Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

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

Privacy & Data: India's Ticket to Global Technological Supremacy

Legal, Regulatory and Tax Considerations

November 2018

Privacy & Data: India's Ticket to Global Technological Supremacy

Legal, Regulatory and Tax Considerations

November 2018

ndaconnect@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 2016 Mckinsey report, all types of data flows acting together have raised world GDP by 10.1 percent over what would have resulted in a world without any cross-border flows. This value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact. Innovation too, has been seen to cause a marked increase in employment rates, as well as on labour productivity, as per a 2017 Report by the International Labour Organization.

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 recently declared the right to privacy as a fundamental right guaranteed under the Constitution of India. Thereafter, the Indian Government has been in the process of introducing a new first of its kind data protection law for the country. 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.

One cannot deny that India has also looked over it's 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.

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.

Enjoy the read.

1. Summary and Chronology of Privacy Developments in India

I. Information Technology Act Enacted - 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.[1] 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.[2] 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.[3]

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.[4]

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.*[5] recognized that a fundamental right to privacy exists under the Constitution that is enforceable against the State even though it was not explicitly worded.

1. 'Body corporates' includes any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities, as per Section 43A of the IT Act.
2. Karmanya Singh Sareen v. Union of India, 233(2016) DLT436.
3. Dharmaraj Bhanushankar Dave v. State of Gujarat, Special Civil Application No. 1854 Of 2015.
4. [Name Redacted] v. The Registrar, Karnataka High Court, Writ Petition No.62038 Of 2016.
5. Supreme Court, Writ Petition (Civil) No 494 Of 2012

This decision overruled previous Supreme Court decisions where the court held that there was no fundamental right to privacy.[6] 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,[7] 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.

VI. Draft Personal Data Protection Bill - July 2018

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.[8] 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. Please refer to Chapter IV for our detailed analysis on the same.

VII. 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.

6. *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.
7. https://www.rbi.org.in/scripts/NotificationUser.aspx-?Id=11244&Mode=0. Last accessed: November 9, 2018.
8. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf. Last accessed: November, 9 2018.

2. Right to Privacy – Now a Fundamental Right of Citizens

I. Judicial Precedents: Right to Privacy

A. 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").**[9]

B. 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.[10] Given that this was a minority opinion, it was not binding.

C. Supreme Court recognizes Privacy as a Common-Law Right - March 1975

The Supreme Court for the first time recognized a common law right[11] 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.[12]

D. 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.[13]

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.*[14] **("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.[15] The question of the right to privacy as a fundamental right has come up before the

9. *MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors.*, 1954 AIR 300, 1954 SCR 1077.
10. *Kharak Singh v. State of Uttar Pradesh*, 1963 AIR 1295, 1964 SCR (1) 332.
11. 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.
12. *Govind Singh v. State of M.P.* 1975 AIR 1378, 1975 SCR (3) 946.
13. *R. Rajagopal v. State of Tamil Nadu*, 1995 AIR 264, 1994 SCC (6) 632.
14. WP (C) 494 of 2012.
15. This is as Article 21 is available to 'persons' and not only citizens.

judiciary multiple times, but was never declared as a fundamental right available to citizens against the State before the Puttaswamy Case.

III. Impact of the Judgment

The impact of recognizing privacy as a fundamental right, as opposed to a statutory or a common-law right, is that it is an inviolable right - these fundamental rights cannot be given or taken away by law, all laws and executive actions must abide by them, and an individual cannot part with these rights. The judgment recognized that the right to privacy was now a fundamental right under Articles 19[16] and 21[17] 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. Rationale

The Judgement recognized that:

i. **Privacy is an inalienable right**: Privacy is a natural right, inherent to a human being. It is thus a pre- constitutional right which vests in humans by virtue of the fact that they are human. The right has been preserved and recognized by the Constitution, not created by it. Privacy is not bestowed upon an individual by the state, nor capable of being taken away by it. It is thus inalienable.

ii. **Relationship with dignity**: It was argued by the State that the recognition of privacy would require a Constitutional amendment, and could not be 'interpreted' into the Constitution. The judgment has recognized that privacy was intrinsic to other liberties guaranteed as fundamental rights under the Constitution. Privacy is an element of human dignity, and ensures that a human being can lead a life of dignity by, among other things, exercising a right to make essential choices, to express oneself, dissent, etc. Dignity is, consequently, an intrinsic aspect of the right to life and liberty enshrined under Article 21 of the Constitution, as 'life' was not limited to mere existence, but is made worth living because of the attendant freedom of dignity. It is only when life could be lived with dignity that liberty could be of any substance.

iii. **Commitment to international obligations**: The recognition of privacy as fundamental constitutional value was a part of India's commitment to safeguard human rights under international law under the International Covenant of Civil and Political Rights **("ICCPR")** which found reference in domestic law under the Protection of Human Rights Act, 1993. The ICCPR recognizes a right to privacy. The Universal Declaration of Human Rights too specifically recognizes a right to privacy. The Judgment has held that constitutional provisions had to be read and interpreted in a manner such that they were in conformity with international commitments made by India.

V. Data Protection / Informational Privacy

The Judgment at several places deals with informational privacy (especially in the context of the inter-connected digital world), both in the hands of state and non-state entities. The Court additionally highlighted the importance of surveillance functioning within prescribed limits and with necessary safeguards. The judgement discusses various aspects of collection, use and handling of data e.g. big data, data analytics, use of wearable devices and social media

16. 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.

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

networks resulting in the generation of vast amounts of user data relating to end users' lifestyles, choices and preferences, use of cookies files on browsers for tracking user behavior and for the creation of user profiles. The judgment specifically deals with informational privacy but a substantial part of the discussion is on the handling of information by the State. Essentially, the new general data protection law to be introduced to protect rights of individuals against non-State parties should deal with these aspects amongst other things.

VII. 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[18] and 21 of the Constitution as mentioned below:

- the 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 would be legitimate aim of the state, 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.

18. 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".*

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.[19]

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.

B. 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,[20] will not apply to any body corporate providing services relating to collection, storage, dealing or handling of

19. 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.

20. Rules 5 and 6 in particular.

SPDI under a contractual obligation with any legal entity located within or outside India. The rules will, however apply to a body corporate, providing services to the provider of information under a contractual obligation directly with them. This clarification thus brought in a lower compliance requirement for 'Data Processors', as have come to be known under the Draft 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.

C. 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.

D. 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.[21]

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:

21. Section 72A, IT Act.

ii. SDPI

As per the IT Act, where a body corporate, possessing, dealing or handling any SPDI is negligent in implementing security measures, and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the affected person.[22] 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.[23]

II. Industry Specific Regulations

A. Telecommunications Law

The *Indian Telegraph Act, 1885*[24] *and the Indian Telegraph Rules, 1951*[25] 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")**[26] 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.

22. Section 43A, IT Act.
23. Section 75, IT Act.
24. Section 5 of the Indian Telegraph Act, 1885.
25. Rule 419A of the Indian Telegraph Rules, 1951.
26. http://www.dot.gov.in/sites/default/files/2016_03_30%20UL-AS-I.pdf?download=1. Last accessed: November 9, 2018.

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.

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*,[27] *RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds*,[28] *RBI Report on Information Systems Security Guidelines for the Banking and Financial Sector*,[29] *RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks*,[30] *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*,[31] *RBI's Master Circular on Customer Service in Banks, 2014*,[32] *and RBI's Master Circular on Credit Card Operations of Banks*.[33]

Importantly, RBI released the Storage of Payment System Data Directive, 2018[34] 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.

C. 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")**.[35] The SEBI Circular is only applicable to Clearing Corporations, Depositories and Stock Exchanges **("MIIs")**.

The SEBI Circular extensively covers the obligations of the MIIs as far as maintaining their IT infrastructure is concerned, such as the need to establish a Cyber Security and Cyber Resilience Policy, along with confidentiality and privacy requirements to be followed by MMIs.

D. Insurance

The insurance regulator, the Insurance Regulatory and Development Authority of India **("IRDAI")** has in place a number of regulations and guidelines which contain provisions on data security. Examples are the *'Guidelines on Information and Cyber Security for Insurers'* **("Insurer Guidelines")**,[36] IRDAI *(Outsourcing*

27. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF. Last accessed: November 9, 2018.
28. https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf. Last accessed: November 9, 2018.
29. https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=275. Last accessed: November 9, 2018.
30. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=3148&Mode=0. Last accessed: November 9, 2018.
31. https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9848. Last accessed: November 9, 2018.
32. https://www.rbi.org.in/scripts/bs_viewmascirculardetails.aspx?id=9008. Last accessed: November 9, 2018.
33. https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7338. Last accessed: November 9, 2018.
34. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Last accessed: November 9, 2018.
35. http://www.sebi.gov.in/sebi_data/attachdocs/1436179654531.pdf. Last accessed: November 9, 2018.
36. https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20

of Activities by Indian Insurers) Regulations, 2017,[37] *IRDAI (Maintenance of Insurance Records) Regulations, 2015*,[38] *and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017*.[39] 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.[40]

E. 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.

Information%20and%20Cyber%20Security%20for%20 insurers.pdf. Last accessed: November 9, 2018.and%20 Cyber%20Security%20for%20insurers.pdf. Last accessed: November 9, 2018.

37. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_ Layout.aspx?page=PageNo3149&flag=1. Last accessed: November 9, 2018.
38. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_ Layout.aspx?page=PageNo2604&flag=1. Last accessed: November 9, 2018.
39. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_ Layout.aspx?page=PageNo3191&flag=1. Last accessed: November 9, 2018.
40. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_ Layout.aspx?page=PageNo3149&flag=1. Last accessed: November 9, 2018.

4. New Data Protection Law Proposed in India

I. Background

The much-awaited *draft Personal Data Protection Bill, 2018* **("Draft Bill")** was released by a committee set up by the Indian Government **("Committee")** on July 27, 2018. The Committee, chaired by retired Supreme Court judge, Justice Srikrishna, was constituted in August 2017 by the MeitY to examine issues related to data protection, recommend methods to address them, and issue a draft data protection law. The Bill is accompanied by its report titled "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*" **("Report")** which provides context to the deliberations of the Committee.

MeitY may accept, reject or alter such Draft Bill. Thereafter, the Draft Bill would need to be approved by the Union Cabinet before it is introduced in the Parliament for deliberations. The MeitY invited public comments on the draft bill which concluded on October 10, 2018. The Draft Bill is intended to be implemented in a staggered manner once enacted.

Major highlights of the proposed law to be kept in mind are as follows:

II. Highlights of the Draft Law

The Draft Bill applies to the processing of both Personal Data **("PD")** and Sensitive Personal Data **("SPD")** of natural persons. The natural person whose data is being processed is referred to as a **"Data Principal"**.[41] Unlike the existing law which regulates only SPD, the proposed law regulates both PD and SPD. Further, the proposed law applies to both manual and automated processing.

A. 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.

B. Sensitive Personal Data

SPD is a subset of PD and consists of specified types of data, such as 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. The Data Protection Authority (as explained hereunder) has the power to declare further categories of data as SPD.

C. Processing

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

Entities processing personal data may be either **"Data Fiduciaries"** (the entity that determines the purpose and means for processing) or **"Data Processors"** (the entity that processes personal data on behalf of a Data Fiduciary). Therefore, depending on the role played by the entity in the processing of data, such entity may be classified as either a Data Fiduciary or Data Processor and will accordingly need to comply with corresponding obligations.

D. Anonymized Data

In addition, the Draft Bill specifically excludes the processing non-personal or anonymized data from the ambit of PD.

41. Section 3(14), Draft Bill.

E. Extra Territorial Application

In addition to being applicable to the processing of personal data collected within the territory of India, and collected by Indian citizens/ companies; the Draft Bill is designed to have extra territorial application. It is linked to the processing of data of Indian Data Principals by Data Fiduciaries or Data Processors not present within the territory of India; if such processing is *"(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to Data Principals within the territory of India; or (b) in connection with any activity which involves profiling of Data Principals within the territory of India"*.

We have captured the scope of the law in the below table:

Applicability of the Draft 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.	✓	✗

III. Major Obligations

A. 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")**. This Notice should be clear, concise and comprehensible and specifies that a Notice may be issued in multiple languages whenever necessary.

B. Purpose and Collection Limitation

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 for the purposes specified to the Data Principals, or for any other incidental purpose that the Data Principals would reasonably expect the personal data to be used for. Therefore, using data for new (or previously unspecified) purposes should therefore need fresh consent.

C. Storage Limitation

Personal data may be retained only until the purpose of collection is completed. Data Fiduciaries must 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.

IV. Grounds for Processing PD and SPD

A. Consent

The Draft Bill lays down the test for 'valid consent' for PD, i.e. consent which is free, informed, specific, clear and capable of being withdrawn. For SPD, explicit consent is required for which the terms "informed", "clear" and "specific" need to meet a higher threshold. The Codes of Practices to be issued or approved by the Authority are likely to provide further guidance to achieve valid consent / explicit consent.

B. Ability to Process Data on Grounds other than Consent:

The Draft Bill permits the processing of data without consent for functions of the State,[42] in compliance with law or with the order of any Court or Tribunal,[43] where it is necessary for prompt action,[44] in specific instances where processing is necessary for purposes necessary for employment,[45] and for reasonable purposes – that must be specified by the Data Protection Authority.[46]

V. Personal and Sensitive Personal Data of Children

Age of consent: The Draft Bill mandates that parental consent will be necessary for the processing of PD of children below the age of eighteen years.[47]

Guardian Data Fiduciaries: Data Fiduciaries who operate commercial websites/online services directed at children; or process large volumes

42. Section 13, Draft Bill.
43. Section 14, Draft Bill.
44. Such as medical emergencies, or in for safety in situations of breakdown of public order – Section 15, Draft Bill. Section 16, Draft Bill.
45. Section 16, Draft Bill.
46. Section 17, Draft Bill.
47. Section 23, Draft Bill.

of personal data of children will be notified as 'guardian data fiduciaries'.

Obligations of Data Fiduciaries: Data Fiduciaries are to verify the age of children and seek parental consent before processing their PD. Thus, the obligation to ensure age gating / verification and the necessary tools will have to be implemented by businesses. The only entities exempted from this requirement are those guardian data fiduciaries who exclusively provide counseling or child protection services.

Restrictions on Processing: These 'guardian data fiduciaries' shall be barred from undertaking activities such as profiling, tracking, behavioral monitoring, or targeting advertising directed at children, or any form of processing that could cause significant harm[48] to children.

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

The Draft Bill provides detailed rights to the Data Principal to access and correct their data. With regards to a right of review, the Draft 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 Draft Bill into a detailed step-wise process for how correction, completion or updating of the PD should be done.

VII. Data Portability

In an attempt to grant users more control over their data, the Draft 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 Draft Bill however does not specify the technical specifications of such a format, or what would be threshold for 'common use' of the format.

The PD which would have 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; (iii) data which forms part of any profile on the Data Principal, or which the Data Fiduciary has otherwise obtained.

VIII. Right to be Forgotten

The Draft 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.

IX. Cross-Border Data Transfers and Data Localization

A. Data localization

- As a general rule, PD can be processed outside India but at least one copy of all PD should be stored on a server or a data center located in India, unless specifically exempted from this requirement.
- Certain critical PD may be identified by the Government which should be processed only in servers / data centers India and cannot be transferred outside India.

B. Cross Border Transfers

The Draft Bill proposes that PD may be transferred outside India only when:[49]

a. The transfer is subject to standard contractual clauses or intra-group schemes (for within group entities, similar to binding corporate rules) approved by the Authority, [50] or

48. Section XVII, Draft Bill.

49. Section 41 of the Draft Bill.

50. The Authority may only approve standard contractual clauses or intra-group schemes that effectively protect the Data

b. The Indian Government (in consultation with the DPA) prescribes a particular country or section within a country or a particular international organization for which the transfer is permissible,[51] or

c. The Authority approves particular transfer(s) due to necessity.

In addition to either of points (a) or (b) above being fulfilled, the Data Principal should also consent to such PD 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 transfer. The Draft 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 permissible where such transfer is necessary for a class of Data Fiduciaries or Data Principals and the enforcement of the Indian law is not hampered.

X. Breach Notifications

If there is a breach of Personal Data processed by the Data Fiduciary which is likely to cause harm to the Data Principal, the Data Fiduciary should notify the Data Protection Authority of such breach. The notifications should contain certain particulars, either submitted to the Data Protection Authority together or in phases.

There is no specific time period prescribed under the Draft Bill for the breach notification reporting, however, such reporting is to be done as soon as possible. The Data Protection Authority, once set up, may prescribe a certain time period for reporting.

XI. Significant Data Fiduciary

The Authority is empowered to notify certain Data Fiduciaries or entire classes of Data Fiduciaries as Significant Data Fiduciaries **("SDF").**[52] The concept of a SDF appears to stem from the Committee's attempt at identifying and regulating entities that are capable of causing significantly greater harm to Data Principals as a consequence of their data processing activities.

Accordingly, the Draft Bill proposes that such SDF register itself with the Data Protection Authority and prescribes for greater levels of compliances which would need to be undertaken by such SDF such as carrying out data protection impact assessments, record keeping, data audits, and the appointment of a data protection officer.

XII. Data Protection Authority

The Draft Bill also contemplates the creation of an independent Data Protection Authority which hitherto did not exist in India. The Authority has been given a wide range of powers, which include inter alia enforcing the

Principal's rights, including in relation to further transfers from the transferee of the PD.

51. 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.

52. 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 resulting from any processing or any kind of processing undertaken by the fiduciary;*
e. *use of new technologies for processing; and*
f. *any other factor relevant in causing harm to any data principal as a consequence of such processing.*

Such SDFs would need to adhere to certain additional compliances such as conducting data protection impact assessments, record-keeping, data audits and appointing a data protection officer.

provisions of the Draft Bill, specifying residual categories of SPD, specifying circumstances a DPIA needs to be undertaken, registering SDFs and Data Auditors, etc. These functions appear to be multi-faceted as they are administrative, rule-making and quasi-judicial. In view of wide ranging rule making power, provisions have to be carefully examined to ensure that there is no excessive delegation.

In addition to its responsibilities of enforcing the provisions of the Bill, it is also heartening to see that inclusion of a Data Protection Awareness Fund, which will be funded out of the penalties recovered under the Draft Bill. In a country like India with a fast-growing digital population, the importance of educating the public on good data security practices cannot be overemphasised.

XIII. Codes of Practice

Do note that the Draft Bill contemplates codes of practice (similar to a self-regulatory mechanism) also to be issued by the Data Protection Authority or approved by the Authority if submitted by an industry or trade association. These codes of practice should address more granular points of implementation including related to various compliances under the Draft Bill, such as on notice requirements, retention of Personal Data, conditions for valid consent, exercise of various rights by users, transparency and accountability measures, methods of destruction / deletion / erasure of Personal Data, breach notification requirements, cross-border data transfers, etc.

XIV. Privacy by design

Similar to the GDPR, Data Fiduciaries will be required to implement managerial, organizational, business and technical systems, policies and measures to ensure that the user privacy of the user is protected.

XV. Penalties, Offences and Compensation

The Draft Bill contemplates penalties to be paid to the Government, compensation to the Data Principal as well as criminal liability in certain cases. The Draft Bill as such differentiates between PD and SPD related offences and penalties depending on the level of harm caused to the Data Principal (significant harm for PD related offences v. harm for SPD related offences).

i. Penalties and Offences

The Draft Bill goes down the GDPR route in terms of financial penalties by not only proposing the imposition of fixed financial penalties (ranging from rupees five crore to fifteen crore – (i.e. approx. USD 728,600-2,185,800) but also penalty based upon a certain percentage (ranging from 2-4%) of its 'total worldwide turnover' in the preceding financial year, in some specific cases: processing of Children's PD, failure to implement security safeguards, data transfers, not taking prompt and appropriate action in case of a data security breach, DPIA, etc., Further, 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.

The Report indicates that the intention behind such inclusion is that if the group companies have benefitted from any unlawful processing undertaken by the Data Fiduciary in India than such group entities should also be subject to penalties.

Further, the Draft Bill includes criminal penalties (ranging from 3-5 years of imprisonment) for intentional, reckless and damage caused with knowledge, for certain offences.

ii. Compensation

The Draft Bill further 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. The 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.

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 Draft 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 Draft 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 a SDF (if classified as one).

Notably, the Draft 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 RBI even requested for regular updates from stakeholders on the status of their compliance efforts. MNCs would be especially affected by the RBI mandate, and may have had to relocate data stored and processed in other countries. 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 Draft 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 Draft 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.

Personal data can be processed outside India but at least one copy of all personal data and sensitive personal data is to be stored on a server or a data center located in India. For instance, businesses such as digital platforms, cloud service providers, AI and machine learning service providers etc. whether Indian or offshore, processing 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 has largely gone unnoticed.

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").**[53] 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%.[54] 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. 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[55]), 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.[56]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.

- Secondly, given that the Draft 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 significant data fiduciaries. The draft law specifically requires that even off shore significant data fiduciaries 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

53. 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.).

54. Excluding surcharge and cess.

55. A.A.R. No 1573 of 2014.

56. 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.

conducting activities in India that support the foreign enterprise in providing services in India then an agency PE could be created.

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

It is clear that the various policies that are proposed to be introduced including the Draft Data Protection 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 Draft Bill draws inspiration from the European Union's General Data Protection Regulation **("GDPR")** in multiple instances. A comparison between the Draft Bill and the GDPR is as follows:

	EU - GDPR	India – Draft 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.[57]	Similar to the GDPR, the Draft 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.[58]
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'[59] and 'sensitive personal data'[60]. The processing of sensitive personal data is subject to similar conditions as provided for in GDPR.
Data Localization	There is no data localization requirement in the EU.	One copy of all personal data 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.[61]
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 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 due to necessity. Further, such transfers must be consented to.

57. Article 3, GDPR.

58. Section 2, Draft Bill, 2018.

59. "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;

60. 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.

61. Section 40, Draft Bill, 2018.

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 Draft 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.[62] 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 fiduciaries[63] may not permitted.
Penalties	The maximum penalty up to 4% of global turnover or 20,000,000 euros (approx. USD 23,061,000) whichever is higher will be imposed in situations of non-compliance such as the violation of basic principles such as in relation to processing, consent, data subject rights, and cross border transfers.[64] 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.[65] Further, both civil and criminal offences have been prescribed.

62. Article 8, GDPR.

63. 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.

64. Article 83, GDPR.

65. Section 69, Draft 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 the Draft Bill to become law. However, irrespective of a general data protection law coming into force, industry practice has been to self-regulate to keep up with globally accepted standards of data protection and consumer interests.

Industries such as banking (the RBI's Data Localization Circular is an example), and potentially healthcare (the draft DISHA bill) have been proactive in regulation, and have in place guidelines and safeguards even in the absence of a general law. Business models, therefore will have to keep up with industry and sector-wise regulation and guidelines, irrespective of a general data protection law being in force.

About NDA

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

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

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

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

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

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

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

- **IFLR1000 2019:** Tier 1 for Private Equity and Project Development: Telecommunications Networks.
- **AsiaLaw 2019:** Ranked 'Outstanding' for Technology, Labour & Employment, Private Equity, Regulatory and Tax
- **RSG-Financial Times:** India's Most Innovative Law Firm (2014-2017)
- **Merger Market 2018:** Fastest growing M&A Law Firm
- **IFLR:** Indian Firm of the Year (2010-2013)
- **Legal 500 2018:** Tier 1 for Disputes, International Taxation, Investment Funds, Labour & Employment, TMT
- **Legal 500 (2011, 2012, 2013, 2014):** No. 1 for International Tax, Investment Funds and TMT

- **Chambers and Partners Asia Pacific (2017 – 2018):** Tier 1 for Labour & Employment, Tax, TMT
- **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

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

Fund Formation: Attracting Global Investors

March 2018

Social Impact Investing in India

July 2018

The Curious Case of the Indian Gaming Laws

February 2018

Corporate Social Responsibility & Social Business Models in India

March 2018

Incorporation of Company LLP in India

April 2017

Outbound Acquisitions by India-Inc

September 2014

Internet of Things

January 2017

Doing Business in India

September 2018

Private Equity and Private Debt Investments in India

March 2018

NDA Insights

TITLE	TYPE	DATE
Blackstone's Boldest Bet in India	M&A Lab	January 2017
Foreign Investment Into Indian Special Situation Assets	M&A Lab	November 2016
Recent Learnings from Deal Making in India	M&A Lab	June 2016
ING Vysya - Kotak Bank : Rising M&As in Banking Sector	M&A Lab	January 2016
Cairn – Vedanta : 'Fair' or Socializing Vedanta's Debt?	M&A Lab	January 2016
Reliance – Pipavav : Anil Ambani scoops Pipavav Defence	M&A Lab	January 2016
Sun Pharma – Ranbaxy: A Panacea for Ranbaxy's ills?	M&A Lab	January 2015
Reliance – Network18: Reliance tunes into Network18!	M&A Lab	January 2015
Thomas Cook – Sterling Holiday: Let's Holiday Together!	M&A Lab	January 2015
Jet Etihad Jet Gets a Co-Pilot	M&A Lab	May 2014
Apollo's Bumpy Ride in Pursuit of Cooper	M&A Lab	May 2014
Diageo-USL- 'King of Good Times; Hands over Crown Jewel to Diageo	M&A Lab	May 2014
Copyright Amendment Bill 2012 receives Indian Parliament's assent	IP Lab	September 2013
Public M&A's in India: Takeover Code Dissected	M&A Lab	August 2013
File Foreign Application Prosecution History With Indian Patent Office	IP Lab	April 2013
Warburg - Future Capital - Deal Dissected	M&A Lab	January 2013
Real Financing - Onshore and Offshore Debt Funding Realty in India	Realty Check	May 2012

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 65509855

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

375 Park Ave Suite 2607
New York, NY 10152

tel +1 212 763 0080

Privacy & Data: India's Ticket to Global Technological Supremacy