Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

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

Privacy & Data: India's Turn to Bat on the World Stage

Legal, Ethical and Tax Considerations

July 2020

Privacy & Data: India's Turn to Bat on the World Stage

Legal, Ethical and Tax Considerations

July 2020

ndaconnect@nishithdesai.com

DMS Code: 9000-5043.

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 to 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.

Accolades

A brief chronicle of our firm's global acclaim for its achievements and prowess through the years –

- **Legal500:** Tier 1 for Tax, Investment Funds, Labour & Employment, TMT and Corporate M&A *2020, 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012*
- **Chambers and Partners Asia Pacific:** Band 1 for Employment, Lifesciences, Tax and TMT *2020, 2019, 2018, 2017, 2016, 2015*
- **IFLR1000:** Tier 1 for Private Equity and Project Development: Telecommunications Networks. *2020, 2019, 2018, 2017, 2014*
- **AsiaLaw Asia-Pacific Guide 2020:** Tier 1 (Outstanding) for TMT, Labour & Employment, Private Equity, Regulatory and Tax
- **FT Innovative Lawyers Asia Pacific 2019 Awards:** NDA ranked 2nd in the Most Innovative Law Firm category (Asia-Pacific Headquartered)
- **RSG-Financial Times:** India's Most Innovative Law Firm *2019, 2017, 2016, 2015, 2014*
- **Benchmark Litigation Asia-Pacific:** Tier 1 for Government & Regulatory and Tax *2019, 2018*
- **Who's Who Legal 2019:**
  Nishith Desai, Corporate Tax and Private Funds – Thought Leader
  Vikram Shroff, HR and Employment Law- Global Thought Leader
  Vaibhav Parikh, Data Practices - Thought Leader (India)
  Dr. Milind Antani, Pharma & Healthcare – only Indian Lawyer to be recognized for 'Life sciences-Regulatory,' for 5 years consecutively
- **Merger Market 2018:** Fastest growing M&A Law Firm in India
- **Asia Mena Counsel's In-House Community Firms Survey 2018:** The only Indian Firm recognized for Life Sciences
- **IDEX Legal Awards 2015:** Nishith Desai Associates won the "M&A Deal of the year", "Best Dispute Management lawyer", "Best Use of Innovation and Technology in a law firm" and "Best Dispute Management Firm"

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 ndaconnect@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

Inika Charles
inika.charles@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 per a 2019 UNCTAD Report, the size of the digital economy ranges from 4.5% to 15.5% of the world GDP.[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 Bill has on December 12, 2019 been referred to a joint parliamentary committee for further debate and examination.

One cannot deny that India has also looked over its shoulder at the EU and the recently introduced 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 PDP Bill. Hence, there may be certain deviations and incremental changes at an organizational and technological level to implement the PDP Bill, 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.

Even prior to the release of the PDP Bill, the Government of India constituted[2] a committee headed by Kris Gopalakrishnan of Infosys to explore the governance of 'non-personal data'; whose recommendations are yet to be released.

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. UN Conference on Trade and Development (UNCTAD) - Digital Economy Report 2019, available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf?user=46 (last accessed April 28, 2020).

2. Constitution of Committee of Experts to deliberate on Data Governance Framework, September 13, 2019, available at https://meity.gov.in/content/constitution-committee-experts-deliberate-data-governance-framework (Last accessed December 9, 2019).

1. Summary and Chronology of Privacy Developments in India

I. Information Technology Act, 2000 Enacted – October 2000

The *Information Technology Act, 2000* (**"IT Act"**) was the first law enacted in India which contained provisions on confidentiality, privacy and security for information stored in a computer resource. In 2011, the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (**"Data Protection Rules"**) were enacted under the IT Act to protect sensitive personal data and information collected from individuals by body corporates.[3] These rules make up the existing general data protection framework in India.

II. WhatsApp User Policy Challenged - September 2016

In a Delhi High Court case, WhatsApp's policy which allowed it to share user data with Facebook was challenged. The High Court upheld the policy but ordered the deletion of user data of those who had opted out of the service. The Court also ordered WhatsApp not to share information which was collected prior to the updated user policy coming into force.[4] This case has since been challenged and is currently pending before the Supreme Court of India.

III. Right to be Forgotten Recognized by High Courts in India - January 2017

The first case in India to deal with the concept of the right to be forgotten was heard in the Gujarat High Court. While the Court didn't per se recognize the 'right to be forgotten'; the case arose as the petitioner had filed a case for the removal of a published judgment in which he had been acquitted. The Court disposed of this case as the petitioner had not been able to point out specific provisions of law that had been violated.[5]

There was also a Karnataka High Court decision which made references to the *"trend in the Western countries"* where they follow the *"right to be forgotten"* in sensitive cases. This Case was filed to remove only the name of the Petitioners daughter from the cause title as it was easily searchable and would cause harm to her reputation. The Court held in the Petitioner's favor, and ordered that the name be redacted from the cause title and the body of the order.[6]

IV. Supreme Court Recognized a Fundamental Right to Privacy - August 2017

The Supreme Court in the landmark decision of *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors.*[7] recognized that a fundamental right to privacy exists under the Constitution that is enforceable against the

3. '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.
4. Karmanya Singh Sareen v. Union of India, 233(2016) DLT436.
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. Supreme Court, Writ Petition (Civil) No 494 Of 2012.

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.[8] Further, the Court also asked for a data protection law to be framed to protect individual's rights against privacy parties.

V. Data Localization Mandate issued by the Reserve Bank of India - April 2018

The Reserve Bank of India (**"RBI"**) released a notification on the storage of payment system data,[9] 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.

VI. Aadhaar Declared Constitutional by the Supreme Court - September 2018

The Supreme Court in *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors.* (the case was filed in 2012) upheld the constitutionality of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (**"Aadhaar Act"**), subject to certain conditions. The Aadhaar Act was introduced to give statutory backing to the Aadhaar scheme, an initiative to provide Indian citizens with a unique 12-digit identification number in order to avail certain services. The Aadhaar Act was challenged on the grounds of violating the right to privacy and for allegedly permitting a surveillance state. There are a number of pending matters that have been transferred to the Supreme Court as of October 2019 where petitions have been filed for the linking of Aadhaar numbers to social media profiles. As per news report, the Supreme Court is to be next heard in January 2020.[10]

VII. Government Issues Draft National E-Commerce Policy – February 2019

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' (**"E-commerce Policy"**). However, the E-Commerce Policy was critiqued for being overtly data centric, as it contained guidelines for the storage of data, a topic covered in the draft bill. Post this feedback and based on the overlap of jurisdiction between different ministries, a clarification was released which noted that data localization would not be dealt with under the e-commerce policy as MeitY was in the process of introducing the draft bill in parliament.[11]

VIII. Committee to Examine Non-Personal Data Constituted – September 2019

MeitY, in September 2019 constituted a special committee (**"NPD Committee"**) to explore the governance of 'non-personal data' (**NPD**).

8. *MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors., 1954 AIR 300, 1954 SCR 1077. Kharak Singh v. State of Uttar Pradesh*, 1963 AIR 1295, 1964 SCR (1) 332.
9. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Last accessed: February 16, 2020.
10. https://www.business-standard.com/article/current-affairs/supreme-court-transfers-all-aadhaar-social-media-linking-cases-to-self-119102201156_1.html. Last accessed November 11, 2019.
11. https://www.livemint.com/politics/policy/data-storage-rules-out-of-e-commerce-policy-1561488393145.html. Last accessed: November 11, 2019.

Through this notification, MeitY emphasized the need to recognize the economic dimensions of such 'community data' and its potential usefulness for policy-making. Accordingly, the Ministry directed the Committee to: *(a) study various issues relating to non-personal data; and (b) make specific suggestions on the regulation of non-personal data for the Government to consider.*

IX. Personal Data Protection Bill 2019 - December 2019

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.[12] In July 2018, the committee released the draft Personal Data Protection Bill, 2018, along with their report with views and deliberations giving context to the Bill.

Over a year later, the PDP Bill was introduced in the lower house of Parliament with a few revisions basis industry and ministerial consultations that had taken place between 2018 and 2019. The PDP Bill has on December 12, 2019 been referred to a joint parliamentary committee for further debate and examination (**"Parliamentary Committee"**). The Parliamentary Committee had been instructed to give its report to the Lok Sabha in the Budget Session, 2020;[13] further changes may be made in the PDP Bill on the basis of the comments of the Parliamentary Committee. The Parliamentary Committee accepted comments from the public. The Lok Sabha has now adopted a motion to extend the deadline for the submission for the Parliamentary Committee Report until the second week of the monsoon session, which we expect to be July-August 2020.[14] This could be further extended given the Covid-19 lockdown imposed by the Central and State Governments. Please refer to Chapter IV for our detailed analysis of the PDP Bill.

12. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf. Last accessed: February 16, 2020.

13. Brief Record of the Proceedings of the Meeting of the Rajya Sabha held on the 11th December 2019, Rajya Sabha.

14. Lok Sabha Bulletin, 23.03.2020, page 16.

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"**).[15]

- 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.[16] 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[17] 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.[18]

- 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.[19]

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.*[20] (**"Puttaswamy Case"**) wherein Article 21 of the Constitution was expanded by judicial reading to recognize privacy as a fundamental right, which can be claimed by individuals in India.[21] 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

15. *MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors.*, 1954 AIR 300, 1954 SCR 1077.
16. *Kharak Singh v. State of Uttar Pradesh*, 1963 AIR 1295, 1964 SCR (1) 332.
17. 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.
18. *Govind Singh v. State of M.P.* 1975 AIR 1378, 1975 SCR (3) 946.
19. *R. Rajagopal v. State of Tamil Nadu*, 1995 AIR 264, 1994 SCC (6) 632.
20. WP (C) 494 of 2012.
21. This is as Article 21 is available to 'persons' and not only citizens.

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 [22]and 21[23] 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[24] 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.*[25] and in the Kerala High Court case of *Oommen Chandy v. State of Kerala*,[26] 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,[27] and where the right to access the internet was determined to constitute the right to privacy and education under the Constitution of India.[28]

22. 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.

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

24. 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"*.

25. 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.

26. 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.

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

28. 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.[29]

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 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,[30] 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

29. 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.

30. Rules 5 and 6 in particular.

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 PDP Bill. 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.

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.[31]

This section prescribes a penalty of imprisonment up to three years and/ or a fine up to INR 5,00,000 (approx. USD 7,750). Important points to be kept in mind are:

ii. SDPI

As per the IT Act, where a body corporate, possessing, dealing or handling any SPDI is

31. Section 72A, IT Act.

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.[32] 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.[33]

II. Industry Specific Regulations

A. Telecommunications Law

The *Indian Telegraph Act, 1885*[34] and the *Indian Telegraph Rules, 1951*[35] 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"**)[36] 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.
- 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 6,901,000) 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 Reserve Bank of India (**"RBI"**), the apex bank in India. There is no specific definition of 'sensitive data' or its equivalent under the banking laws. However, different Banking Laws, based on their subject matter seek to protect such kind of information.

32. Section 43A, IT Act.
33. Section 75, IT Act.
34. Section 5 of the Indian Telegraph Act, 1885.
35. Rule 419A of the Indian Telegraph Rules, 1951.
36. http://www.dot.gov.in/sites/default/files/2016_03_30%20UL-AS-I.pdf?download=1 . Last accessed: February 16, 2020.

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*,[37] *RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds*,[38] *RBI Report on Information Systems Security Guidelines for the Banking and Financial Sector*,[39] *RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks*,[40] *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*,[41] *RBI's Master Circular on Customer Service in Banks, 2014*,[42] *and RBI's Master Circular on Credit Card Operations of Banks.*[43]

- Importantly, RBI released the *Storage of Payment System Data Directive, 2018*[44] 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 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.[45] 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. Capital Markets 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"**).[46] 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.

C. 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'*

37. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF. Last accessed: February 16, 2020.
38. https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf. Last accessed: February 16, 2020.
39. https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=275. Last accessed: February 16, 2020.
40. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=3148&Mode=0. Last accessed: February 16, 2020.
41. https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9848. Last accessed: February 16, 2020.
42. https://www.rbi.org.in/scripts/bs_viewmascirculardetails.aspx?id=9008. Last accessed: February 16, 2020.
43. https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7338. Last accessed: February 16, 2020.
44. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Last accessed: February 16, 2020.
45. https://www.rbi.org.in/Scripts/FAQView.aspx?Id=130. Last accessed: February 16, 2020.
46. http://www.sebi.gov.in/sebi_data/attachdocs/1436179654531.pdf. Last accessed: February 16, 2020.

("Insurer Guidelines"),[47] *IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017,*[48] *IRDAI (Maintenance of Insurance Records) Regulations, 2015,*[49] *and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017.*[50] 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

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.[51]

D. Healthcare

The Ministry of Health and Welfare released a draft bill for Digital Information Security in Healthcare Act (**"DISHA"**). The main purpose of DISHA is to: (i) establish a National eHealth Authority to regulate the e-Health records and digital health information across India, and Health Information Exchanges; (ii) standardize and regulate the process related to collection, storing, transmission and use of digital health data; (iii) and to ensure reliability, data privacy, confidentiality and security of digital health data. However, since the draft Personal Data Protection Bill, 2018 has been introduced, it is left to be seen whether DISHA will be enacted.

47. https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20Information%20and%20Cyber%20Security%20for%20insurers.pdf. Last accessed: February 16, 2020.
48. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1. Last accessed: February 16, 2020.
49. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo2604&flag=1. Last accessed: February 16, 2020.
50. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3191&flag=1. Last accessed: February 16, 2020.
51. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1. Last accessed: February 16, 2020.

4. New Data Protection Law Proposed in India

I. Background

The PDP Bill 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 *draft* Personal Data Protection Bill, 2018, that was proposed in July 2018 by a Committee of Experts set up by the Government, chaired by retired Supreme Court judge, Justice Srikrishna (**"Committee"**). Along with the bill, the Committee had released their report with views and deliberations giving context to the bill (**"Report"**).

On December 12, 2019, the PDP Bill was referred to a Joint Parliamentary Committee for further debate and examination (**"Parliamentary Committee"**). The Parliamentary Committee has been instructed to give its report to the Lok Sabha on the first day of the last week of the Budget Session, 2020. The Parliamentary Committee has invited comments from stakeholders on the PDP Bill, based on which further changes may be made in the PDP Bill, along with the inputs of the Parliamentary Committee. The Lok Sabha has now adopted a motion to extend the deadline for the submission for the Parliamentary Committee Report until the second week of the monsoon session, which we expect to be July-August 2020. [52]This could be further extended given the Covid-19 lockdown imposed by the Central and State Governments.

The PDP Bill will need to go through the following steps before it becomes binding law:

1. Submission of the Parliamentary Committee report;
2. Passing by both Houses of Parliament;
3. Presidential assent followed by notification in the Official Gazette.

However, since the PDP Bill 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. Some reports suggest that the Government is likely to give companies a two-year window to comply,[53] although this remains a matter of discretion and we would suggest that a transition period is provided for in the text of the PDP Bill.

The PDP Bill seems to dilute provisions with respect to data localization and cross-border data transfers, as well as provisions for criminal liability as compared to the earlier avatar. However, it introduces some new concepts and provisions such as 'social media intermediaries', a 'consent manager' and the provision of a regulatory sandbox.

52. Lok Sabha Bulletin, 23.03.2020, page 16.

53. https://tech.economictimes.indiatimes.com/news/internet/companies-may-get-up-to-2-years-to-comply-with-data-law/72432037, last visited on December 18, 2019.

II. Highlights of the PDP Bill 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 PDP Bill is a far more complex and far-reaching than the current law.
2.	*Extra-territorial application:*	It applies to entities outside India if they have a business connection to India or carry on profiling of individuals in India.
3.	*New data regulator (the Data Protection DPA, the **"DPA"**), adjudicating officers, and appellate tribunal:*	The PDP Bill introduces a specialized regulatory approach to data protection. The DPA will be the first cross-sector data protection regulator in India and has significant regulation-making powers.
4.	*Subordinate legislation:*	The PDP Bill 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:*	Most parts of the PDP Bill apply to all 'personal data'. Higher benchmarks of compliance are prescribed for 'sensitive personal data' and 'critical personal data' (which are subsets of 'personal data'). Non-personal data / anonymized data does not qualify as 'personal data', and the compliance requirements applicable to personal data do not apply to these forms of data. However, as discussed below, the PDP Bill provides an important exception for the Government to direct organizations to provide their non-personal in certain circumstances.
6.	*Data localization for sensitive data:*	A copy of all 'sensitive personal data' must be stored in India but may be transferred outside India. 'Critical personal data' (which will be defined by the Central Government) must be processed only in India, with exceptions. Organizations processing sensitive personal data should prepare their infrastructure for data localization.
7.	*Cross-border transfer restrictions:*	Mere personal data (that is non sensitive personal data or critical personal data) has been exempted from cross-border transfer restrictions. Sensitive personal data 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 'critical personal data' may be transferred outside India on certain narrow grounds.
8.	*Privacy principles:*	The principles underlying the PDP Bill 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 data portability; ▪ the right to be forgotten; and ▪ the rights to access, correction, and erasure. 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. It appears intended to mitigate the concern of 'consent fatigue' and help educate 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 intermediaries' with over a certain number of users.
12.	*Data breach notification:*	In case of a data breach, the DPA is to be intimated, who may require that the data breach be reported to affected individuals and that remedial action be taken.
13.	*Special provisions on children's data:*	The PDP Bill provides for age verification; parental consent; and raised obligations for 'guardian data fiduciaries' (a class of designated entities whose services are directed at children or who process large volumes of children's personal data).
14.	*Innovation sandbox for artificial intelligence and emerging technology:*	The innovation sandbox is supervised by the regulator, and eligible data fiduciaries can avail of relaxations from certain obligations of the PDP Bill up to a maximum period of 3 years.
15.	*Government requests for anonymized and non-personal data:*	The Central Government has been given the power to direct that anonymized / non-personal data be shared by any entity with the Central Government, in certain circumstances. This is a provision directed at the use of data for public good; Rules in this connection are awaited to flesh out more detail. A separate government-appointed committee is also examining this subject.
16.	*GDPR-like penalties:*	The PDP Bill 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.

III. Detailed Analysis of the PDP Bill

The key points to note in the PDP Bill are as follows:

A. Amendments to Current Law

The PDP Bill, when enacted, will replace Section 43A[54] 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 PDP Bill applies to the processing of personal data (**"PD"**) of natural persons, of which sensitive personal data and critical personal data are subsets. The natural person whose data is being processed is referred to as a **"Data Principal".** Further, the proposed law applies to both manual and automated processing.

i. Retrospective Applicability

The PDP Bill is silent about retrospective applicability, i.e. applicability to data collected before the law coming into effect and if the provisions would apply to such data. However, the PDP Bill will apply to any ongoing processing once introduced.

Practically this may be problematic for the following reasons:

Ongoing processing activity: In all likelihood, substantial PD would not have historically been obtained with consent. Thus, for any continued processing necessary consents may need to be obtained. This may mean renegotiation of previously concluded contracts, because if Data Principals do not give consent, the Data Fiduciaries may refuse to provide goods or services. However, the PDP Bill does not specifically clarify this.

Deletion of data: Data Fiduciaries may have to delete PD previously collected or PD for which they have not been granted specific consent unless specific consent is taken. Also, for consent given earlier Data Principals would also have the right to withdraw consent and request erasure of the data.

ii. Personal Data

PD is 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.

The definition of PD is extremely wide in comparison to the Current Law. Barring a few provisions, the PDP Bill also applies to manual processing of PD, where certain exemptions may be granted. However, there are no thresholds for which the exemptions can be granted. Thus, several non-digital businesses handling even non-sensitive PD are likely to be burdened with huge compliances, unless the DPA provides exemptions.

iii. Sensitive Personal Data

Sensitive Personal Data (**"SPD"**) is a subset of PD and consists of specified types of data, such as financial data, health data, official identifier, sex

54. 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.*"

life, sexual orientation, biometric data,[55] 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.

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:

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, is independently less likely to cause harm to the Data Principal, as opposed to a bank account number in combination with a password used for authenticating transactions. 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. Similarly, the Unified Payments Interface ("UPI") has made peer-to-peer financial transfers easily accessible through use of Virtual Payment Addresses ("VPAs"), which sometimes merely consist of mobile phone numbers with short codes as suffixes. This makes it difficult for a third party to cause harm to the Data Principal merely by possessing the VPA. Harm is typically caused with the misappropriation of authentication information alongside login information and not one independent of the other.

Therefore, the PDP Bill in its current construct would cause inconvenience to those individuals who use the system regularly to transact among each other as they would have to technically comply with the stringent provisions of the PDP Bill to the extent of standards prescribed for SPD, merely because they possess each other's payment identifiers.

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 possibly impact voice activated assistants and assistive technologies which are used by people with disabilities. Further, the Government has the overarching power of carving out certain kinds of biometric data from processing, as it may deem fit.

Religious or political beliefs/ caste or tribe: Interestingly, the PDP Bill 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. Aadhaar has been removed from the definition of official identifiers, as compared to the draft Bill of 2018. However, the definition is still broad enough to include Aadhaar, as it includes any number or identifier used for the purpose of verifying the identity of a Data Principal.

iv. Data Fiduciaries and Data Processors

Entities processing PD may be either **"Data Fiduciaries"** (the entity that determines the purpose and means for processing) or **"Data Processors"** (the entity that processes PD on behalf of a Data Fiduciary). While most obligations under the PDP Bill are on Data Fiduciaries which include notice and consent, implementing operation framework for the enforcement of user rights, and transparency and operability measures; there are limited obligations on Data Producers, such as the necessity to implement security safeguards.

55. The PDP Bill 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.

v. Anonymized Data

Anonymized data (i.e., data which cannot identify a Data Principal) largely falls outside the scope of the PDP Bill. The extent to which large datasets can be truly anonymized (an irreversible process) is still a matter of global debate, but for the purposes of the PDP Bill, anonymization is presumed to be possible, and the discussion here is on that basis. However, there is an ongoing worldwide debate on whether data can truly be anonymized, as there may always be identifiers from which it may be re-identified as PD.

The Central Government may direct any Data Fiduciary or Data Processor to provide any anonymized personal data or other non-personal data in order to enable **better targeting of service delivery** or to **aid evidence-based policy making** in a manner as may be prescribed. 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 PDP Bill also reserves the power of the Central Government to frame policies for the promotion of the digital economy, to the extent such policies do not govern PD.

Interestingly, a committee under the chairmanship of Mr. Kris Gopalakrishnan was set up recently to recommend a framework to regulate non-personal/community data. That committee has not yet submitted its report. In our view, this aspect should be kept out of the PDP Bill, and this committee should be allowed to conduct public consultations before giving their recommendations on non-personal data.

vi. Extra Territorial Application

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

Applicability of the PDP Bill		**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

The PDP Bill 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'.

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

For instance, the definition of PD is not limited to Indian citizens/residents; as Section 2 of the PDP Bill in relation to applicability of the law uses a method of territorial nexus with India for establishing jurisdiction for the purposes of the PDP Bill. Under the PDP Bill, if the data is processed by any person or entity within India, then the provisions of the PDP Bill 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 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 Compliance Obligations

i. Notice

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 (**"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 PD being collected;
- The right of the Data Principal to withdraw their consent, and the procedure for such withdrawal, if the PD is intended to be processed on the basis of consent; and
- information regarding any cross-border transfer of the PD that the Data Fiduciary intends to carry out, if applicable.

This Notice should be clear, concise and comprehensible and specifies that a Notice may be issued in multiple languages whenever necessary. ***However, the PDP Bill is not clear as to when such multilingual notices maybe necessary.***

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 PD 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 PD the Data Fiduciary is unlikely to have access to the names of all entities who may process such PD.***
- ***The source from where such PD 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. It is hoped that, the DPA does not make Notice too cumbersome by including granular details, whereby it gets difficult to make it clear and concise as required under the PDP Bill.***

ii. Purpose and Collection Limitation

Data Fiduciaries processing PD are required to do so in a fair and reasonable manner so as to ensure the privacy of the Data Principal.

Data Fiduciaries 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 (a) for the purposes specified to the Data Principal; or (b) for any other incidental purpose that the Data Principal would reasonably expect the PD to be used for, given the context and circumstances in which the PD was collected and the purpose for collection. Therefore, using data for new (or previously unspecified) purposes should therefore need fresh consent.

iii. Storage Limitation

PD may be retained only until the purpose of collection is completed. ***It is recommended that Data Fiduciaries have a data retention policy in place 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 data at any time, with the Data Fiduciary confirming removal from its systems and from the systems of any other companies who were processing the data on its behalf. ***However, it must be noted that in a digital ecosystem, the complete deletion of data and confirmation that no digital footprints remain is questionable.***

iv. Transparency of Processing.

The PDP Bill 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 PDP Bill requires Data Fiduciaries to provide the following information relating to their processing of PD, in the manner as may be specified by regulations:

- Categories of PD being collected.
- The purpose for which such PD is being processed.
- Categories of data processed in exceptional situations or any exceptional purposes of processing. that create a risk of significant harm.
- The existence of, and the procedure to exercise Data Principal rights.
- Information relating to cross border transactions generally carried out by the Data Fiduciary.
- Where applicable, the Data Trust Score of the Data Fiduciary.

The above list is not exhaustive, since the PDP Bill 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 PD. However, what constitutes 'important' has not been defined under the PDP Bill and is left to the regulators. This requirement assumes significance since it would impact compliance levels by Data Fiduciaries. It is therefore necessary that only important (rather than routine) operations in data processing are eventually included in this requirement by the regulator.

D. Grounds for Processing PD and SPD

The PDP Bill provides that PD cannot be processed without consent, except for a specific ground set out in the PDP Bill:

i. Processing on the basis of consent

- The PDP Bill lays down the test for 'valid consent' for PD, 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).
- For SPD, explicit consent is required after meeting the following additional requirements: 1) the Data Principal must be informed of the purpose of processing which is likely to cause significant harm; 2) the consent has to be clear and may not be inferred; 3) the Data Principal must be provided a choice of separately "consenting to the purposes of, operations in, the use of different categories of, SPD" that may be relevant to processing.
- In an attempt to make consent more meaningful and prevent its abuse, the PDP Bill 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 PD *that is not necessary for the provision of the services / goods by the Data Fiduciary*. Accordingly, a Data Fiduciary may condition the provision of services on the consent of the Data Principal, provided that such processing is necessary for the provision of services by the Data Fiduciary. Considering the increasingly complex nature of personalized services derived from processing of multiple fields of PD, the determination of whether some PD 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 PDP Bill places the burden on the Data Fiduciary to show that consent meets all the elements specified above. However, this aspect needn't have been specified in the PDP Bill. The principle as per the Indian Evidence Act could have been adopted here as well, i.e. the party which alleges a particular fact, needs to prove it. When any fact is especially within the knowledge of any person, the burden of proving that fact is upon him. For proving free consent, with the current scheme under the PDP Bill, the Data Fiduciary will need to prove absence of coercion. This goes against the basic principles of burden of proof.***

Consent Manager

The PDP Bill 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. It appears intended to mitigate the concern of 'consent fatigue' and help educate the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on implementation of consent managers.

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 Fiduciary, or a separate category of Data Processors who may be subject to limited compliances. In order to qualify as Data Fiduciaries under the PDP Bill, the

consent managers would have to determine the purpose and means for processing of data.

ii. Processing on grounds other than consent

PD may be processed without consent for specified grounds including:

i. 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;

ii. prevention, investigation or prosecution of any offence or any other contravention of any law;

iii. compliance with court orders;

iv. in connection with legal proceedings;

v. in connection with disasters or medical emergencies;

vi. employment-related purposes (where the Data Principal is an employee of the Data Fiduciary);

vii. journalistic purposes;

viii. personal or domestic purposes;

ix. classes of research, archiving or statistical purposes specified by the DPA; and,

x. 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. Interestingly, a new ground – the operation of search engines – (which did not find place in the draft Bill of 2018) has been included as a reasonable purpose for which PD may be processed without consent. These reasonable purposes may be specified after taking into consideration factors such as the interest of the Data Fiduciary in processing for that purpose, whether it is reasonably expected for consent to be taken, and the reasonable expectations of the Data Principal having regard to the context of processing.

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 PD, the Bill 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 PDP Bill, to the extent that such treatment did not impede compelling State interests.

The 'reasonable purposes' provision leaves discretion with the DPA to notify additional purposes for which consent may not be required to process PD. 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 PDP Bill mandates that parental consent will be necessary for the processing of PD 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 PD.[56] 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.

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

Guardian Data Fiduciaries: Data Fiduciaries who operate commercial websites / online services directed at children; or process large volumes of PD of children will be notified as 'Guardian Data Fiduciaries'. These 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.

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

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.

Businesses catering to those below 18 might be affected by this PDP Bill. Education focused startups who rely on targeted advertisements or audio / video streaming platforms functioning on behavioral monitoring may need to alter their business models to comply with the provisions of the PDP Bill.

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

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

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

In addition, the PDP Bill 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 PD has been shared; and (b) details as to the categories of their PD which has been shared with such Data Fiduciaries, which seems quite onerous.

The PDP Bill requires businesses to provide the Data Principal with summaries of the PD 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 PDP Bill introduces a provision with respect to Data Portability, whereby Data Principals may seek from the Data Fiduciary, their PD in a 'structured, commonly used and machine-readable format'. The PDP Bill however does not specify the technical specifications of such a format, or what would be threshold for 'common use'.

The PD 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 would reveal a trade secret for a Data Fiduciary, or would not be technically feasible.

In relation to points (ii) and (iii) of the PD 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 PD? 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 what constitutes 'data which forms part of the profile of the Data Principal', especially the manner in which this 'profile data' would differ from PD 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 PD but also smaller companies and start-ups that may collect PD for the purpose of improving their services. ***While large platforms may be able to sufficiently comply with these requirements but 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 PD in this format may be onerous for smaller companies, particularly when the standard of providing such PD 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 PD may be quite different from a format for a user wanting their PD to move to a different service. Some of these practical issues are not adequately addressed by the PDP Bill and need to be fleshed out more thoroughly.***

H. Right to be Forgotten

The PDP Bill 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 of PD'. It is not clear at this stage whether this provision requires the Data Fiduciary to disable 'continuing disclosure' or whether it requires the Data Fiduciary to also delete the PD. In any event, a Data Principal is empowered to request for erasure of PD, which is no longer necessary for the purpose for which it was processed, and the storage period limitation requires PD to be ordinarily be deleted once the purpose of processing has been achieved.

I. Data localization

From the earlier draft, local data storage requirements have been substantially reduced. The PDP Bill now provides that SPD may be transferred outside India, but a copy of the data should be stored in India. Further, certain critical PD may be identified by the Government which should only be processed in India. Further, PD may be freely transferred and stored outside India. The intention behind the PDP Bill appears to be to make the data localization obligation applicable only for PD and SPD belonging to Indian residents, however, this has not been made clear, as the data localization obligation applies generally to SPD under the PDP Bill presently.

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 PD and SPD. Since, it may be practically difficult to separate the SPD from such a data set, the entire data set would have to be stored locally, due to the element of SPD. 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.

Critical personal data: The PDP Bill does not give any guidance/examples on what data would compromise or be notified as critical personal data. Delegation of the right to determine / notify critical PD to the Government without specific guidance under the PDP Bill grants excessive powers to the Government in relation to PDP Bill, 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 PDP Bill 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 DPA,[57] or

b. The Indian Government (in consultation with the DPA) prescribes a particular country or section within a country or a particular international organization (or class thereof) for which the transfer is permissible,[58] or

c. The DPA approves particular transfer(s) for a specific purpose.

In addition to either of points (a) or (b) above being fulfilled, the Data Principal should also explicitly consent to such data transfer.

SPD may be transferred outside India subject to either points (a) or (b) above being fulfilled (similar to PD), and wherein the Data Principal has explicitly consented to such a transfer. The PDP Bill however also empowers the Indian Government to notify specific SPD 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, and
- A particular country or section within a country or a particular international organization prescribed by the Indian Government for which the transfer is deemed permissible.

It appears that the Government favors the use of approved clauses / schemes between the transferor and transferee, or specifically notifying certain countries / organizations that in its view, meets 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.

K. Breach notifications

If there is a breach of PD processed by the Data Fiduciary which is likely to cause harm to the Data Principal, the Data Fiduciary should notify the Data Protection DPA of such breach. The notifications should contain certain particulars, either submitted to the DPA together or in phases. The DPA may determine if the Data Principal should also be notified of such breach.

There is no specific time period prescribed under the PDP Bill for the breach notification reporting, however, such reporting is to be done as soon as possible. The Data Protection DPA,

57. The Authority 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 PD.

58. 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 PD, as well as effectiveness of enforcement by authorities.

once set up, may prescribe a certain time period for reporting.

The data breach reporting provisions prima facie appear reasonable and practical.

L. Significant Data Fiduciary

The DPA is empowered to notify certain Data Fiduciaries or entire classes of Data Fiduciaries as SDFs.[59] 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 PDP Bill proposes that such SDF register itself with the DPA 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 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.

Social Media Intermediaries

New provisions have been introduced with regard to 'social media intermediaries'.[60] Any social media intermediary that has more users than a certain threshold DPA and whose actions may have a significant impact on electoral democracy and other public interest factors may be notified by the Central Government as an SDF. Accordingly, such a social media intermediary would be required to register itself with the DPA and comply with the other SDF obligations discussed above. In addition, the Bill requires any such social media intermediaries that are notified as an SDF 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 definition of 'social media intermediary' has certain subjective elements, which could be contentious:

- ***Whether an organization "primarily" enables online interaction between users, since even gaming and education platforms (for instance) enable interaction between users; and***
- ***The scope of the term "commercial or business-oriented transactions" in light of ad-based revenue models.***

The introduction of these new provisions seems to be outside the overall scope of the PDP Bill and does not fit within the broad purpose of the PDP Bill as set out under the "Statement of Objects and Reasons". As per the "Statement of Objects and Reasons", the PDP Bill seeks to bring 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", which does not cover regulation of social media intermediaries.

While it is possible for social media intermediaries 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 intermediaries to verify identities of its users and then identify their accounts as verified accounts may not be

59. The Data Protection Authority may from time to time notify certain Data Fiduciaries (or class of Data Fiduciaries) as 'Significant Data Fiduciaries' (**"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; and*
    f. *any other factor causing harm to any data principal from such processing.*

60. A 'social media intermediary' is defined as "an intermediary 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" but does not include any intermediaries that primarily — (a) enable commercial or business-oriented transactions; or (b) provide access to the Internet; or (c) are in the nature of search-engines, on-line encyclopedias, e-mail services or on-line storage services.

preferable. ***Fortunately, 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 intermediaries 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.***

M.Sandbox

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

Eligibility: Data Fiduciaries 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 PD;
- Limitation on collection of PD;
- Restriction on retention of PD; and
- Any other obligation under purpose and collection limitations under Sections 5 and 6 of the PDP Bill.

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 PDP Bill, 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.

N. Data Protection Authority

The PDP Bill 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 PDP Bill,
- 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 PD without consent,
- prescribing regulations in respect of processing of children's PD,
- certification of privacy by design policy,
- approval of codes of practice,
- registration of 'consent managers', and
- notifying entities as SDFs

The DPA also has the power to undertake actions that are crucial for a majority multi-national 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 critical PD.

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.***

O. Codes of Practice

The PDP Bill 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 PDP Bill, such as on notice requirements, retention of PD, conditions for valid consent, exercise of various rights by users, transparency and accountability measures, methods of destruction / deletion / erasure of PD, breach notification requirements, cross-border data transfers, etc.

P. Privacy by design

Similar to the GDPR, the PDP Bill stipulates that Data Fiduciaries implement a policy along the lines of a "Privacy by Design" principle.[61] Further, subject to regulations made by the DPA, Data Fiduciaries may submit their privacy by design policy to the DPA for certification, which upon examination / evaluation by the DPA or its authorized officer shall be certified to be in compliances with the requirements under the PDP Bill. 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. Exemptions

The PDP Bill 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 PD 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 PDP Bill.

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,[62] 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 by an order with reasons to be substantiated in writing.

Notably, the grounds of discretion are fairly broad and allow the government significant leeway to provide exemptions from the application of the PDP Bill, whereas civil society had expressed the hope that the PDP Bill would ensure that Government's use of personal data would be restricted to necessary and proportionate instances.

61. 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 PDP Bill; (c) certification that the technology used to process PD 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 PD (from point of collection to deletion); (f) PD is processed in a transparent manner; and (f) the Data Principal's interests are accounted for at each stage of processing of PD.

62. 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.

Processing of personal data in the interests of criminal investigation and prosecution, including "prevention", is also exempt from most provisions of the PDP Bill. ***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 PDP Bill.***

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 PD 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 PD and the volume of PD 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.

R. Penalties, Offences and Compensation

The PDP Bill 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.

i. Financial Penalties

The PDP Bill follows the GDPR route in terms of financial penalties by not only proposing the imposition of fixed financial penalties (ranging from Rupees 5 crore to 15 crore (i.e. approx. USD 700,000- 2,100,000)) but also penalties based upon a certain percentage (ranging from 2-4%) of a Data Fiduciary's 'total worldwide turnover' in the preceding financial year. 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 PDP Bill 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 PD, and extend to imprisonment for a term not exceeding three years and/or a fine which may extend to INR 2,00,000 (approx. USD 2,000).

The PDP Bill has diluted the criminal penalties proposed in the draft bill of 2018 (which suggested criminal sanctions for the processing of PD/SPD which caused harm to the Data Principal) by providing for criminal sanctions only for the re-identification of PDP. However, it is still not clear whether this criminal sanction is appropriate. Penalties as harsh as imprisonment may not be appropriate in a data processing context, where a right to compensation is already provided to the individual. Professors Elizabeth Pollman & Jordan M. Barry in their paper on Regulatory Entrepreneurship recognize that "if a law provides for the incarceration of the executives of a company that violate it, that may deter the guerrilla growth strategies that some modern regulatory entrepreneurs employ". Rather, the threat of financial penalties and compensation may act as a sufficient deterrent.

Further, since the PDP Bill contains a specific clause clarifying that other laws would continue to apply, there was no requirement to include specific criminal

penalties under the PDP Bill, as IPC and IT Act would continue to apply. For example, data theft may, in rare cases, if required may be punished under theft of IPC.

iii. Compensation

The PDP Bill importantly allows the Data Principal to apply to the adjudicating authority 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 PDP Bill and a specialized forum for redress, this may lead to a stream of data protection litigation. This will in turn help provide guidance on subjective provisions.***

iv. Class action

The PDP Bill also appears to allow for the institution of class action suit 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 single complaint on behalf of all such Data Principals for seeking compensation for harm suffered as a result of any infringement of any provision of the PDP Bill.

S. Road Ahead

As the PDP Bill is pending with the Parliamentary Committee, the industry should submit its views and recommendations to ensure the members of the Parliamentary Committee take into account the unforeseen implications of the current draft of the PDP Bill, and focus on the pain points for the industry. The industry should also take proactive steps to formulate rules and codes of practice, which can be submitted to the DPA.

Once implemented, the PDP Bill will mean a complete overhaul of the current data protection law in India. The PDP Bill introduces additional compliance requires for all forms of personal data, limits on data collection, processing and storage, and hefty penalties for non-compliance to name a few changes as compared to current law. Since this is a radical change in the law, it would be recommended that the government gives sufficient implementation / transition time before enforcing the provisions of the PDP Bill. In addition, compliance exemptions for PD along with clarity on whether the PDP Bill will apply retrospectively would also be welcomed.

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 PDP Bill 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 DISHA. It is left to be seen whether this sector-specific law would be enacted in the foreseeable future.

The PDP Bill 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 PDP Bill 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 Bill 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 two-factor authentication process 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 and provided a deadline of October 15, 2018 for all entities to comply with this requirement. While there were requests for this deadline to be extended, the RBI was not in favour of its extension. 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.

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 PDP Bill implements certain restrictions when processing the data of a 'child', or an individual under eighteen years of age. Further, digital platforms with services targeting children may be classified as 'guardian data fiduciaries' as a result of operating a commercial website or online service directed at children, or processing large volumes of personal data of children. There may be certain restrictions on guardian 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.

IV. Technology Industry

The technology industry may be impacted by the PDP Bill 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.

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"**).[63] 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%.[64] 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[65]), 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.[66] 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.

63. The 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.).

64. Excluding surcharge and cess.

65. A.A.R. No 1573 of 2014.

66. 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.

Further, Section 34 of the PDP Bill,[67] 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 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.[68] 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.[69]

- Secondly, given that the PDP Bill 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 PDP Bill 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.

67. 34. (1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—
(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority:
Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—
(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and
(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or
(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that—
(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and
(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction:
Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;
(c) The Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

68. Id.

69. 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.";**

It is clear that the various policies that are proposed to be introduced including the PDP Bill 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.

7. India Taking A Leaf From The GDPR Book

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

	EU - GDPR	**India – PDP Bill**
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.[70]	Similar to the GDPR, the PDP Bill 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.[71]
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.	Similar to the GDPR, the bill has categorized data into two categories: 'personal data'[72] and 'sensitive personal data'.[73] The processing of sensitive personal data is subject to similar conditions as provided for in GDPR.
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 PDP Bill allows the processing of PD under consent (along with exceptions to this rule), the PDP Bill 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.

70. Article 3, GDPR.

71. Section 2, PDP Bill, 2018.

72. "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;

73. 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.

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.[74]
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 sensitive personal data outside India may be permitted if (a) certain provisions are included which are pre-approved by the data protection authority, or (b) the Government approves the location or organization for the transfer, or (c) the data protection authority specifically approves such a transfer as necessary for any specific purpose. Further, such transfers must be consented to.
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 PDP Bill, 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 subscription, or information forming 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.[75] 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 Guardian Data Fiduciarie[76] may not permitted.

74. Section 40, PDP Bill, 2018.

75. Article 8, GDPR.

76. Guardian data fiduciaries are of two kinds (i) Who operate commercial websites or online services targeted at children (ii) Who process large volumes of personal data of children.

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.[77] 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 2,185,800) 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. [78] Further, both civil and criminal offences (for certain offences) have been prescribed.

77. Article 83, GDPR.

78. Section 69, PDP Bill, 2018.

8. Road Ahead

Interesting and exciting times lie ahead. As one can see, 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. One will have to wait and watch for recommendations of the Joint Parliamentary Committee, and the subsequent changes made to the PDP Bill, if any. We may even see the revised version of the PDP Bill sometime this year, though it may be delayed due to Covid-19 considerations.

However, irrespective of a general data protection law coming into force, some industries such as banking (the RBI's Data Localization Circular is an example), insurance, telecommunication and potentially healthcare (the draft DISHA bill) have been proactive and already have relevant guidelines and safeguards in place.

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**

Technology and Tax Series: Platform Aggregators |Business Model Case Study

June 2020

5G Technology in India

May 2020

Investment in Healthcare

May 2020

Privacy & Data: India's Turn to Bat on the World Stage

May 2020

3D Printing: Ctrl+P the Future

April 2020

Dispute Resolution in India

April 2020

Construction Disputes in India

April 2020

Digital Health in India

April 2020

Introduction to Cross-Border Insolvency

April 2020

NDA Insights

TITLE	TYPE	DATE
Delhi Tribunal: Hitachi Singapore's Liaison Office in India is a Permanent Establishment, Scope of Exclusion Under Singapore Treaty Restrictive	Tax	November 2019
CBDT issues clarification around availment of additional depreciation and MAT credit for companies availing lower rate of tax	Tax	October 2019
Bombay High Court quashes 197 order rejecting Mauritius tax treaty benefits	Tax	May 2019
Investment Arbitration & India – 2019 Year in review	Dispute	January2020
Changing landscape of confidentiality in international arbitration	Dispute	January2020
The Arbitration and Conciliation Amendment Act, 2019 – A new dawn or sinking into a morass?	Dispute	January2020
Why, how, and to what extent AI could enter the decision-making boardroom?	TMT	January2020
Privacy in India - Wheels in motion for an epic 2020	TMT	December 2019
Court orders Global Take Down of Content Uploaded from India	TMT	November 2019
Graveyard Shift in India: Employers in Bangalore / Karnataka Permitted to Engage Women Employees at Night in Factories	HR	December 2019
India's Provident Fund law: proposed amendments and new circular helps employers see light at the tunnel's end	HR	August 2019
Crèche Facility By Employers in India: Rules Notified for Bangalore	HR	August 2019
Pharma Year-End Wrap: Signs of exciting times ahead?	Pharma	December 2019
Medical Device Revamp: Regulatory Pathway or Regulatory Maze?	Pharma	November 2019
Prohibition of E-Cigarettes: End of ENDS?	Pharma	September 2019

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 California Avenue, Suite 201
Palo Alto, CA 94306-1636, 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 30, Six Battery Road
Singapore 049 909

tel +65 6550 9856

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

C–5, Defence Colony
New Delhi 110 024, 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