

Technology Law Analysis

January 06, 2021

PRIVACY AND DATA PROTECTION – INDIA WRAP 2020

2020 was the year in which the world went more digital than ever before, owing to the pandemic that altered life as we knew it. One of the silver linings of the year was the spotlight on the importance of data and data flow. Taking this cue, the Indian Government took significant steps in tech policy and data regulation in 2020, viz. non-personal data, health data, financial data, and data related to e-commerce and other consumer facing services. The judiciary has also made observations on individual rights regarding data privacy, and the ever-deliberated *Personal Data Protection Bill*, 2019 (“PDP Bill”) was a moving piece under Government deliberation during the year.

The highlights are as follows:

1. THE LOOMING PROPOSED PRIVACY LAW

Inspired by the GDPR, the PDP Bill was proposed in 2019 to bring about a comprehensive overhaul to India's current data protection regime, which is currently governed by the *Information Technology Act, 2000* and the rules thereunder. The current draft of the PDP Bill prescribes compliance requirements for all forms of personal data, broadens the rights given to individuals, introduces a central data protection regulator, as well as institutes data localization requirements for certain forms of sensitive data. The PDP Bill applies extra territorially to non-Indian organizations in the event certain nexus requirements are met, and also imposes hefty financial penalties in case of non-compliance.

The PDP Bill was referred to a Joint Parliamentary Committee (“JPC”) on December 12, 2019 for recommendations. The JPC's report, after timeline extensions granted, is now due to be submitted to the Parliament, in the Budget Session to be tentatively held in January 2021.

The JPC has been conducting a number of meetings with Government ministries, industry bodies and various stakeholders; as well as holding meetings for clause by clause considerations of the PDP Bill. Importantly, as per recent reports,¹ the JPC is now planning to expand the scope of the PDP Bill from just personal data to ‘encompass overall data protection’ and non-personal data. As per further reports,² members of the JPC are still undecided and split over these key issues of data localization and Government access to data held especially by social media platforms among others, and some reports³ have confirmed that the PDP Bill will not be passed in its current version and that it will be “redrawn” by the JPC.

We expect considerable time until the PDP Bill is enacted, given the substantial delays in progress and recent reports on the scope of the PDP Bill being reopened and broadened. Whether there will be a change in scope of the PDP Bill, and specifically in the compliance requirements including data localisation and cross border data transfer restrictions and compliances under this proposed law is yet to be seen.

2. PROPOSED NON-PERSONAL DATA FRAMEWORK

The Ministry of Electronics and Information Technology, Government of India constituted a committee (“NPD Committee”) to explore the governance of non-personal data (“NPD”). The terms of reference of the NPD Committee were to: (a) study various issues relating to non-personal data; and (b) to make specific suggestions for considerations of the Central Government on the regulation of non-personal data. Currently, processing NPD is not regulated under law. Further, “anonymized data” is specifically excluded from the applicability of the current draft of the PDP Bill.

On July 12, 2020, the NPD Committee released their report⁴ on the Non-Personal Data Governance Framework for public comments. The report called for a separate NPD governance framework to be put into place. However, the report was not a well-articulated document in terms of definitions, proposed provisions and the purpose sought to be achieved by the framework.

Subsequently, in January 2021, the NPD Committee released a revised version of their report clarifying certain aspects. The revised report expands on how the PDP Bill and the recommended NPD framework would function in tandem, clarifying that it is only anonymised data that will fall under the NPD framework. The revised report, amongst other things, details the types of NPD that may be collected, delves into public and private rights that may subsist in such data, as well as provides for a detailed data sharing mechanism that exempts transfers between private entities. The report provides separate guidelines for ‘Data Businesses’⁵, or data collecting entities that meet certain thresholds, calls for the separate treatment of certain ‘High Value Datasets’⁶, and also calls for the creation of a separate regulator that would function independently.

However, as mentioned above, certain reports⁷ indicate that the JPC may be looking to broaden the scope of the PDP Bill to include NPD as well. These reports run contrary to the NPD Committee's recommendation for all NPD-related provisions in the PDP Bill to be removed. We expect more clarity once the JPC issues its report on the PDP Bill.

3. DATA EMPOWERMENT AND PROTECTION ARCHITECTURE FOR FINTECH

Research Papers

Horizon Technologies

January 21, 2025

Compendium of Research Papers

January 11, 2025

FAQs on Setting Up of Offices in India

December 13, 2024

Research Articles

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals

January 15, 2025

Key changes to Model Concession Agreements in the Road Sector

January 03, 2025

The Revolution Realized: Bitcoin's Triumph

December 05, 2024

Audio

Securities Market Regulator's Continued Quest Against “Unfiltered” Financial Advice

December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps

November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I

August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

“Investment return is not enough” Nishith Desai with Nikunj Dalmia (ET Now) at FI8 event in Riyadh

October 31, 2024

Analysing SEBI's Consultation Paper

In August 2020, NITI Aayog (a policy think tank run by the Government of India) released a draft framework on the Data Empowerment and Protection Architecture (“**DEPA**”) in consultation with a few industry regulators, banks and fintech players. Through DEPA, NITI Aayog aims to institute a mechanism for secure consent-based data sharing in the fintech sector, which they believe will be “*a historic step towards empowering individuals with control over their personal data*”⁸. DEPA aims to build over existing regulation by the RBI on ‘Account Aggregator’⁹ models, through which individuals will be able to share their financial data across banks, insurers, lenders, mutual fund houses, investors, tax collectors, and pension funds in a secure manner. While this document released by NITI Aayog is focused on the implementation of DEPA in the financial sector alone, DEPA is also proposed to be introduced as a similar framework beyond just financial data, and across all sectors, beginning with the health and telecom sectors.

While NITI Aayog goes into much detail on the motivation behind introduction of the DEPA platform, the exact process of how the architecture would be implemented is yet to be detailed. In order to fully implement DEPA, the relevant Government regulators and ministries would be required to release a detailed document that lays down the processes for the information flow in DEPA. DEPA was open for public comments until November 30, 2020, and there has been no further update till date.

4. A POLICY FOR THE MANAGEMENT AND SHARING OF HEALTH DATA

A National Digital Health Mission (“**NDHM**”) was announced by the Central Government and the Ministry of Health and Family Welfare (“**MOHFW**”) published a blueprint¹⁰ in late 2019 recommending the creation of a National Digital Health Ecosystem (“**Ecosystem**”) which allows for interoperability of digital health systems at the patient, hospital, and ancillary healthcare provider level. On December 14, 2020 the MOHFW approved¹¹ a Health Data Management Policy (“**HDM Policy**”)¹² largely based on the PDP Bill to govern data in the Ecosystem. The HDM Policy recognises entities in the data processing space, i.e. data fiduciaries (similar to data controllers under GDPR) and data processors similar to the PDP Bill, and establishes a consent framework for processing personal data.

The HDM Policy provides for rights to individuals, and provides for the creation of Health IDs for individuals, Health Practitioner IDs for medical practitioners, and Health Facility IDs for operators/owners of health facilities. It mandates data fiduciaries to abide by the basic data protection principles and establishes certain compliance requirements including security practices and impact assessments., the HDM Policy also allows for consent-based sharing of data and establishes a grievance redressal procedure through the National Health Authority. Guidelines for an ‘NDHM Sandbox’¹³ were also published in August 2020 to encourage the incubation of new technologies in a contained environment.

The HDM Policy will have a significant impact on the medical and pharmaceutical industry once implemented, as healthcare institutions will have increased compliance obligations and the telemedicine sector is set to become busier than before. However, the HDM Policy has significant overlaps with the PDP Bill, which may cause a conflict between the HDM Policy and the PDP Bill. It is therefore unclear why the HDM Policy was separately proposed, and in case of a conflict – which may prevail.

5. DATA IMPLICATIONS IN THE IMPENDING E-COMMERCE POLICY

A draft of the new e-commerce policy has reportedly been in the works¹⁴ and proposes to set up an e-commerce regulator with wide-ranging powers over e-commerce entities and platforms. The draft contained wide-ranging proposals on sharing source codes, algorithms and other data with the Government, use of non-personal data of consumers, anti-piracy, cross border data flows, etc. As per more recent media reports, the Central Government is in the ‘final stages’ of drafting India’s e-commerce policy¹⁵ and may set up an ‘investigation body’ to look into violations by e-commerce entities.¹⁶

It would be interesting to see whether many of the data related provisions such as on ownership, Government access and data sharing have been diluted in the e-commerce policy in light of industry feedback, and the provisions of the PDP Bill and the NPD governance framework currently under Government consideration.

6. GOVERNANCE OF DATA OBTAINED BY MOTOR VEHICLE AGGREGATORS

The Ministry of Road Transport and Highways published the Motor Vehicle Aggregator Guidelines 2020 (“**MV Aggregator Guidelines**”)¹⁷ on November 27, 2020 to regulate the business of transport aggregators and sets out recommendations for a licensing regime for aggregators; regulation of fares; compliances with regards to vehicles, apps and websites; ride-sharing, safety measures and ride cancellations. The MV Aggregator Guidelines state that the data generated on an aggregator’s app or website must be stored in India for a minimum of 3 months and maximum of 24 months from the date of generation. This data must also be made available to the State Governments as per law. It also prescribes that the aggregator must not disclose customer data without their written consent.

The Guidelines do not detail parameters on the scope of data covered, the conditions of storage, or any exemptions to the data localization requirement. Since both the Central Government and State Governments have legislative powers over motor vehicles¹⁸, and the *Motor Vehicles Act, 1988* provides that a State Government *may* follow guidelines notified by the Central Government on issuance of licenses to transport aggregators, it remains to be seen how individual State Governments implement these guidelines in their respective jurisdictions.

7. INDIAN JUDICIARY ON REGULATION OF PERSONAL DATA

⁸ The Kerala High Court in the case of *Balu Gopalakrishnan v. State of Kerala*¹⁹ passed an interim order on April 24, 2020 on the export of COVID-19 related data by the State Government of Kerala to a US-based entity, Sprinklr, for data analytics. The High Court held that certain measures were to be implemented by the State Government before granting Sprinklr access to the data. These measures include anonymizing the data, obtaining specific consent from citizens, and ensuring the return of data once contractual obligations end. The High Court also barred advertisements and the commercial exploitation of the data by Sprinklr. This judgment sets an important benchmark for all public-private partnerships in the post COVID-19 era in the field of data protection and emphasizes the accountability of the State in handling data of its citizens. Our detailed update on this matter is available [here](#).

⁹ The Odisha High Court in the case of *Subhranshu Rout @ Gugul v. State of Odisha*²⁰ observed in its order on November 23, 2020 the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The case involved objectionable content regarding a woman that was posted online. While the victim had not made any arguments with regard to the permanent removal of her data, the court encouraged the victim to seek

appropriate orders for the protection of their fundamental right to privacy even in the absence of an explicit right to be forgotten. The court went on to note that recognizing such a right by law would help in safeguarding woman's rights online, thus highlighting the importance of strong individual privacy rights. The court was cognizant of the fact that the current draft of the PDP Bill if passed as law, would introduce a right to be forgotten in India. Our detailed update on this matter is available [here](#).

8. THE EUROPEAN UNION COURT'S DECISION IN 'SCHREMS II'

In what has been a significant development in global data protection law, the Court of Justice of the European Union ("CJEU") in a case popularly known as *Schrems II*²¹ invalidated the EU-US Privacy Shield ("Privacy Shield") and read down the inviolability of the Standard Contractual Clauses ("SCCs"). The Privacy Shield is an adequacy decision issued by the European Commission ("EC") regulating data transfers between the United States of America ("US") and any member state of the European Union ("EU") or the European Economic Area ("EEA") data transfer framework. SCCs are contractual clauses approved by the EC under EU's data protection law, the General Data Protection Regulation ("GDPR") which may be incorporated into data transfer agreements to export data outside the EU or EEA. Adequacy decisions and SCCs are two amongst a host of permissible ways to transfer data outside the EU or EEA member states under the GDPR.

The CJEU invalidated the EC decision approving the Privacy Shield observing that due to the operation of surveillance laws in the US, the Privacy Shield does not provide adequate protection of data protection rights of an individual that is similar to the GDPR. It also ruled that the SCCs by themselves do not provide adequate protection of an individual's data protection rights and additional due diligence of the transferee's country's laws has to be made to be a legitimate cross-border transfer of data under the GDPR. This would have a direct impact on businesses transferring personal data from the EU or EEA to India since data transfers through the SCCs may be suspended at any time by an EU or EEA regulator if it opines that Indian Law operating along with the SCCs do not adequately offer protection to individual rights. Hence businesses may need to undertake a separate assessment of Indian laws in addition to the use of SCCs and implement appropriate safeguards to ensure that the adequate protection to individual rights is offered that is similar to the GDPR.

WHAT TO EXPECT IN 2021

2020 has laid the groundwork for a pipeline of developments on the privacy and data protection front. While we may see the scope and purpose of the PDP Bill broadened before it is tabled before the Parliament in 2021, we could also expect significant regulation on the economic and commercial usage of non-personal data, as well as ownership aspects. The PDP Bill may also be made available for discussion and stakeholder comments once the revised version is released. The position on data localization and cross border sharing of data is yet to be finalized, which is a policy decision that will impact most businesses operating in India. However, in the backdrop of the PDP Bill, we expect to continue to see industry-specific data policies and regulation by sectoral regulators such as drone-related policies which may give rise to new issues including cybersecurity and mandatory disclosure to the Government. It is also clear that the judiciary is more cognizant of privacy rights than ever before, which is a sign of a strong data protection regulation ahead.

– Purushotham Kittane, Inika Charles, Aaron Kamath & Gowree Gokhale

You can direct your queries or comments to the authors

¹ Available at <https://www.livemint.com/news/india/nothing-personal-about-data-protection-bill-11606194232029.html> (Last accessed on December 29, 2020).

² Available at <https://economictimes.indiatimes.com/tech/tech-bytes/joint-parliamentary-committee-split-over-draft-data-privacy-law-govt-access/articleshow/79483872.cms> (Last accessed on December 29, 2020).

³ Available at <https://theprint.in/india/data-protection-bill-wont-get-cleared-in-its-current-version-bjp-mp-rajeev-chandrasekhar/568003/> (Last accessed on December 29, 2020).

⁴ Available at https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf (Last accessed on December 29, 2020).

⁵ The NPD Committee report defines a 'Data Business' as any organization (Government or private organization) that collects, processes, stores, or otherwise manages data.

⁶ The NPD Committee report defines a 'High-value Dataset' as a dataset that is a public-good and benefits the community at large

⁷ Available at <https://www.livemint.com/news/india/nothing-personal-about-data-protection-bill-11606194232029.html> (Last accessed on December 29, 2020).

⁸ Available at https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf (Last accessed on December 29, 2020).

⁹ An Account Aggregator is defined by the RBI as a non-banking financial company that undertakes the business of an account aggregator i.e. providing under a contract, the service of, retrieving or collecting such financial information pertaining to its customer, as may be specified by banks from time to time; and consolidating, organizing and presenting such information to the customer or any other financial information user as may be specified by such banks. The RBI has notified directs for Account Aggregators available at <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0> (Last accessed on December 29, 2020).

¹⁰ Available at <https://nha.gov.in/home/ndhb> (Last accessed on December 29, 2020).

¹¹ Available at https://ndhm.gov.in/assets/images/media/press_releases/Press%20Release%20-%20Government%20of%20India%20approves%20Draft%20Health%20Data%20Management%20Policy.pdf (Last accessed on December 29, 2020).

¹² Available at <https://ndhm.gov.in/assets/uploads/NDHM%20Health%20Data%20anagement%20Policy.pdf> (Last accessed on December 29, 2020).

¹³ Available at https://nha.gov.in/assets/uploads/Sandbox_Guidelines_v6.pdf (Last accessed on December 29, 2020).

¹⁴ Available at <https://www.medianama.com/2020/07/223-second-draft-e-commerce-policy-india/> (Last accessed on December 29, 2020).

¹⁵ Available at <https://www.financialexpress.com/industry/sme/govt-e-commerce-policy-in-final-stages-of-drafting-retail-trade-policy-to-benefit-65m-small-traders/2115990/> (Last accessed on December 29, 2020).

¹⁶ Available at <https://www.financialexpress.com/economy/draft-e-commerce-policy-govt-mulls-new-probe-body-data-audits/2145985/> (Last accessed on December 29, 2020).

¹⁷ Available at https://morth.nic.in/sites/default/files/notifications_document/Motor%20Vehicle%20Aggregators27112020150046.pdf (Last accessed on December 29, 2020).

¹⁸ Motor Vehicles are covered under Item 35 – 'Mechanically propelled vehicles including the principles on which taxes on such vehicles are to be levied' of List III (Concurrent List) in the Seventh Schedule of the Constitution of India.

¹⁹ WP (C) 9498/2020.

²⁰ BLAPL No. 4592 of 2020.

²¹ *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems* (Case C-311/18) available at <http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=19983767> (Last accessed on December 29, 2020).

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US

any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.

