of any profile on the Data Principal, or which the Data fiduciary has otherwise obtained.

Exemptions have been provided for instances where (i) the data processing is not automated; (ii) where the processing is necessary for compliance of law, order of a court or for a function of the State; and significantly, (iii)

where compliance with the request is technically not feasible.[88] The erstwhile exemption in the PDP Bill for data that reveals trade secrets has been omitted from this version of the law.

In relation to points (ii) and (iii) of the personal data to be provided to Data Principals above, following issues arise:

- **It is not clear whether this provision would include the passing of the 'ownership' or 'title' of the processed data to the Data Principal or mere transfer.**
- **It is not exactly clear as to what would constitute data which is 'generated' by the Data Fiduciary, which would also be in the nature of personal data? Would this extend to derivative data as well? This may result in digital businesses(s) having to forcibly share user information which may also include information / methodologies gathered by data analytics, with competitors. Hence, this may act as a disincentive for data technology innovation.**
- **It is also not clear as to what constitutes 'data which forms part of the profile of the Data Principal', especially the manner in which this 'profile data' would differ from personal data of the Data Principal.**

Crucially, the right to data portability may be exercised not only against SDF's but any Data fiduciary. This includes large platforms that collect personal data but also smaller companies and startups that may collect personal data for the purpose of improving their services. **While large platforms may be able to sufficiently comply with these requirements, it may be difficult for smaller companies who may not have the resources to spare from their core services.** For instance, major platforms are now introducing tools to enable transferring photos from one platform to another. But introducing the obligation to provide personal data in this format may be onerous for smaller companies, particularly when the standard of providing such personal data is not specified. **Standards that are "commonly used" differ between developers and the general populace may not be well versed with the technicalities of various formats. Besides, the purpose of seeking such data is also important. The format for a user wanting to inspect their personal data may be quite different from a format for a user wanting their personal data to move to a different service. Some of these practical issues are not adequately addressed by the DPB and need to be fleshed out more thoroughly.**

H. Right to be Forgotten

The DPB introduces a 'Right to be Forgotten'. **The right can be exercised by a Data Principal only through an order of an adjudicating authority who will determine the reasonability of the request for erasure.** This right appears to apply with regard to publishers or intermediaries who may be regarded as Data Fiduciaries, such as content streaming platforms, e-commerce platforms, aggregators etc.

A Data Principal can request for an order directing the Data Fiduciary to 'restrict or prevent continuing disclosure or processing of personal data'. **The DPB brings in the restriction to 'process' data under the Right to Be Forgotten, which may unnecessarily widen the scope of this right. As a general concept this right is meant to remove information from the public domain that is no longer relevant. Since 'processing' is a wider term, it may restrict data where it is used even in an anonymized form, or where it is irreversibly integrated with other data sets. However, it should be examined whether the exercise of the right to be forgotten should be subject to further restrictions such as processing as required under law.**

A Data Principal can request for an order directing the Data Fiduciary to 'restrict or prevent continuing disclosure or processing of personal data'. **The DPB brings in the restriction to 'process' data under the Right to Be**

88. The determination of technical feasibility has also been made subject to rules prescribed by the Central Government.

Forgotten, which may unnecessarily widen the scope of this right, which is meant to remove information from the public domain that is no longer relevant. Since 'processing' is a wider term, it may be restricting data where it is used even in an anonymized form, or where it is irreversibly integrated with other data sets.

Courts in India have adjudicated on the question of the right to be forgotten before in a number of instances.[89] Notably, the Madras High Court observed that it would be more appropriate to wait for the enactment of a Data Protection Act and rules thereunder to recognise and enforce a right to be forgotten. In this respect, enactment of this provision would be crucial.

The Right to be Forgotten is not absolute and is subject to the Data Principal showing that his/her right overrides (a) the right to freedom of speech and expression of any other citizen. (b) the right to information of any other citizen, or (c) the right to retain, use and process such personal data legally by a data fiduciary.

In addition, it is important to note that, the Supreme Court in **Justice K.S Puttaswamy v. Union of India**[90] has observed that the right to remain anonymous may form a part of the fundamental right to privacy. While there seems to be no conclusive ruling to this effect in India to this effect, in the United States, the right to publish anonymously is protected as part of the right to free speech. In the case **McIntyre v. Ohio Elections Commission,** the US Supreme Court said that **"Anonymity is a shield from the tyranny of the majority. . .. It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."** Similarly, even if it can also be argued that the right to speak anonymously is protected by Article 19(1)(a) of the Constitution of India, Article 19(2) provides that any restriction in the interest of security of the State is reasonable.

In any event, a Data Principal is empowered to request for erasure of personal data, which is no longer necessary for the purpose for which it was processed, and the storage period limitation requires personal data to be ordinarily be deleted once the purpose of processing has been achieved.

I. Data localization

The DPB provides that SPD may be transferred outside India, but a copy of the data should be stored in India. Further, certain CPD may be identified by the Central Government which should only be processed in India. Additionally, personal data may be freely transferred and stored outside India. The intention behind the DPB appears to be to make the data localization obligation applicable only for SPD belonging to Indian residents, however, this has not been made clear, as the data localization obligation applies generally to SPD under the DPB presently. One of the recommendations of the Parliamentary Committee is that the Central Government should, in consultation with sectoral regulators, prepare an extensive policy on data localisation encompassing broadly aspects such as: (i) the development of adequate infrastructure for the safe storage of data of Indians which may generate employment; (ii) introduction of alternative payment systems to cover higher operational costs; (iii) inclusion of systems to support local business entities and start-ups; (iv) promote investment, innovations and fair economic practices; (v) proper taxation of data flow; and (vi) creation of local AI ecosystem to attract investment and to generate capital gains.

The Parliamentary Committee also stated that the revenue generated from data location should be used for welfare measures in the country, especially to help small businesses and start-ups to comply with data localization norms, and that Government surveillance on data stored in India must be strictly based on necessity.

89. X vs. Https://www.youtube.com/watch?v=iq6k5z3zyso and ors. [Delhi HC - CS(OS) 392/2021]; Jaideep Mirchandani and Ors. vs. Union of India and Ors. [Delhi HC - W.P. (C) 8557/2021]; and Jorawer Singh Mundy vs. Union of India and Ors. [Delhi HC - W.P. (C) 3918/2021].

90. Judgment issued by the Supreme Court in Writ Petition (civil) No 494 of 2012, dated August 24, 2017.

A few concerns arise:

Mixed data sets: It is very likely that data will be collected and stored as a mixed data set, comprising of both personal data and SPD, and at times possibly even CPD. Since, it may be practically difficult to separate the SPD and CPD from such a data set, the entire data set would have to be stored locally, due to the element of SPD and CPD. For example, as stated earlier in the Indian context, surnames of individuals would demonstrate the caste / religion of Data Principals. This may result in data collected containing items of SPD, even though it was not intended.

CPD: The DPB does not give any guidance/examples on what data would compromise or be notified as CPD. Delegation of the right to determine / notify CPD to the Government without specific guidance under the DPB grants excessive powers to the Government in relation to DPB, which may not be preferable.

Data collected directly by foreign entities: It is to be determined whether data collected directly by foreign entities would be subject to the localisation requirement.

J. Cross Border Transfers

The DPB proposes that SPD may be transferred outside India only when:

a. The transfer is subject to a contract or intra-group scheme (for within group entities, similar to binding corporate rules) approved by the DPB in consultation with the Central Government,[91] or

b. The Central Government (in consultation with the DPB) prescribes a particular country or section within a country or a particular international organization (or class thereof) for which the transfer is permissible,[92] or

c. The DPB, in consultation with the Central Government, approves particular transfer(s) for a specific purpose.

SPD may be transferred outside India subject to either points (a) or (b) above being fulfilled (similar to personal data), and wherein the Data Principal has explicitly consented to such a transfer. The DPB however also empowers the Central Government to notify specific 'critical personal data' that may be transferred outside India, without restriction:

- To a party outside India engaged in provision of health services or emergency services and where the transfer is required for prompt action such as to respond to a severe medical emergency, provision of medical treatment or health services or to provide safety or assistance to individual during any disaster or break-down of public order (although, this transfer must be informed to the DPA within a period of time as prescribed), and
- A particular country or section within a country or a particular international organization prescribed by the Central Government for which the transfer is deemed permissible.

The DPB continues to retain restrictions upon cross-border transfer of personal data, SPD and CPD. However, several modes of cross-border transfer have now been made subject to decisions taken by the Central Government. For instance, the DPA is now required to consult with the Central Government prior to approving intra-group schemes or standard contractual clauses for cross-border transfers of SPD. Likewise, the transfer of SPD to a foreign government is prohibited without the approval of the Central Government.

---

91. The DPA may only approve standard contractual clauses or intra-group schemes that effectively protect the Data Principal's rights, including in relation to further transfers from the transferee of the personal data, and is not against public policy or State policy.
An act is deemed to be against public policy or State policy, if it promotes breaches any law, is against the relevant public policy or State policy, or has a tendency to harm the interest of the State or its citizens.

92. This would be subject to the Indian Government finding that the other country or section within a country or international organization shall provide for an adequate level of data protection for the personal data, as well as effectiveness of enforcement by authorities. Where SPD is being further shared to a third foreign government or agency, such sharing must be approved by the Indian Government.

It appears that the Central Government favors the use of approved clauses / schemes between the transferor and transferee, or specifically notifying certain countries / organizations that in its view, meets an adequate level of data protection and enforcement mechanism.

In addition, it is unclear as to whether the restrictions and compliances pertaining to cross border transfer of SPD would apply in the instance of direct collection of SPD of Indian Data Principals by Data Fiduciaries outside India, or if the restrictions may only apply to transfer of SPD from Data Fiduciaries in India (post collection from the Data Principal) to third parties outside India.

The explanation to what constitutes to be against public or State policy includes where an act has a 'tendency' to harm the interest of the State or its citizens. It is unclear as to how the term "tendency" is likely to be interpreted.

K. Breach notifications

A 'data breach' under the DPB includes breach of personal data as well as breach of NPD. While a breach of personal data is defined in respect of a particular Data Principal, a breach of NPD is defined as that which generally compromises its confidentiality, integrity or availability.

If there is a breach of personal data processed by the Data Fiduciary, the Data Fiduciary should notify the Data Protection DPB of such breach within 72 hours of becoming aware of the breach. The notifications should contain certain particulars, either submitted to the DPB together or in phases. **The data breach reporting is now mandatory (to be done within 72 hours) and is not subject to the result of any self-assessment by a Data Fiduciary.**

Further, while no reporting obligations have been included with regard to NPD breaches, the DPB contemplates the issuance of rules by the Government, for mitigating NPD breaches.

In case of a breach of personal data, the DPB may direct the Data Fiduciary to notify the Data Principal of such breach, undertake remedial actions and to post the details of the breach on its website after considering the personal data breach and the severity of harm to the Data Principal. The DPA may also direct the Data Fiduciary to adopt any urgent measures or remedy to mitigate harm to a Data Principal.

In case of a breach of NPD the DPA must take steps as may be prescribed later by the Government through subsequent rules.

It is unclear as to how the DPA will coordinate with specialised agencies such as the Computer Emergency Response Team (CERT-In) and the MeitY's Standardisation Testing and Quality Certification (STQC) which are currently vested with the responsibility of monitoring and mitigating the impact of data breaches, and testing and certifying hardware and software products. The DPB does not provide a general obligation for the DPA to consult with other sectoral regulators. However, the specification of appropriate actions required of data fiduciaries in the aftermath of a data breach, is included within the scope of subjects on which the DPA may issue or approve a Code of Practice. The DPA is required to consult with sectoral regulators in the development of a Code of Practice. It is therefore likely that the CERT-In would be consulted in the development of the relevant code of practice.

L. Significant Data Fiduciary

The DPB is empowered to notify certain Data Fiduciaries or entire classes of Data Fiduciaries as 'Significant Data Fiduciaries' (**"SDFs"**).[93] The concept of an SDF appears to stem from the attempt at identifying and regulating entities that are capable of causing significant harm to Data Principals as a consequence of their data processing activities.

Accordingly, the DPB proposes that such SDF register itself with the DPB and prescribes greater levels of compliances to be undertaken by such SDF, such as carrying out data protection impact assessments prior to significant processing activities, record keeping, independent data audits, and the appointment of a data protection officer.

The data protection officer appointed by an SDF is required under the DPB to be a senior level officer or a key managerial personnel[94] (in case of a company) or an equivalent employee (in case of other entities). The DPB also describes various functions of such a data protection officer including acting as the point of contact for redressal of grievances of Data Principals and advising the SDF on various compliances under the bill. The DPB also mentions that SDFs will be regulated by respective sectoral regulators.

In addition, the DPB requires any social media platforms[95] with users above a certain threshold as may be prescribed by the Government in consultation with the DPA, whose actions are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order; as well as Data fiduciaries who process data relating to children, or provide services to children are also included in the definition of an SDF. Such social media platforms are required to enable voluntary verification for its users in a manner that may be specified. It is not clear whether this will be specified by the DPA or the Central Government.

The factors to be taken into account for the notification of SDFs are quite subjective, leaving significant discretion with the DPA. Certain obligations like a data protection impact assessment prior to commencing data processing may slow down time-sensitive Big Data exercises and have a chilling effect on experimental processing activities.

As with the expanded definition of "harm", the inclusion of certain types of social media platforms within the definition of "significant data fiduciaries", appears to stem from concerns of harm arising from profiling. Social media platforms, whose actions are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of State or public order, have been designated as significant data fiduciaries. The inclusion of the phrase "electoral democracy" appears to acknowledge evidence of coordinated misinformation and voter manipulation campaigns run by third parties on major social media platforms in India and other jurisdictions.

The introduction of these provisions seems to stem from the broad purpose of the DPB as set out under the "Statement of Objects and Reasons". As per the "Statement of Objects and Reasons", the DPB seeks to bring

---

93. The Data Protection Authority may from time to time notify certain Data Fiduciaries (or class of Data Fiduciaries) as SDFs based on:
    a. volume of personal data processed;
    b. sensitivity of personal data processed;
    c. turnover of the data fiduciary;
    d. risk of harm by processing undertaken by the fiduciary;
    e. use of new technologies for processing;
    f. any social media platform with users above a certain threshold number as may be prescribed by the Government in consultation with the DPA, whose actions are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order;
    g. processing of children's data or providing services to them; or
    h. any other factor causing harm to any data principal from such processing.
94. Key managerial personnel under the DPB may be the Chief Executive Officer or the managing director or the manager, the company secretary, the whole-time director, the Chief Financial Officer, or any other personnel as prescribed.
95. A 'social media platform' is defined as "a platform who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services".

a strong and robust data protection framework for India and to set up an authority for protecting personal data and empowering the citizens' with rights relating to their personal data ensuring their fundamental right to "privacy and protection of personal data", as well as "ensure the interest and security of the State". While it is possible for social media platforms to make verification a part of their terms and conditions for users to register on the platform (which is a matter of contract between the platform and its user), a provision that mandates social media platforms to verify identities of its users and then identify their accounts as verified accounts may not be preferable, unless conclusively substantiated to be in the interest of security of the State. However, the current provision only prescribes voluntary verification of users. It is also important to note that anonymity may operate for at least two distinct levels – anonymity of the user with respect to the company that operates a platform, and anonymity of the user with respect to other users on the platform. The Government could consider requesting social media platforms to verify user accounts for the purpose of the company that operates the platform (in order to comply with law enforcement agencies, etc.) while allowing the users to retain anonymity with respect to other users on the platform.

The Parliamentary Committee also makes certain recommendations to hold social media platforms who do not function as intermediaries liable as publishers for the content on their platforms and posted via unverified accounts. While these recommendations do not find their way into the text of the law, these recommendations appear out of the scope of the DPB and may be subject to challenge.

M.Sandbox

The DPB has empowered the DPA to create a sandbox[96] in public interest for the purpose of encouraging innovation in Artificial Intelligence, Machine Learning or other emerging technologies.

Eligibility: Data Fiduciaries as well as start-ups whose privacy by design policies have been certified by the DPA are eligible to apply.

Application: Data Fiduciaries applying for inclusion in the sandbox will have to submit the term for which it intends to use the sandbox (which cannot exceed 12 months), the innovative use of technology, Data Principals participating, and any other information as may be specified by regulations.

Term: The maximum period a Data Fiduciary may use the sandbox is 3 years.

Exemptions: Participation in the sandbox will exempt the participating Data Fiduciary from certain obligations:

- To specify clear and specific purposes for collection of personal data;
- Limitation on collection of personal data;
- Restriction on retention of personal data; and
- Any other obligation under purpose and collection limitations under Sections 5 and 6 of the DPB.

The DPA is empowered to specify the penalties applicable to Data Fiduciaries participating in the sandbox, along with the compensation that can be claimed by Data Principals from such Data Fiduciaries. **From a reading of the DPB, it appears that no additional penalties would be applicable to such Data Fiduciaries other than those specified by the DPA.**

The DPA should keep in mind existing sectoral sandboxes while issuing these regulations.

96. The expression "Sandbox" has been defined to mean such live testing of new products or services in a controlled or test regulatory environment for the limited purpose of the testing. The DPA may also permit certain regulatory relaxations for a specified period of time.

N. Data Protection Authority

The DPB also contemplates the creation of an independent data protection authority (DPA). The DPA has been given a wide range of powers and responsibilities, which inter alia include:

- making regulations under the DPB,
- specifying the additional information to be included in a notice which the Data Fiduciary is required to provide to the Data Principal at the time of collection,
- specifying reasonable purposes of processing of personal data without consent,
- prescribing regulations in respect of processing of children's personal data,
- certification of privacy by design policy,
- approval of codes of practice,
- registration of 'consent managers',
- notifying entities as SDFs,
- taking steps as may be prescribed for data breaches, including personal data and NPD breaches; and
- undertake monitoring, testing and certification through a Government-verified agency to ensure ensure "integrity and trustworthiness" of hardware and software on computing devices in order to prevent any malicious insertion that may cause data breach.

The DPA also has the power to undertake actions that are crucial for a majority multinational corporate groups, such as the power to approve a contract or intra-group scheme by laying down conditions for cross-border transfer of SPD and CPD.

These functions are multi-faceted as they include powers and duties which are administrative, rule-making and quasi-judicial in nature. **The wide range and extent of delegation of legislative powers to the DPA appears to be excessive delegation of legislative powers to the DPA, which should be adequately addressed. The Parliamentary Committee Report recommends that the DPA should handle both personal data and NPD, which appears to be inappropriate and may lead to overlaps in jurisdiction.** Moreover, there appear to be inherent conflicts in the regulatory mandate vested upon the DPA. A review of the recommendations of the NPD Committee would suggest that the primary purpose of regulating NPD is to promote sharing of high-value NPD (including anonymised personal data) for the purposes of accelerating the growth of the digital economy. Should the DPA be vested with such a mandate by way of subordinate legislation, it would be in direct conflict with the DPA's mandate to ensure the security of personal data, and prevent re-identification of anonymised personal data - since greater sharing of NPD is likely to increase the risks of re-identification and subsequent misuse of anonymised personal data. The independence of the DPA is also debatable considering the proximity the DPA's composition has to the executive i.e. the Central Government. Further, many functions that were previously autonomous to the DPA has now been made subject to the view of the Central Government (e.g. approving intra-group schemes for cross-border transfer of SPD must be done in consultation with the Central Government). The Central Government also has been empowered to issue binding directions to the DPA (see section XVII below). This issue of lack of autonomy has also been raised by a few dissent notes submitted by members of the Parliamentary Committee.

O. Codes of Practice

The DPB contemplates codes of practice (similar to a self-regulatory mechanism) also to be issued by the DPA or approved by the DPA if submitted by an industry or trade association, an association representing the interests of Data Principals, any sectoral regulator / statutory authority or any departments of the Central or State Government.

These codes of practice should address more granular points of implementation including related to various compliances under the DPB, such as on notice requirements, retention of personal data, conditions for valid consent, purpose limitation, exercise of various rights by users, transparency and accountability measures, methods of destruction / deletion / erasure of personal data, breach notification requirements, cross-border data transfers, etc.

P. Privacy by design

Similar to the GDPR, the DPB stipulates that Data Fiduciaries implement a policy along the lines of a "Privacy by Design" principle.[97] Further, subject to regulations made by the DPB, Data Fiduciaries may submit their privacy by design policy to the DPB for certification, which upon examination / evaluation by the DPB or its authorized officer shall be certified to be in compliance with the requirements under the DPB. Such a certified policy has to be published on the website of both the Data Fiduciary and the DPA.

Hence, industry players would have to include privacy and its related principals as a part of their systems / architecture at the time of launching their business / operations itself, and not as an afterthought. However, the fact that the certification requirement from the DPA is not mandatory may ease the compliance burden overall.

Q. Power of the Government to issue directions to the DPA

The Government is empowered under the DPB to issue directions to the DPA in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order. The DPA is bound to abide by these directions but would be given an opportunity to express its views beforehand, as far as practicable.

The power to issue binding directions by the Government to the DPA was limited to questions of policy in the PDP Bill. This power of the Government has now been expanded widely allowing it to issue binding directions beyond just policy questions subject to certain grounds.

R. Exemptions

The DPB also has provisions that exempt certain kinds of data processing from its application.

Outsourcing

In what may be a welcome provision for the Outsourcing industry, the Central Government can exempt the processing of personal data of Data Principals that are not within the territory of India. This can be done in respect of processing by data processors who are contracting with foreign entities. Indian outsourcing entities processing foreign individuals' data therefore may be exempt from the provisions of the DPB.

97. The policy needs to contain/ specify (a) the organizational / business practices and technical systems in place to prevent harm to the Data Principal; (b) their obligations under the DPB; (c) certification that the technology used to process personal data is in accordance with commercially accepted / certified standards; (d) that legitimate business interests, including innovation are achieved without compromising privacy interests; (e) protection of privacy is ensured throughout the life cycle of processing of personal data (from point of collection to deletion); (f) personal data is processed in a transparent manner; and (f) the Data Principal's interests are accounted for at each stage of processing of personal data.

Indian captive units of foreign multinationals may look forward to availing this exemption as far as foreign individuals are concerned.

Government and public interest

With respect to the Government's own processing of information, the Central Government has the power, on various grounds of public interest,[98] to direct the inapplicability of any or all provisions of the Bill to any agencies of the Government, subject to safeguards which are to be prescribed by rules.

Notably, the grounds of discretion are fairly broad and allow the government significant leeway to provide exemptions from the application of the DPB, whereas civil society had expressed the hope that the DPB would ensure that Government's use of personal data would be restricted to necessary and proportionate instances. The dissent notes expressed by a number of the members of the Parliamentary Committee have also highlighted the liberal exemptions provided to the Government as a point of concern. Individuals will hence observe keenly whether the safeguards to be prescribed by rules under the DPB will meet the principles laid down by the Supreme Court in its 2017 Right to Privacy judgment.

The retention of this provision by the Parliamentary Committee has been objected to in separate dissent notes provided by 8 members of the Parliamentary Committee. The grounds for triggering the exemption are relatable to the reasonable restrictions on the freedom of speech and expression, as listed under Article 19(2) of the Indian Constitution. However, the possibility of an absolute exemption from all obligations of the DPB, may not fulfil the constitutional requirement for narrow tailoring of restrictions. While the revised provision clarifies that the exemption so granted would be subject to just, fair, reasonable and proportionate procedures, it is unclear whether this alone would remedy the widely worded scope of the exemption.

Processing of personal data in the interests of criminal investigation and prosecution, including "prevention", is also exempt from most provisions of the DPB. **Unlike the above provision, this exemption has not been conditioned with safeguards to be prescribed by rules. With law enforcement agencies gaining en masse access to biometric and facial recognition information, often cited to be in the interests of prevention of crime, civil society will have a significant concern on whether all such data is exempt from the safeguards in the DPB.**

Small businesses; personal/domestic purposes

Certain provisions, such as the requirement to provide notice, transparency and accountability, and rights of the Data Principal, are also inapplicable in the case of personal data processed by a 'small entity' where such processing is not automated. A small entity may be defined by the DPA after considering the turnover of the Data Fiduciary, the purpose of collecting personal data and the volume of personal data processed. This provision appears intended to cover small brick-and-mortar businesses.

Other exemptions

Exemptions from many provisions of the Bill are also granted in other circumstances in connection with judicial functions, legal proceedings, and research, archiving, and journalistic purposes.

S. Penalties, Offences and Compensation

The DPB contemplates various streams of enforcement: penalties to be paid to the Government, compensation to the Data Principal, as well as criminal liability in certain cases.

98. This may be done when the Central Government is satisfied that it is necessary to do so either (a) in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order; or (b) to prevent incitement to the commission of any cognizable offence relating to any of the grounds in (a) above.

i. Financial Penalties

The DPB follows the GDPR route in terms of financial penalties by not only proposing the imposition of financial penalties that may be prescribed, with the ceiling of INR 5 crore (approx. USD 655,982) or to 2% of the 'total worldwide turnover' of the Data Fiduciary in the preceding financial year for certain offences, and with the ceiling of INR 15 crore (USD 1,967,947) or 4% of the 'total worldwide turnover'. Penalties arise in a variety of cases: violation of processing obligations, failure to implement security safeguards, cross-border data transfers, and not taking prompt and appropriate action in case of a data security breach, among others. The term 'total worldwide turnover' not only includes the total worldwide turnover of the Data Fiduciary but also that of its group entities, if such turnover of the group entity arises as a result of processing activities of the Data Fiduciary.

ii. Criminal Penalties

The DPB prescribes criminal penalties for re-identifying de-identified data without appropriate consent. These criminal penalties are not limited to Data Fiduciaries or Data Processors, but 'any person', who knowingly, or intentionally reidentifies and processes personal data, and extend to imprisonment for a term not exceeding three years or a fine which may extend to INR 2,00,000 (approx. USD 2,624).

iii. Compensation

The DPB allows the Data Principal to seek compensation either from the Data Processor or the Data Fiduciary, for harm suffered as a result of any infringement of any provision in the law. Given some of the subjective provisions in the DPB and a specialized forum for redress, this may lead to a stream of data protection litigation.

iv. Class action

The DPB also appears to allow for the institution of class action by Data Principals who have suffered harm by the same Data Fiduciary or Data Processor. These Data Principals or an identifiable class of Data Principals can institute a representative application on behalf of all such Data Principals for seeking compensation for harm suffered as a result of any infringement of any provision of the DPB. These actions can be filed before the DPA which may then forward them to a designated officer.

T. Implementation Period

Elaborating on the recommended phased approach for implementation, the Parliamentary Committee suggested that the Chairperson and Members of DPA should be appointed within three months, the DPA commences its activities within six months from the date of notification of the Act, the registration of data fiduciaries should start not later than nine months and be completed within a timeline, and adjudicators and appellate tribunal should commence their work not later than twelve months, and the provisions of the Act shall be deemed to be effective not later than 24 months from the date of notification of this Act. However, the DPB does not include provision in this regard. It simply allows the Government to implement different provisions of the DPB at different times by way of notification.

U. Road Ahead

As next steps, we will need to wait and watch as to how the parliamentary proceedings unfold, and it is a possibility that the DPB may go through further changes before it is passed as law. Given that the Parliamentary Committee has deliberated this for about 2 years and provided more than 90 recommendations, it would not be amiss to open the DPB for public consultation and invite stakeholder comments.

In any event, irrespective of the course of legislative review adopted, the industry should start to focus on the development of Codes of Practice pertaining to subjects covered under the DPB. Given that the DPB continues to omit specific references to timelines for phased implementation, proactive engagement at this stage is likely to enhance the industry's preparedness for complying with the DPB as and when enacted.

5. Industry Impact

The proposed data protection law may have wide ramifications for industries which rely on the collection and processing of individuals' data. In pursuance of the same, we have pointed out below certain key impact points for select industries.

I. Pharmaceutical and Healthcare Industry

The pharmaceutical and healthcare industry consists of not only big pharmaceutical companies or hospitals but also small clinics, fitness apps, nursing homes, diagnostic centers, test centers and med-tech start-ups that rely on technological developments to provide medical and health-related services to customers. However, the DPB clubs all these entities into one bucket – in terms of compliance.

Further, industry specific laws and guidelines have been proposed to regulate specific aspects of collection and processing of sensitive data, such as the draft HDM Policy. The final version of this policy and its implementation is left to be seen.

The DPB classifies health data, genetic data and biometric data as SPD. Hence small businesses such as startups building fitness apps, standalone gyms, dieticians, chemists etc. by virtue of collecting and processing certain data now would need to comply with various obligations laid down under the law including taking explicit consent and possibly comply with the obligations placed on an SDF (if classified as one).

Notably, the DPB provides an exemption to seeking consent for the processing of PD and SPD if such processing is necessary to respond to medical emergencies, to provide medical treatment or health services. Further, cross border transfer of PD or SPD (when notified by the Central Government) may be transferred outside India in the event of necessities or emergencies.

II. Banking, Finance Services and Insurance Industry

The definition of 'financial data' under the DPB includes account numbers and credit/debit card, and payment instrument numbers of data principals. In the current legal landscape where, sufficient safeguards exist to prevent fraud, for instance, by way of additional factor of authentication processes for Card Not Present transactions as well as PINs for credit/debit card transaction, the possibility of misuse of mere account numbers and credit/debit card numbers is significantly low. Therefore, the heightened obligations that come with the collection of SPD would be applicable to a significant number of players in the BFSI space. For instance, fintech companies that save user's credit card numbers (but not CVV) on the platform for ease of convenience would be subject to additional compliances applicable for SPD.

Another significant development is the recent RBI notification on Storage of Payment System Data that mandated that the entire data relating to payment systems operated by authorized entities must be stored in a system only in India. The circular however provided some respite by allowing for the storage of data that relates to the foreign leg of a transaction in a foreign country.

The RBI prohibits merchants and payment aggregators from storing customers' card data and requires that existing data be purged from their systems by 30th June 2022. However, the last 4 digits of the actual card number and card issuer's name can be stored for transaction tracking and reconciliation purposes. This data could also

be deemed as 'financial data' under the DPB and the corresponding heightened obligations may then apply on merchants and payment aggregators.

III. Media and Advertising Industry

The proposed law would apply to the media and entertainment industry as well, including production houses, talent, talent agencies, distributors, digital platforms, and various suppliers and service providers in the ecosystem. Unlike the existing data protection law which applies to electronic and online businesses, the proposed law will apply to both online and offline businesses.

The DPB implements certain restrictions when processing the data of a 'child', or an individual under eighteen years of age. There may be certain restrictions on data fiduciaries such as a bar on the profiling, tracking or behavioral monitoring of, or targeted advertising directed at children; or other processing that has a risk of causing significant harm to the children. Such restrictions could affect the business models of those centered around creating/distributing content for children.

Further, media companies may only be able to collect data from data principals that is necessary for the purposes of processing; and the processing of data may be done only for the purposes specified to the data principal, or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for. For example, production houses must be careful to only use collected data for purposes required for the task at hand (or for an incidental purpose) from the talent that they engage. For instance, a streaming service may not be permitted to use personal data collected from the users for any purpose related to their other businesses (such as merchandise, experience centers etc.) unless they are able to show that the purpose is necessary for processing and necessary consent has been taken for such processing.

Streaming services and OTT content providers, and even gaming platforms may be required to take explicit consent to provide personalized content, in-app purchases or undertake digital marketing. Children-oriented platforms may also need to build age verification mechanisms and processes to take parental consent.

E-commerce websites would find the data localization and mirroring requirement of sensitive personal data especially relevant.

IV. Technology Industry

The technology industry may be impacted by the DPB on a number of aspects. For instance, the restrictions on cross border transfers of data along with the proposed data portability laws may be hurdles for the industry.

Sensitive personal data can be processed outside India but at least one copy of all sensitive personal data is to be stored on a server or a data center located in India. There are no restrictions on the processing and storage of personal data. For instance, businesses such as digital platforms, cloud service providers, AI and machine learning service providers etc. whether Indian or offshore, processing sensitive personal data of Indian users, may need to store a copy of such data in India. Furthermore, to comply with the localization requirement in day-to-day operations, it may be practically and operationally difficult to segregate PD and SPD from large buckets of data to store a copy in India.

In order to bring in the seamless transition for users from one platform to the other, the proposed law provides for a data portability concept. Based on a request from a user, technology / internet companies may have to provide to the user or transfer to another platform in a structured and machine-readable format: information that is not

restricted merely to the data provided by the user. This may result in a digital platform having to forcibly share with rival platform(s) user information which may also include information / methodologies gathered by data analytics. A competitor, on receiving such information, could utilize reverse engineering techniques to reveal the algorithms, proprietary techniques, and know-how used in data analysis and user profiling. This should overall benefit a user in terms of the new platform offering a bespoke experience but may also act as a disincentive for data technology innovation.

V. Social Media Intermediaries

Since the enactment of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,** social media intermediaries which are designated as 'significant social media intermediaries' are subject to certain additional compliances including appointment of key officers, reporting requirements, deployment of technology-based measures to monitor content and removal of content. The DPB also provides for designation of social media platforms as SDFs based on certain parameters and imposes additional compliances on them including to enable voluntary verification for its users. The Report recommends that social media platforms who do not function as intermediaries must be held liable as publishers for the content on their platforms posted via unverified accounts. This may lead to excessive regulation of social media platforms by the DPB on entities which are already being regulated under a separate framework. Moreover, questions may also arise on the scope of the DPB, a law meant for data protection and privacy, being extended to social media regulation.

VI. Industry stakeholders processing non-personal data

The DPB allows the Central Government to direct any data fiduciary or data processor to provide any anonymized personal data or other NPD in order to enable better targeting of service delivery or to aid evidence-based policy making. Data processors, bound by the instructions of data fiduciaries, may not be at liberty to freely share such non-personal data. There is also no clarity on the policy framework within with any NPD requisitioned will be processed by the Government. However, one can wait for the Central Government to frame policies for handling of anonymized data, which it is empowered to do so under the DPB.

6. Tax Considerations on The Draft Data Protection Law

Despite disparate regulations being issued in a haphazard manner, the one common policy push appears to be towards a mandatory data localization requirement in India. Amidst the frenzy of various reactions to localisation, the incidental tax risk due to localisation is set to become larger in the future.

Some of the key risks are below:

- Firstly, the requirement of mandatory storage of data on a server or data center in India could potentially form the basis to tax income of a foreign company in India due to the creation of a server permanent establishment (**"PE"**).[99] As a consequence, the tax department may seek to tax all income derived by that foreign company from India at a tax rate of 40%.[100] The exposure to tax would typically depend on the level of control the foreign company would exercise over the server in India in which data is stored. It would also depend on the role of the server in the larger business of the company and whether it forms a core part or not. Until recently, such risks were normally mitigated if the server was owned and operated by an Indian service provider or by an Indian subsidiary of the data controller. However, courts in recent times have held (e.g. recent AAR ruling in the MasterCard case[101]), that if operational control is vested with the foreign entity, it would create taxable nexus in India irrespective of ownership of the server. Therefore, going forward companies would have to be careful about the manner in which they choose to comply with data localization requirements. While for the data protection law, companies may want to exercise control, it could lead to unintended tax exposures.

- That said, even if a server PE were to be created in India, it has traditionally been understood to be a low level function of mere storage as the value addition in the business happens offshore. In such cases, India should not be able to tax a significant portion of the income of the foreign company since it is settled position that the income that can be subject to tax to a PE is only proportionate to the activities carried out in India.[102] However, if profits are sought to be attributed to such Server PE based on the number of users or amount / manner of collection and usage of data, this may give rise to significant tax risks for digital businesses. In fact, the recent amendments to the Income Tax Act, 1961, have expanded the concept of significant economic presence (SEP) and expressly stated that income derived from data collected in India shall be attributable to and taxable in India. More specifically, sale of data and sale of services or goods through use of data will amount to SEP, as most companies use data to target their customers and increase their sales.

  Further, information sharing between the DPB and tax authorities may paint a clearer picture for the tax authorities in terms of the data flows within or across groups and borders. For instance, Section 34 of the DPB,[103] states that a transfer can only be made pursuant to an Intra-group scheme that is approved by the data protection authority. Further, the Central government may not approve the transfer after consulting with the Data Protection Authority if such transfer shall not prejudicially affect the enforcement of relevant

99. Government of India has expressed its reservation on the issue of whether a fixed server should be required in order to constitute a virtual PE stating (in its reservation to the OECD Commentary to the Model Tax Convention) that a "website may constitute a permanent establishment in certain circumstances". However, Indian courts, having taken this into consideration, have observed that the effect of these reservations is merely to reserve a right to set out the circumstances in which a website alone can be treated as PE; and have therefore, reiterated the OECD principles on PE (see Income Tax Officer v. Right Florists, [2013] 25 ITR(T) 639 (Kolkata - Trib).

100. Excluding surcharge and cess.

101. A.A.R. No 1573 of 2014.

102. Article 7 of the OECD Model Tax Convention provides that profits an enterprise that carries on business in another country through a permanent establishment may be taxed in that country, but only so much of them as is attributable to that permanent establishment. This principle has been upheld numerous times by the Indian judiciary.

103. Section 34, DPB.

laws by authorities with appropriate jurisdiction. This portion of Section 34 is extremely relevant, as the Data Protection Authority can use this information to supplement investigations by other authorities if the Central government feels it is necessary for law enforcement.[104] This section would definitely be used by tax authorities as the flow of data through intra-group schemes can show the level of participation and the volume of data being transferred at each stage, which may help the tax authorities determine how strong their digital presence in India.[105] Recently, the Government has also passed legislation focusing on the tracking and taxing of Virtual Digital Assets, which are defined very broadly to cover data as well subject to certain conditions. While in principle Data under the DPB and VDAs should be separate, in practice it remains to be seen if there is any unintended overlap that creates tax consequences.

- Secondly, given that the DPB is intended to have extra territorial application it is likely to give rise to tax risks when implemented. For example, the Draft Data Protection Bill categorizes a class of Data Processors engaging in high risk data processing as SDFs. The DPB specifically requires that even off shore SDFs would need to appoint a data protection officer, who shall be based in India and, who must represent the data fiduciary in compliance of obligations under this Act. Should such officers of the data fiduciary contractually have the power to bind the foreign data fiduciary then there is a risk of the formation of an agency permanent establishment in India, thereby leading to tax consequences. In fact, due to recent amendments to the tax treaties, even if the data officer in India is construed as conducting activities in India that support the foreign enterprise in providing services in India then an agency PE could be created.

- Thirdly, over the last few months' tax authorities are increasingly trying to attribute more value to Indian operations of foreign companies in transfer pricing proceedings. This includes taking a position that the collection of data is a significantly valuable activity without any basis to justify the same. Such an approach also ignores the fact that raw data by itself is not useful and requires much processing and analysis to be of value. In fact, it is arguable that it is the secondary data that is generated from cleaning up and analysing data collected from customers or users is much more valuable and therefore majority of the taxes should not be payable in India merely on the basis that the data is collected or stored in India. Therefore, the form and manner of existing cross border data flows would need to be re-examined in light of the proposed law as well as judgments on this point.

It is clear that the various policies that are proposed to be introduced including the DPB are likely to have far reaching effects on business models, however, the need for a tax impact assessment before laws are introduced has become the need of the hour. The Government should not approach this topic in a siloed manner and rather adopt an interdisciplinary approach keeping in mind the collateral impact on Indian start-ups and companies, which would also have to comply with such onerous requirements. Given that the Government is taking steps to reduce the amount of tax litigations unintended consequences as those arising out of the draft law would inevitably result in litigation and must therefore be addressed at a policy level before they are introduced as law.

104. Id.

105. Explanation 3A of section 9(1)(i) of the Income-tax, Act, 1961: "ii) Sale of data collected from a person who resides in India or from a person who uses internet protocol address located in India; and iii) Sale of goods or services using data collected from a person who resides in India or from a person who uses internet protocol address located in India.."

7. India Taking A Leaf from The GDPR Book

The DPB draws inspiration from the European Union's General Data Protection Regulation (**"GDPR"**) in multiple instances. A comparison between the DPB and the GDPR is as follows:

Extra-Territorial Application	The law applies to organizations outside the EU, where the processing activities are related to: (a) the offering of goods or services, or (b) the monitoring of their behavior as far as their behavior takes place within the EU.[106]	Similar to the GDPR, the DPB has extra-territorial applicability, where the law extends to processing outside India only if such processing is (a) in connection with any business carried on in India / systematic offering of goods or services; or (b) in connection with any activity which involves profiling of Data Principals within the territory of India.[107]
Personal / Sensitive Personal Data	'Personal data' has been defined as any information relating to an identified or identifiable natural person. The GDPR further prohibits the processing of certain special categories of personal data unless specified conditions are satisfied – such as the provision of explicit consent, and the necessity of processing.	Unlike the GDPR, the bill has categorized data into categories of personal data,[108] SPD,[109] CPD,[110] as well as NPD.[111] While the DPB provides for certain compliances and restrictions for processing personal data, the processing of sensitive personal data is at a higher standard, similar to conditions as provided for in GDPR. Compliances regarding CPD, as with SPD, are also at a higher standard.
Notice	Where personal data relating to a data subject is collected from the data subject, the controller shall, at the time when personal data is obtained, provide the data subject with certain information.	Similar to the GDPR, the Data Fiduciary is obligated to provide a Data Principal with adequate notice prior to collection of PD either at the time of collection of the PD or as soon as reasonably practicable if the PD is not directly collected from the Data Principal. This notice should be clear, concise and comprehensible and specifies that a Notice may be issued in multiple languages whenever necessary.
Lawfulness of Processing (Consent Requirement)	In addition to allowing processing of personal data under consent (along with exceptions to this rule), the GDPR allows the processing of personal data when it is necessary for the performance of a contract, and for the purposes of legitimate interests of the controller.	While the DPB allows the processing of PD under consent (along with exceptions to this rule), the DPB does not allow for the processing of PD if necessary for the performance of a contract, or for the purposes of legitimate interests of the Data Fiduciary.
Certification of data protection levels	The establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.	Data fiduciaries may also elect to seek certification from the DPA for the privacy-by-design policies, in which case the policy would be published on both the data fiduciary's and the DPA's website. However, unlike GDPR, the DPB allows the DPA to devise a framework and authorize an appropriate agency to monitor, test and certify hardware and software.

106. Article 3, GDPR

107. Section 2, DPB.

108. "Personal data" has been defined as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

109. SPD has been defined to include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief, etc.

110. The DPB provides that critical personal data may be notified by the Government at a later point of time.

111. "Non-personal data" is defined as data other than personal data.

7. India Taking A Leaf from The GDPR Book

Data Localization	There is no data localization requirement in the EU.	One copy of all and sensitive personal data needs to be stored in India and certain data classified by the government as 'critical personal data' needs to be stored in India only and cannot be transferred outside India.[112]
Cross Border Transfers	Transfer of data outside the EU may be permitted if certain conditions are met by the parties transferring and receiving the data; and it is classified by the European Commission as a jurisdiction that provides an adequate level of data protection.	Transfer of SPD outside India may be permitted if there is (a) a regulator-approved contract or intra-group scheme for the transfer, or (b) a regulator-approved transferee entity or country. Further, such transfers must be explicitly consented to. CPD may be transferred outside India only with the permission of the Central Government on certain prescribed grounds.
Right to Erasure / Right to be Forgotten	The GDPR introduces a right for individuals to have personal data erased as part of the Right to be Forgotten.	The Right to be Forgotten has been provided for in the DPB, but in a limited form, where it is not a right to erasure per se, but the Data Principal will have the right to restrict or prevent continuing disclosure of the data, if approved by the Adjudicating Officer.
Data Portability	The GDPR provides for data portability. However, derived or inferred data (such as by personalization or recommendation process, user categorization or profiling) from the personal data of the user does not appear to fall within the ambit of data portability and need not forcefully be transferred from one organization to another.	Based on a request from a user, Data Fiduciaries may have to provide to the user or transfer to another platform: information provided by the user, information generated during the use of services or goods by the user, data which forms part of the profile of the user, or which they have otherwise obtained. It is ambiguous whether this may include derived data.
Child Rights	A child is defined as an individual below 16 years of age. For processing data of a child, consent will have to be taken from the parents or guardians of the child.[113] Specific protection is mandated with regard to the processing of child data, which extends to restrictions on profiling and monitoring.	A child is defined as an individual under 18 years of age. In order to process data of a child parental consent is required. Profiling, tracking or behavioral monitoring of or targeted advertising towards children by Data Fiduciaries may not permitted.
Penalties	The maximum penalty up to 4% of global turnover or 20,000,000 euros (approx. USD 23,061,000) whichever is higher will be imposed in situations of non¬compliance such as the violation of basic principles such as in relation to processing, consent, data subject rights, and cross border transfers.[114] Further, only civil offences appear to have been prescribed.	The maximum penalty up to 4% of global turnover or INR 150,000,000 (approx. USD 1,967,947) whichever is higher will be imposed in situations of non-compliance such as the wrongful processing of personal and sensitive personal data, the data of children, as well as non-compliance of security safeguards.[115] Further, both civil and criminal offences (for certain offences) have been prescribed.

112. Section 33, DPB.
113. Article 8, GDPR.
114. Article 83, GDPR.
115. Section 57, DPB.

8. Road Ahead

The importance of data is ever increasing, and exciting times lie ahead. Data is no longer looked at as an intangible commodity but rather as an asset on which further value can be derived. Both consumers as well as organizations see value in data, its usage and security. After numerous variations of a draft data protection bill and multiple consultations by the Joint Parliamentary Committee, one will have to wait and watch for the final version of the DPB. We may even see the DPB passed by the Indian Parliament in the near future.

However, irrespective of a general data protection law coming into force for which the process is driven by the Central Government, sector regulators have been very active in regulating of data, including introducing sectoral data localization requirements, in their specific industry segments such as banking (the RBI's restrictions on card data storage is an example), insurance, telecommunication and healthcare (the draft HDM policy). Even MeitY has issued directions separately for notifying cyber security incidents, independent of what breach notification requirements may be introduced by the DPB.

Going forward, business models, will not only have to keep up with industry and sector-wise regulations, but will also need to factor the general data protection law, once enforced.

The following research papers and much more are available on our Knowledge Site: www.nishithdesai.com

Digital Health in India

March 2022

Social Finance

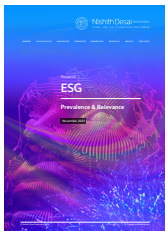
February 2022

The Indian Pharmaceutical Industry

February 2022

Regulations on E-Wallets, Gift Cards and Vouchers Given a Facelift

January 2022



ESG

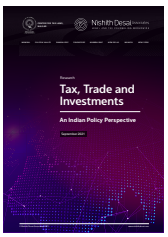
November 2021

The Global Drone Revolution

November 2021

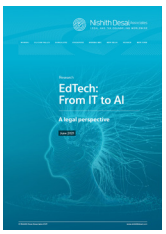
The Future of mobility

September 2021



Tax, Trade and Investments

September 2021



EdTech: From IT to AI

June 2021

NDA Insights

TITLE	TYPE	DATE
Employment Generation in India: Prioritise Service Sector - If Speed is the Essence	HR Law	April 2022
India's New Labor Codes - Reduced Direct Liability of Directors?	HR Law	April 2022
New Labour Codes In India Delayed	HR Law	April 2022
Climate Change Disputes Series (I) - An Overview	Dispute Resolution	April 2022
Put Option Enforced: Conflict With Indian Exchange Control Laws Not A Ground For Setting Aside The Award In Singapore	Dispute Resolution	March 2022
English High Court's Guide On Litigation Privilege And Waiver Of Privilege	Dispute Resolution	March 2022
What Does Liberalisation Of Drone Laws Mean For The Pharmaceutical Industry?	Technology Law	March 2022
The Rbi Stand On Crypto Lacks Balance	Technology Law	March 2022
The Data Protection Bill: In Search Of A Balanced Horizontal Data Protection Framework	Technology Law	March 2022
Gift City's Gift- Welcome Foreign Universities	Education Sector	March 2022
Decoding The Ugc And Aicte's Notices On Franchising And Mis-Advertising For Online Degree Programmes	Education Sector	January 2022
Education Regulatory And Legal Update: Year 2021 In A Wrap	Education Sector	January 2022
Regulatory Yearly Wrap 2021: Pharmaceuticals In India	Pharma & Healthcare	December 2021
Regulatory Yearly Wrap 2021: Medical Device In India	Pharma & Healthcare	December 2021
Regulatory Yearly Wrap 2021: Healthcare In India	Pharma & Healthcare	December 2021

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.

Our dedication to research has been instrumental in creating thought leadership in various areas of law and public policy. Through research, we develop intellectual capital and leverage it actively for both our clients and the development of our associates. We use research to discover new thinking, approaches, skills and reflections on jurisprudence, and ultimately deliver superior value to our clients. Over time, we have embedded a culture and built processes of learning through research that give us a robust edge in providing best quality advices and services to our clients, to our fraternity and to the community at large.

Every member of the firm is required to participate in research activities. The seeds of research are typically sown in hour-long continuing education sessions conducted every day as the first thing in the morning. Free interactions in these sessions help associates identify new legal, regulatory, technological and business trends that require intellectual investigation from the legal and tax perspectives. Then, one or few associates take up an emerging trend or issue under the guidance of seniors and put it through our "Anticipate-Prepare-Deliver" research model.

As the first step, they would conduct a capsule research, which involves a quick analysis of readily available secondary data. Often such basic research provides valuable insights and creates broader understanding of the issue for the involved associates, who in turn would disseminate it to other associates through tacit and explicit knowledge exchange processes. For us, knowledge sharing is as important an attribute as knowledge acquisition.

When the issue requires further investigation, we develop an extensive research paper. Often we collect our own primary data when we feel the issue demands going deep to the root or when we find gaps in secondary data. In some cases, we have even taken up multi-year research projects to investigate every aspect of the topic and build unparallel mastery. Our TMT practice, IP practice, Pharma & Healthcare/Med-Tech and Medical Device, practice and energy sector practice have emerged from such projects. Research in essence graduates to Knowledge, and finally to **Intellectual Property.**

Over the years, we have produced some outstanding research papers, articles, webinars and talks. Almost on daily basis, we analyze and offer our perspective on latest legal developments through our regular "Hotlines", which go out to our clients and fraternity. 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 Lab Reports 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 articles and disseminate them through our website. Our research has also contributed to public policy discourse, helped state and central governments in drafting statutes, and provided regulators with much needed comparative research for rule making. Our discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged. Although we invest heavily in terms of time and expenses in our research activities, we are happy to provide unlimited access to our research to our clients and the community for greater good.

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 eco-system 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 your suggestions on our research reports. Please feel free to contact us at **research@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
Fax +91 22 6669 5001

SILICON VALLEY

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

Tel +1 650 325 7100
Fax +1 650 325 7300

BANGALORE

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

Tel +91 80 6693 5000
Fax +91 80 6693 5001

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
Fax +91 22 6159 5001

NEW DELHI

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

Tel +91 11 4906 5000
Fax +91 11 4906 5001

MUNICH

Maximilianstraße 13
80539 Munich, Germany

Tel +49 89 203 006 268
Fax +49 89 203 006 450

NEW YORK

1185 Avenue of the Americas, 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 & Data in India: Fostering the World's Digital, Innovation and Outsourcing Destination

Legal, Ethical and Tax Considerations & Comparative Notes to the GDPR

Please reach out to: privacy.nda@nishithdesai.com