Non-Personal Data 2.0

Mapping the way forward for optimal regulation of Non-Personal Data

CUTS International

#2211

Non-Personal Data 2.0

Mapping the way forward for optimal regulation of Non-Personal Data

Published By

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org
Web site: www.cuts-international.org

Authors
Sidharth Narayan and Vidushi Sinha (CUTS International)

#2211

Table of Contents

Acknowledgements

This paper has been prepared with the efforts, guidance and support of several people who have been very kind to spare their valuable time for contributing to this paper. This paper has seen the involvement of multiple stakeholders in various forms, including direct inputs, timely reviews, incessant encouragement, and guidance.

The paper also underwent feedback from several experts in the field of data governance. In this regard, the following experts deserve a special mention for sparing their precious time to share very valuable inputs and comments:[1]

- Mr. Ameya Naik, Head of Policy, eGov Foundation
- Ms. Aparajita Bharti, Founding Partner, Quantum Hub
- Ms. Barbara Prainsack, Head - Research Platform Governance of Digital Practices and Chair - European Group on Ethics in Science and New Technologies (EGE), University of Vienna
- Ms. Brinda Lashkari, Policy Associate, eGov Foundation
- Ms. Charlotte Ducuing, PhD Fellow Researcher, Centre for IT and IP law (CITIP), KU Leuven
- Dr. Geeta Gouri, Former Member, Competition Commission of India
- Ms. Linnet Taylor, Professor of International Data Governance, Tilburg Institute for Law, Technology, and Society (TILT) and Lead, Global Data Justice Project
- Ms. Niti Chatterjee, Principal Associate, Shardul Amarchand Mangaldas
- Mr. Supratim Chakraborty, Partner, Khaitan and Co.
- Mr. Setu Bandhopadhyay, Technology Policy Analyst
- Mr. Siddharth de Souza, Postdoctoral Researcher at the Global Data Justice Project and Tilburg Institute for Law, Technology, and Society (TILT)
- Mr. Tommaso Fia, PhD Researcher, European University Institute

We also appreciate the efforts of our colleagues, Madhuri Vasnani, for editing, Rajkumar Trivedi, and Mukesh Tyagi, for preparing the layout of this report. Vijay Singh and Akshay Sharma deserve a special mention for their contribution to the outreach of the report.

We are thankful to Pradeep S Mehta, Secretary-General and Bipul Chatterjee, Executive Director, CUTS International, for their thorough and timely guidance, input, and encouragement.

[1] It is to be noted that their comments and suggestions were accepted/ rejected solely at the discretion of CUTS, and any errors in the report are solely made by CUTS.

We also express our sincere gratitude to all such individuals, whether or not named above, without whom the publication of this report would not have been possible. CUTS International will not profit from this report since it is for informative and educational purposes. Any error that may have remained is solely ours.

Executive Summary

Background and Context

This paper seeks to analyse the recommendations of the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 (PDPB'19). The proposed recommendations pertain to widening the ambit of the PDPB'19, by incorporating NPD aspects of Non-Personal Data (NPD) in it, and renaming it as the Data Protection Bill 2021 (DPB'21).

The key proposed changes include empowering the GoI to frame rules on NPD (including the steps to be taken by Data Protection Authority (DPA) in case of breach of NPD under the draft DPB'21), permitting the Data Protection Authority (DPA) to govern NPD in instances of a data breach and provides for criminal liability in case of re-identification from NPD.

The first section of this paper provides a brief contextual understanding and developments (such as prevalence of data breaches) over the years which preceded the latest version of the draft DPB'21. This includes the long deliberations on the J. Srikrishna Committee Report titled 'A Free and Fair Digital Economy- Protecting Privacy, Empowering Indians'. PDPB'19 and the two Kris Gopalakrishnan NPD reports.

A special emphasis has also been placed on the seemingly disjoint developments in the data regulatory landscape, including Open Network for Digital Commerce, Reserve Bank of India's (RBI) Account Aggregator framework, Draft India Use and Accessibility Policy, National Data Governance Framework Policy, draft Health Data Retention Policy and the new cybersecurity and breach reporting directions by the Indian Computer Emergency Response Team (Cert-In guidelines)- all of which seem to indicate a shift from the privacy goalpost of GoI to realising the economic value of data.

Analysis of Incorporation of NPD in DPB'21

The recommendations proposed by the JPC have been lauded for rekindling the debate on NPD, which has been missing in the public domain for a while. It can also be argued that by including NPD in the DPB'21, several concerns such as categorisation or splitting of datasets shall not be required as all datasets shall automatically fall under the safety net of DPB'21 and be regulated.

This being said, the recent JPC recommendations are not minor tweaks but rather major amendments which alter the scope of the proposed Bill altogether. Further, several concerns have arisen due to the inclusion and regulation of NPD. In this light, the paper deep dives into analysing the incorporation of aspects of NPD aspects in the current Indian landscape. In doing so, the following concerns are identified:

- Premature and piecemeal regulation of NPD:
  Firstly, there is a lack of understanding and clarity regarding the value, nature and sensitivity of data, data sharing mechanisms and possible benefits derived from the sharing of NPD. Despite the final report of the Gopalakrishnan Committee pending to come in the public

domain, the JPC has recommended including NPD aspects in the draft DPB'21 without adequate cost-benefit analysis, or exploration of good international practices.

Secondly, the JPC report rightly opined that different layers of protection or security are required for sensitive, non-sensitive, personal data and NPD. However, citing administrative impossibility to differentiate personal data and NPD, it recommends both to be regulated under the same enactment, without separate treatment of personal data and NPD in mixed datasets.

- Vague definition of NPD:
  The draft DPB'21 provides a vague definition of NPD. It does not take cognizance of different types of NPD classified under the Gopalakrishnan Committee report, such as public, private and community NPD or general, sensitive and critical NPD.

- Dilution of the objective of individual privacy of PDPB'19:
  The objectives and envisaged outcomes of personal data protection and NPD governance are at odds with each other, therefore, inclusion of NPD in PDPB is not appropriate.

- Over-burdened and architectural issues of DPA:
  There is a risk of putting too much too soon on the proposed Data Protection Authority (DPA) to regulate both personal data and NPD, even before its inception and with existing regulatory and architectural issues. It is feared that issues such as jurisdictional turf wars, wide range of powers and functions, DPA's high discretion and transaction intensive powers may be exacerbated

- Government access to NPD without guardrails:
  As discussed in the Gopalakrishnan Committee's reports, the nuances of NPD sharing do not seem to have been considered. Further, in light of recent regulatory developments in the data landscape, there seem to be certain functional overlaps.

- Possible impact on start-ups:
  The unfettered power of GoI to explicitly frame any policy for handling of NPD (including anonymised personal data) and mandatory data-sharing requirements are a cause of concern to start-ups. It poses competition concerns and potential loss of investment.

- Uncertainty for data processors:
  India's Business Process Outsourcing (BPO) and cloud service provider sector caters to many foreign clients. Therefore sharing their NPD may have cross-jurisdictional complications, dissuading foreign conglomerates from outsourcing their business processes to the Indian industry.

Recommendations and Way Forward

On the basis of the lacunae identified, a few action points have been provided below, as the way forward.

- ***Action Point 1:*** *Exclude NPD from the applicability ambit of the bill*
- ***Action Point 2****: Narrow down the scope and definition of NPD, recognise different types of NPD and publish informative guidance*
- ***Action Point 3****: Operationalise two separate frameworks for personal data and NPD and continue developing a nuanced understanding of different data sets*
- ***Action Point 4****: Recommended changes in draft DPB'21 for restricting powers of DPA to personal data breach and removing references to NPD breach*
- ***Action Point 5: (Arguendo to Action Point 1)*** *Recommended alterations in the draft DPB'21 to provide a few checks and balances on the unfettered government access to NPD*

1. Background

1.1 Run-up to the draft DPB'21

India currently lacks a dedicated personal data protection and privacy law. While the need for the same has been felt since many years, it became pressing in 2017, when privacy was declared as a fundamental right by the Supreme Court of India (SC), vide the Puttaswamy judgement.[2]

Around the same time, the Government of India (GoI) had setup a Committee of Experts under the Chairmanship of retired Justice B. N. Srikrishna (Srikrishna Committee), which submitted its report 'A Free and Fair Economy – Protecting Privacy, Empowering Indians'[3] in 2018, along with a draft Personal Data Protection Bill 2018 (draft PDPB'18).[4]

The draft PDPB'18 went through changes after stakeholder consultation, and the GoI tabled the Personal Data Protection Bill 2019 (PDPB'19) in Parliament.[5] The same was referred to a Joint Parliamentary Committee (JPC), under the Chairmanship of Shri P. P. Chaudhary, Member of Parliament (MP), Lok Sabha (Smt. Meenakshi Lekhi, MP, was the erstwhile Chairperson). After stakeholder consultation and a gap of around two years, the JPC submitted its report on the bill, which also entailed a draft Data Protection Bill, 2021 (draft DPB'21).[6]

1.2 NPD Debate in India so far

The NPD regulation debate in India began with the Expert Committee on NPD Governance Framework (Gopalakrishnan Committee), which submitted its first report in July 2020,[7] and revised report,[8] after stakeholder consultation in December 2020. The report(s) are based on

2 Justice K. S. Puttaswamy v. Union of India, 2017 10 SCC 1, Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

3 The Srikrishna Committee Report, available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

4 Draft Personal Data Protection Bill 2018, available at: https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

5 Personal Data Protection Bill 2019, available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

6 Report of the Joint Parliamentary Committee on the Personal Data Protection Bill 2019, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

7 The Gopalakrishnan Committee First Report, available at: https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

8 The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

certain assumptions,[9] which raise multiple concerns.[10] However, the report(s) have been lauded for certain aspects, such as highlighting the promotion of innovation and public benefits that can potentially be derived from data[11] and for covering the interface between regulation for NPD and PDPB'19.[12] The Gopalakrishnan Committee Report stated, "*it would be appropriate to amend the provisions of the PDPB to ensure that it does not regulate NPD*."[13] And it further clarified that "*the PDPB will govern mixed datasets that typically have inextricably linked personal and NPD*".[14]

This also resonated with global practices, particularly EU, wherein a dataset is split to process personal data and NPD separately. Even though there are some emerging concerns on the interpretation of the term 'inextricably linked' and regulation of mixed datasets[15], the European Commission's evaluation of the regulation implementation is awaited.[16] Notably, the dynamic

[9] Assumptions include the following:
   a. Nature of Data: The Report does not adequately identify a comprehensive problem statement that it wants to address through enabling data sharing for public interest purposes in the same way as other material resources. Further, as regards High Value Datasets (HVDs) being public goods, the Report identifies data as 'public good' without considering the externalities that might emerge from such interpretation.
   b. Value of Data: The Report assumes that regulation is a silver bullet to unlock and internalise the value of data without identifying problems with the existing scenario, establishing market failure, considering the capacities of the community, data trustees and data requestors to leverage the data access such that its value can be realised. Further, the Report assumes that a community's understanding of data is similar to other resources, and through data trustees, communities will be able to leverage the value of data.
   c. Benefits of Sharing: The Report assumes that data sharing with the government and other stakeholders leading to 'public interest' purposes as envisaged by the Report will motivate data custodians to sustain their data collection and processing mechanisms. Further, that businesses will be able to leverage data sharing opportunities and deliver on the promise of public interest. Also, the Report assumes that trust relationships can be established within the data economy in India without considering existing realities and dynamics between different stakeholders.
   Refer to: Navigating the Puzzle of Non-Personal Data Sharing, available at: https://cuts-ccier.org/pdf/report-navigating-the-puzzle-of-npd-sharing.pdf

[10] Concerns include the following:
   a. Nature of Data: There also exists a need to question - is data similar to other economic resources? And, in what form is the value derived from data, specifically in the Indian context?
   b. Value of Data: What considerations should be taken for assigning value to the data in the Indian context? Are there any use cases in which data has been valued in quantifiable terms? And, who are the stakeholders involved in such value creation?
   c. Benefits of Sharing: We lack an understanding of consumer behaviour regarding data sharing in the Indian context. Thus, the government may need to assess - how do data principals currently share data? Will they still be willing to share data if they know that data may be shared with government entities in some form? And, even if data sharing remedies such as portability exist, can they leverage its full benefits?
   Refer to: Navigating the Puzzle of Non-Personal Data Sharing, available at: https://cuts-ccier.org/pdf/report-navigating-the-puzzle-of-npd-sharing.pdf

[11] CUTS Comments on the Revised Report of the Committee of Experts on Non-Personal Data Governance Framework, available at: https://cuts-ccier.org/pdf/comments-on-revised_npd-governance-framework.pdf

[12] Clause 5.3, The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

[13] Clause 5.3, The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

[14] Clause 5.1, The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

[15] TRUSTS Trusted Secure Data Sharing Space, available at: https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf

[16] The European Commission is slated to submit a report on the implementation of the Regulation by 29 November, 2022.

nature and the notion of personal data in the data economy makes it difficult, if not squarely impossible, to identify NPD once and for all.

1.3 Key changes made to the PDPB'19 in the draft DPB'21 wrt NPD

The key proposed changes to the PDPB'19 *wrt* NPD (including anonymised data), pertain to empowering the GoI to frame rules on NPD[17], including the steps to be taken by Data Protection Authority (DPA) in case of breach of NPD under the draft DPB'21. Accordingly, the title of the bill has also been changed. Furthermore, the Data Protection Authority (DPA) has been proposed to govern personal data and NPD in instances of a data breach.[18] The bill also provides for criminal liability in case of re-identification from NPD, which was not considered in the earlier version of the PDPB'19.[19] The JPC has provided a three-point rationale for such proposed changes.

- NPD may have the potential to impact privacy;
- It may not always be possible to differentiate between personal data and NPD; and
- Having two separate DPAs to deal with these two types of data may not be practical.

Details of the proposed changes have been covered in **Annexures – 1 and 2**.

Parallel to the long deliberations on the PDPB'21, the GoI has also enacted and proposed many other regulations and initiatives, such as the draft National Data Governance Framework Policy, Reserve Bank of India's (RBI) Account Aggregator (AA) Framework, Open Network of Digital Commerce (ONDC), proposed Health Data Retention Policy, among others. These also contain aspects of data regulation and have been briefly discussed in **Annexure – 5**.

Changes recommended to the PDPB'19, coupled with these regulatory developments, indicate a shift in priority from privacy and data protection to realising the economic value of data, sometimes even at the expense of risking privacy.

1.4 Reasons behind the shift of goalpost from privacy to realising economic value of data and its uses

A global movement towards harnessing the potential of data and adopting strategic approaches to the maximisation of the value of their data is being witnessed.[20] From data collection to value creation, several steps are involved (as shown in Figure 1),[21] and the same is being used to derive insights, algorithms, optimise performance through products, personalisation or maintaining

[17] Clause 92(1) of the draft DPB'21

[18] Clause 25(6) of the draft DPB'21 states that the DPA shall in case of a NPD breach, take necessary steps, as may be prescribed, thus, there is lack of clarity on the data breach reporting procedure,

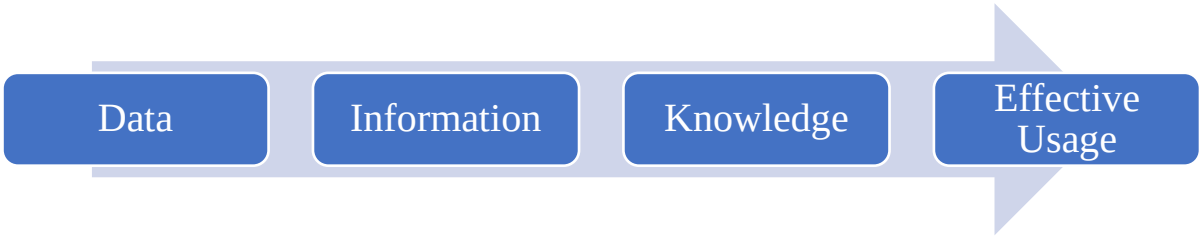
[19] Clause 83(1) of the draft DPB'21

[20] Creating Value from Data, available at: https://www.strategyand.pwc.com/gx/en/insights/2019/creating-value-from-data.html

[21] This study identified nine key factors that characterize this data-based value creation: (1) data source, (2) data collection, (3) data, (4) data analysis, (5) information on the data source, (6) information delivery, (7) customer (information user), (8) value in information use, and (9) provider network. From data to value: A nine-factor framework for data-based value creation in information-intensive services, available at: https://www.sciencedirect.com/science/article/pii/S0268401217300816#:~:text=This%20study%20identified%20nine%20key,and%20(9)%20provider%20network

long-standing relationships.[22] Additionally, data has the potential of bringing a substantial improvement in socio-economic indicators across sectors as well.[23] In light of this, data has emerged as a new asset class.[24]

Figure 1: Value Chain of Data



Source: Report of the Joint Parliamentary Committee on the Personal Data Protection Bill 2019, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

Governments worldwide have been taking note of these developments. They are shaping up their regimes to protect the privacy of their citizens and keep a check on misuse by these organisations.[25]

Recent international developments show that realising the economic value of data is becoming an important aspect for many other countries as well. For instance, the European Union (EU) has adopted The Data Governance Act,[26] which provides a legal framework for sharing non-personal data. It has also proposed the Data Act, which complements the recently provisionally approved Data Governance Act, seeks to maximise the value of data in the economy by enabling a wider range of stakeholders to gain control over their data, and ensuring that more data is available for innovative use, while preserving incentives to invest in data generation.

However, it is to be noted that the EU already has a dedicated personal data protection law, i.e., the General Data Protection Regulation (GDPR), and issues of NPD and access to data, have been deliberated subsequently and in dedicated frameworks. However, India must learn its lesson from the European Union and ensure that there are no risks of overlapping and inconsistencies while deliberating on the law.[27]

Keeping this in mind, it becomes important that data exchange happens in a trusted ecosystem. The scope for innovating and driving positive change in the same is enormous. Studies suggest

---

22 Creating Value with Data Guidebook, available at: https://www.digitalfluency.guide/creating-value-with-data/introduction-to-creating-value-with-data

23 Report of the Joint Parliamentary Committee on the Personal Data Protection Bill 2019, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

24 World Economic Forum, Personal Data: The Emergence of a New Asset Class, available at: https://www.weforum.org/reports/personal-data-emergence-new-asset-class/

25 Data Protection and Privacy Legislation Worldwide, available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

26 EU Data Governance Act, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

27 The Data Governance Act proposal by European Union brings with it several complications as it overlaps and is inconsistent with certain sectoral data regulation and even in the object of the data that it is regulating. There still remains some lack of clarity and consistency when it comes to NPD. Refer to: White Paper on the Data Governance Act, CiTiP Working Paper Series, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703

that data access and sharing can help generate social and economic benefits worth between 0.1 per cent and 1.5 per cent of global gross domestic product (GDP) in the case of public-sector data. While the imperative for data sharing by the public sector and the demand for trusted data are established, the enabling policy framework to accelerate data sharing and purpose-based application in a rights-respecting environment is missing.[28]

[28] https://academic.oup.com/medlaw/article-abstract/21/1/71/949171?redirectedFrom=fulltext&login=false

2. Analysis of Implications of Incorporation of NPD in PDPB

The recommendation of the JPC on including aspects of NPD regulation in the draft DPB'21, has received flak from several legal experts in India. However, the JPC has been lauded for rekindling the debate on NPD, which was missing in public domain since a while. This move may enable clarity and consistency in the provisions and is especially important since the concept of personal data and NPD are still shrouded in confusion as the problem of inextricable datasets and static definitions have not been solved even by jurisdictions like EU.

The dynamic concept of data also raises questions on protecting collective privacy. By including NPD in the DPB'21, several lacunae will automatically fall under the safety net of DPB'21 and be regulated. Also, by the inclusion of NPD in the DPB'21, there is bound to be amping up of research and development activity,[29] which is the need of the hour.

This being said, the recent JPC recommendation of changing the title of the draft to DPB'21 and expanding the scope of the bill to include aspects of NPD has complicated the navigation of the puzzle of NPD. These recommendations are not minor tweaks but rather major amendments which alter the scope of the proposed Bill altogether.

They have also attracted dissent and concern from different stakeholders like select Members of the JPC (compiled in **Annexure – 3**), industry associations and players, consumer groups, and subject experts, among others, on account of the following lacunas.

2.1 Premature and piecemeal regulation of NPD

Privacy of citizens is the front-running issue when it comes to data protection. Accordingly, the net of privacy protection must be cast sooner rather than later. The PDPB'19 has gone through multiple rounds of consultations and deliberations. Despite certain lacunas remaining to be addressed, the bill is in the final lap of enactment. However, the same is not the case with the NPD governance framework.

While the Gopalakrishnan Committee reports had the right intent, various stakeholders raised concerns over a lack of clarity regarding the value, nature and sensitivity of data, data sharing mechanisms and possible benefits derived from data sharing. Despite the final report of the Gopalakrishnan Committee pending to come in the public domain, the JPC has recommended including NPD aspects in the draft DPB'21 without adequate cost-benefit analysis, or exploring good international practices. In addition, it is imperative to note that while the PDPB'19 aimed to safeguard privacy rights of individuals, the proposed NPD framework discussed in the Gopalakrishnan Committee reports, intends to draw out the economic value of NPD based on

[29] Critical to back up framework on non-personal data by ramping up research and development, available at: https://www.thehindubusinessline.com/news/critical-to-back-up-framework-on-non-personal-data-by-ramping-up-research-and-development/article36228932.ece

'community rights'– thus, there is an inherent contradiction in the regulatory objective of the PDPB'19 vis-à-vis the NPD framework that is currently under consideration by the Gopalakrishnan Committee.

In its present form, the draft bill refers to NPD selectively and in a piecemeal manner that leaves scope for ambiguity in its scope, applicability and even provisions. This is particularly reflected by the loose and exclusionary definition of NPD under Clause 3(28).

Some JPC members in their dissent notes have also cautioned that including NPD in the draft DPB'21 would lead to a process that fails to acknowledge the nuances of NPD regulation. Furthermore, extensive consultation and deliberation shall be necessary before the nature, value and benefits of NPD can be thoroughly assessed. Regulation of NPD without this thorough analysis, which is a time-consuming process, will merely lead to a case of premature regulation, which shall be responsible for foreclosure of the possibility of future techno-legal regulatory innovations.[30] This has the propensity of slowing the pace of innovation, which is currently at its zenith, and have unintended adverse impacts on start-ups and consumers. This has been explained in subsequent sections of this paper.

Action Point 1: *Exclude NPD from the applicability ambit of the bill*

There is merit in excluding NPD from the ambit of the bill. Therefore, clause 1(1) of the bill may be renamed 'The **Personal** Data Protection Act, 2021'. Also, the marginal heading of Clause 2 may be reworded as 'Application of the Act to processing of personal ~~and non-personal data~~'. And, Clause 2(d) may also be omitted. The long title of the bill, may also be restricted to refer to only personal data.

Also, the JPC report rightly opined that different layers of protection or security are required for sensitive, non-sensitive, personal data and NPD. However, citing administrative impossibility to differentiate personal data and NPD, it recommends both to be regulated under the same enactment, without separate treatment of personal data and NPD in mixed datasets.

Recognising that splitting a dataset to process personal data and NPD separately may be challenging, the European Commission clarifies that: *the Free Flow of Data (**FFD**)*[31] *Regulation applies to the non-personal data part of the dataset*, and *the **GDPR's***[32] *free flow provision applies to the personal data part of the dataset*.[33]

To clarify any overlaps of datasets, it is provided that "*if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming*

[30] Shri Gaurav Gogoi's Dissent Note, annexed with the JPC report

[31] Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

[32] Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[33] European Commission, Commission publishes guidance on free-flow of non-personal data- Questions and Answers, Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2750

from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset."

In line with the same, the Gopalakrishnan Committee report also suggested having two separate frameworks for personal data and NPD, which are mutually exclusive yet work harmoniously in tandem. Even though it is argued that soon everything may fall under the ambit of personal data[34], a broad understanding of personal and NPD exists. Therefore, the focus should remain on protecting personal data and operationalising a framework in that regard.

2.2 Vague definition of NPD

Clause 3(28) of draft DPB'21 carries forward the same definition as was given under the PDPB'19, i.e., *"non –personal data" means the data other than personal data*.[35] This has been criticised by many for being vague, and open to different interpretations.[36] The definition also fails to recognise different types of NPD[37], as were classified under the Gopalakrishnan Committee report.

***Action Point 2**: Narrow down the scope and definition of NPD, recognise different types of NPD and publish informative guidance*

In this regard, it is important to take inspiration from good international practices of defining NPD. Notable in this regard is EU's GDPR, which differentiates personal data from NPD and in doing so states that: *data which originally did not relate to an identified or identifiable natural person, such as data on weather conditions generated by sensors installed on wind turbines, or data on maintenance needs for industrial machines; or data which was initially personal data, but later made anonymous*.[38]

Singapore has adopted an alternate way of segregating data. While its data protection law does not particularly employ the term NPD but defines various data sets, including: Personal data,[39] Derived personal data,[40] Publicly available data,[41] User activity data,[42] and User-provided data.[43]

---

34 The law of everything, Broad concept of personal data and future for EU data protection law, available at: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

35 Clause 3(28) of the draft DPB'21

36 Shri Manish Tewari's Dissent Note, annexed with the JPC report

37 These include public NPD, community NPD and private NPD.

38 What is considered personal data under the EU GDPR? Available at: https://gdpr.eu/eu-gdpr-personal-data/

39 "personal data" means data, whether true or not, about an individual who can be identified — (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access, Singapore's Personal Data Protection Act, 2012 , Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

40 "derived personal data" (a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but (b) does not include personal data derived by the organisation using any prescribed means or method; Singapore's Personal Data Protection Act, 2012 , Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

41 "publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event — (a) at which the individual appears; and that is open to the public. Singapore's Personal Data Protection Act, 2012, Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

42 "user activity data", in relation to an organisation, means personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation; Singapore's Personal Data Protection Act, 2012 , Available at: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

43 "user-provided data", in relation to an organisation, means personal data provided by an individual to the organisation.

This degree of granular classification and precise definitions enable regulation to be more specific. Accordingly, different obligations and exemptions can be placed per the data set's sensitivity.

Furthermore, it becomes important to invest in a regulatory process through detailed study, informative guidelines and Frequently Asked Questions (FAQs). Article 8 of EU's FFD expressly provides that the Commission has to publish informative guidance on the interaction of personal data and NPD regulation.[44] A similar initiative is also needed for India, wherein comprehensive information guides and white papers are released to the public.

2.3 Dilution of the objective of individual privacy of the PDPB'19

The inclusion of NPD in the draft DPB'21 appears to be problematic, given that objectives and envisaged outcomes of personal data protection and NPD governance are at odds with each other. This has also been flagged by many different stakeholders[45] and is visible in the comparison below.

Personal Data Protection	NPD Governance
Extracts of the two regimes	
The objective of the PDPB'19 was to *provide for the protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed laying down norms for remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected in addition to that or incidental thereto*. The same stemmed from the Puttaswamy judgement, and was envisioned to be a legislation to protect the fundamental right to privacy.	The case for governing NPD, as mentioned in the Gopalakrishnan Committee's Report-I, was to i. *Come up with a set of recommendations such that India can create a modern framework for the creation of economic value from the use of Data. To generate economic benefits for citizens and communities in India and unlock the immense potential for social/public/economic value data.* ii. *To create certainty and incentives for innovation and new products/services creation in India.* iii. *To encourage start-ups in India.* iv. *To create a data-sharing framework such that community data is available for social/public/economic value creation.* v. *To address privacy concerns, including re-identification of anonymised personal data, preventing collective*

[44] Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

[45] Industry concerned over inclusion of non-personal data, expanded localisation mandates, JPC report, available at: https://www.thehindu.com/sci-tech/technology/industry-concerned-over-inclusion-of-non-personal-data-expanded-localisation-mandates-jpc-report/article37985361.ece

Personal Data Protection	NPD Governance
	harms arising from the processing of Non-Personal Data, and to examine the concept of collective privacy.
Objectives	
The policy imperative for personal data protection is protecting individuals' privacy and preventing harm.	The policy perspective of NPD governance is aimed at unlocking economic value from NPD.
The personal data protection regime is concerned with minimisation of processing and data protection.	NPD framework must be designed to encourage greater data sharing and maximise NPD processing.

There is a clear distinction between personal data protection objectives and NPD governance. While there is a slight overlap between the two, it is to be noted that the Srikrishna Committee had left NPD-related issues to be considered by a different body. Notably, consistently throughout all previous policy deliberations on India's data regime (including the White Paper,[46] Srikrishna report and the foremost goal of the PDPB'19 and draft DPB'21),[47] the protection of the privacy of individuals relating to their personal data has been the foremost objective.

Furthermore, the Gopalakrishnan Committee revised report rightly emphasised recognising the interface between personal data and NPD. The revised report highlighted Clause 2(B) of PDPB'19,[48] which explicitly prohibited the bill's provisions that do not apply to anonymised data processing[49] other than anonymised data referred to in section 91. The report also recommended the removal of references to NPD from the PDPB'19 (by suggesting amending clauses 91(2)[50] and 93(x)[51]).[52]

The revised report clarified that any personal data, subjected to the process of anonymisation[53] and consequently anonymised, would become NPD and fall outside the purview of the PDPB'19.[54]

---

46 White Paper of the Committee of Experts on a Data Protection Framework in India, Available at: https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

47 Bhandari, Vrinda and Bailey, Rishab and Parsheera, Smriti and Rahman, Faiza, Comments on the (draft) Personal Data Protection Bill, 2019 (March 7, 2021). Available at SSRN: https://ssrn.com/abstract=4051127 or http://dx.doi.org/10.2139/ssrn.4051127

48 The Personal Data Protection Bill, 2019, Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

49 Clause 3(3) draft DPB'21, "anonymised data" means data which has undergone the process of anonymisation,

50 The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

51 The manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 91

52 Interface between regulation for non-personal data (NPD) and PDP Bill, Gopalakrishnan Committee Report-II

53 Clause 3(2) draft DPB'21 Anonymisation has been defined under the PDP Bill to be the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Data Protection Authority (DPA).

54 Clause 5.1.iii., The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

The report further states that the data set shall again fall under the purview of personal data regulatory provisions in case of re-identification of data. Furthermore, the Gopalakrishnan Committee report also recommends that mixed datasets that typically have inextricably linked personal and non-personal data will be governed by the PDP Bill (similar practice is followed in EU as well).[55]

***Action Point 3**: Operationalise two separate frameworks for personal data and NPD and continue developing a nuanced understanding of different data sets*

Expanding the scope of the PDPB'19, to include NPD as well, may be counter-productive, given that a single legislation may chase opposite poles, thereby diluting the importance and objectives of both. Accordingly, "*to ensure that the two frameworks*, i.e., on personal data regulation and NPD governance *are mutually exclusive yet work harmoniously with each other, it would be advisable to delete these sections from the PDPB'19* (here draft DPB'21) *and ensure that they are appropriately covered under the NPD framework*".[56]

2.4 Over-burdened and architectural issues of the DPA

Having a single regulatory authority for both personal data and NPD is a welcome move by the JPC[57]. However, placing the onus on the DPA to regulate both, even before its inception and with existing regulatory, and architectural issues prevalent in it, risks putting too much too soon on the proposed regulator. Also, the proposed DPA is an overarching regulator for data that shall cut across different sectors, which fuels risks of jurisdictional turf wars. Furthermore, the DPA is vested with a wide range of powers and functions, which are high on discretion and transaction-intensive. These have been briefly discussed below.

- High on discretion: Such powers include assessing the severity of harm in case of a personal data breach[58], directing data fiduciary to report the breach to data principal and take remedial action,[59] approval of the contract or intra-group scheme for the transfer of Sensitive Personal Data (SPD) and Critical Personal Data (CPD) in consultation with the CG,[60] certifying privacy by design policy of data fiduciary[61], determination of manner of obtaining valid consent,[62] and now the power to take "*necessary steps in case of breach of NPD*"[63], among others.
- Transaction intensive: Such powers include laying down regulations for data fiduciary and data processor to periodically review security standards,[64] transparency and

[55] Clause 5.1.v., The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf
[56] Clause 5.3.i., The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf
[57] A single regulator is needed for personal and non-personal data: CUTS International, available at: https://cuts-ccier.org/a-single-regulator-is-needed-for-personal-and-non-personal-data-cuts-international/
[58] Clause 25(5), draft DPB'21
[59] Clause 25(5), draft DPB'21
[60] Clause 34(1)(a), draft DPB'21
[61] Clause 22(2), draft DPB'21
[62] Clause 50(6)(d), draft DPB'21
[63] Clause 25(6), draft DPB'21
[64] Clause 24(2), draft DPB'21

accountability measures to be maintained by data fiduciary and data processors, to lay down the criteria for assigning data trust score,[65] notification of categories of personal data as SPD in consultation with the CG and concerned sectoral regulator,[66] to provide form and procedure for the conduct of audits,[67] among others.

Experts opine that it may not be appropriate to give a regulator a combination of expansive jurisdiction and many varied responsibilities and powers in its early days when its regulatory capacity is low. Considering that regulation of NPD would additionally require close coordination with various sectoral regulatory authorities (such as the Competition Commission of India), the inclusion of NPD would require the DPA to focus on multiple frameworks and develop expansive concepts around NPD and personal data at the same time, in its initial phase. Studies have also pointed out that premature load bearing can often lead to stressed systems, causing capability to weaken (if not collapse).[68] Given the above, it is feared that the DPA may fall within this category in its proposed form under the DPB'21.

When compared with other advanced countries having data protection laws, based on World Bank's Worldwide Governance Indicators, India has a low regulatory capacity.[69] Additionally, it is feared that there is a mismatch between the DPA's limited capacity and its broad mandate.

Furthermore, there exist other architectural lacunas in the DPA as well. These include skewed member selection committee; regulation making powers shared with the GoI[70][71]; lack of requirement of transparency in use of discretion; and a general lack of independence from the government.[72]

The JPC has recommended to arm the proposed DPA with the power to take "*necessary steps in case of breach of NPD*"[73], which poses a risk of unfettered power and consequently threat of concerns such as regulatory capture. In addition, the DPA is also expected to "take prompt and appropriate action" in response to any data breach per the provisions of draft DPB'21.[74] Expecting a new regulator with such lagging issues, to deal with NPD related issues on top of those related with personal data appears to be a tall ask.

It is also recommended that local councils are introduced, as they can ensure modern data protection best practices.[75] As a part of the Local Digital Movement, the foundation for local public services of the future is being laid down. This includesmore user-centred, cost-effective local

---

65 Clause 29(6), draft DPB'21
66 Clause 15(1), draft DPB'21
67 Clause 29(3), draft DPB'21
68 Capability Traps? The Mechanisms of Persistent Implementation Failure, available at: https://deliverypdf.ssrn.com/delivery.php?ID=273099104103084092071096093082075023035071009020021045096002007098083106067096080075028001097122048126037067127096113013096113046045033089029071018100084122098110029050052113018031105066088072020064087011101000100101097083001108068106100023012125026&EXT=pdf&INDEX=TRUE
69 Worldwide Governance Indicators, available at: http://info.worldbank.org/governance/wgi/Home/Reports
70 Clause 49(2)(a) and (b) read with Clause 92(1), Draft DPB'21
71 Clause 92(2), draft DPB'21
72 Data Protection Authority, available at: https://cuts-ccier.org/pdf/policy-brief -data-protection-authority.pdf
73 Clause 25(6), draft DPB'21
74 Clause 49(2)(b), draft DPB'21
75 https://www.openaccessgovernment.org/how-local-councils-can-ensure-modern-data-protection-best-practices/114516/

public services through open, collaborative and reusable work.[76] Effectively, this enables a grassroot presence and easier interface for consumers. Local bodies could work in tandem with the DPA in order to establish a vast network with multiple touch points.

***Action Point 4**: Recommended changes in draft DPB'21 wrt DPA*

Accordingly, the following changes are recommended to be made in the draft DPB'21.

C. No.	Recommended Changes in the draft DPB'21
~~25(6)~~	~~The authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed~~
49(2)(b)	Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include taking prompt and appropriate action in response to **personal** data breach in accordance with the provisions of this Act;
50(6)(o)	The code of practice under this Act may include appropriate action to be taken by the data fiduciary or data processor in response to a **personal** data breach under section 25;
94(2)(e)	~~In particular, and without prejudice to the generality of the foregoing power, such rules may provide for the steps to be taken by the Authority in case of breach of non-personal data under sub-section (6) of section 25;~~

Ideally, reference to NPD breach should be omitted in the draft DPB'21.

The proposed DPA will be a new regulator, having an enormous task of regulating data across multiple sectors. Given the limited resources, lack of jurisprudence, and teething problems the proposed regulator is likely to face, the DPA will have to prioritise and optimise its resources effectively in order to perform its duties efficiently.[77] Adopting a privacy centric risk-based approach towards different kinds of data, may be useful in this regard.

Given that its primary task would be regulating personal data, SPD and CPD, it may avoid venturing into NPD governance for the time being. This will enable the regulator to first build capacity in dealing with data classes which pose most threat to consumers' privacy, instead of spending its limited resources to regulate all types of data.

Accordingly, there is perhaps merit in waiting for the DPA to become operational in six months from the date of enactment of the DPB'21, and another one and a half years for the DPB'21 to become fully operational, before burdening the DPA with regulating NPD as well. The GoI may also undertake capacity building exercises for the regulator during this period.

[76] https://www.localdigital.gov.uk/proptech-engagement-fund-round-2/

[77] Data Protection Authority has multi-sector role, but must be efficient, available at: https://theprint.in/opinion/banking-to-groceries-data-protection-authority-has-multi-sector-role-but-must-be-efficient/561470/

Similar to other jurisdictions' practice of adopting a stringent liability framework for penalising unauthorised re-identification of data,[78] the draft DPB'21 has made re-identification of data principals from anonymised data a criminal offence.[79] However, it misses out on recommending appropriate standards of anonymisation of data. Accordingly, a clause 83(3) may be added in the bill, which paves the way for the GoI/ DPA to frame appropriate standards.

C. No.	Recommended Change in the draft DPB'21
83(**3**)	**The Central Government, in consultation with the Data Protection Authority shall frame and publish appropriate standards of anonymisation of personal data.**

Inspiration may also be taken from Germany's Stringent Liability Framework, which places a high standard for determining that data is anonymous. However, the Federal Commissioner for Data Protection and Freedom of Information in Germany, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) also recognises that the risk of re-identification cannot be absolutely eliminated. Thereafter, in 2020, Germany published a consultation paper to identify data anonymisation safeguards which highlights the importance of stricter standards.[80]

2.5 Government access to NPD without guardrails

The issue lies with Clauses 92(1) and 92(2) which empowers the GoI to gain access to NPD to enable better delivery of services, and formulating evidence-based policies, as well as frame policies towards handling of NPD including anonymised personal data. While the provision appears to well intentioned, it over-simplifies such data sharing, by not getting into the nuances of NPD sharing, as discussed in the Gopalakrishnan Committee's reports. Also, guardrails in the form of need for access to data on Fair Reasonable and Non-Discriminatory (FRAND) terms and as per the four-part test of the Puttaswamy judgment,[81] is amiss.

Furthermore, mandating such data sharing for the sake of evidence-based policy making, without undertaking any evidence-based analysis or stakeholder consultation, itself appears to be ironical, and may have unintended adverse consequences on start-ups and consumers. Clarity remains to be given on how the government will protect the accessed data, prevent access by any third parties, refrain from possible infringement of Intellectual Property Rights (IPRs) over NPD, address competition concerns of Government-owned entities arising from advantageous access to NPD in a free market economy, deal with conflicting data processors contractual obligations viz-a-viz data fiduciaries on non-sharing of data, and lay down mechanism for data fiduciaries right to be heard/ challenge against data sharing with the government. In its present form, the draft DPB'21 has unabated and vague powers, which may fuel risks of misuse and give rise to

[78] Refer to Annexure-4, Table C.
[79] Clause 83, draft DPB'21 penalises with imprisonment for three years or a fine which may extend to INR2lakhs or with both.
[80] BfDI Press Release, Available at: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/16_Konsultationsverfahren_erfolgreich.html
[81] This includes legal basis, purpose limitation, proportionality and adequate safeguards.

regulatory uncertainty, which may also have the unintended effect of diluting trust in the framework.

Furthermore, it is worrisome that the draft DPB'21 misses to clarify whether the government in case of access to NPD, would continue to be treated as data fiduciary for such data accessed, thereby obligating it to conform with other relevant provisions of the bill, and thereby bounding it with a duty of care in so far as to provide adequate security and integrity of the data accessed.

2.6 Possible impact on start-ups

The inclusion of NPD in the draft DPB'21 once again forefronts the debate on impact on start-ups, who may possibly be significantly impacted by future regulation. The unfettered power given to the CG in Clause 92(1) to explicitly frame any policy for handling of NPD (including anonymised personal data) and mandatory data-sharing requirements under Clause 92(2) are a cause of concern to start-ups.

Experts have highlighted the adverse impact of mandatory data sharing, stating if the market is not mature, it stifles competition and investment instead of promoting it.[82] It is feared that complying with data sharing obligations with the government, may fuel risks of blunting their competitive edge. A recent report by Internet and Mobile Association of India (IAMAI) and Ernst & Young (EY), based on a survey of start-ups in India, found that 76% start-ups believe that external access to their company's data even in an anonymised format will hamper their growth prospects.[83]

Furthermore, it must be noted that start-ups may need to incur costs for developing mechanisms to enable data sharing with the GoI. While the concept of open data and mandatory data sharing requirements specifically in mature data economies are being considerably boosted, an OECD report notes that many institutions are "struggling to keep up with the demand for providing or funding the infrastructure needed for data stewardship and data sharing, as well as the necessary training to support these activities.[84] This will increase their compliance burden. In addition to this, compliance burdens will disproportionately impact start-ups given that smaller players may not have the necessary wherewithal to comply with data sharing requirements, in contrast to larger industry players.

It is also to be noted that Clause 92(2) does not clarify whether start-ups would be appropriately incentivised to provide the government access to NPD. Accordingly, mandating government's access to NPD including anonymised data, without providing for any incentive mechanism for such data sharing, is likely to harm the interests of start-ups.

82 https://cuts-ccier.org/pdf/report-webinar-optimal-governance-of-non-personal-data-august11-2020.pdf
83 IAMAI-EY Report on Impact Assessment of Non-Personal Data
84 Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, Available at: https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en

2.7 Uncertainty for data processors

Data processors are subject to contractual relationships with data fiduciaries, for the data they process on their behalf. Not only do they may have limited control over data, but are also often obligated to maintain confidentiality of the data shared with them by the data fiduciary. These aspects were also recognised by the Gopalakrishnan Committee report.[85]

India is home to a vibrant data processing and outsourcing industry. As per recent estimates, it is estimated to grow at 8 percent CAGR, and reach USD225-250bn by 2025.[86] Given that India's Business Process Outsourcing (BPO) and cloud service provider sector caters to many foreign clients, sharing their NPD may have cross-jurisdictional complications. This has the potential to dissuade foreign conglomerates from outsourcing their business processes to the Indian industry. Accordingly, there may be merit in exempting data processors from the requirement of data sharing with the GoI, under clause 92(2) of the draft DPB'21.

Action Point 5: *Recommended alterations in the draft DPB'21 regarding government access*

Accordingly, it becomes imperative for the DPB'21 to provide guardrails against such eventualities. Given below are a few recommended changes to be made in the draft PDPB'21.

C. No.	Recommended Change in the draft DPB'21
92(2)	The Central Government may, in consultation with the Authority, direct any data fiduciary ~~or data processor~~ to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, **through a reasoned written order, and** in such manner as may be prescribed **through rules**. ***Explanation: the expression "reasoned written order" refers to an order seeking access to such data, which contains the reasons as to why access to such data as is necessary and proportionate to the Central Government's purpose for which the data is sought.*** **92(2)(1): No such order shall be passed, till the time appropriate rules are framed on the manner and contours of central government's access to non-personal data, which ensure that –** **(a) The data so requested is non-proprietary in nature, and does not infringe upon the intellectual property rights or trade secret of the data fiduciary;** **(b) The central government shall be treated as a data fiduciary and be bound by duty of care in so far as to provide adequate security and integrity of the data accessed;**

[85] Gopalakrishnan Committee First Report, available at: https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf and The Gopalakrishnan Committee Revised Report, available at: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

[86] https://theprint.in/theprint-valuead-initiative/indias-ites-bpo-industry-expected-to-grow-at-8-per-cent-cagr-reach-us225-250-bn-by-2025/796827/

	(c) The data fiduciary is not held responsible for any re-identification of any data principal through non-personal data, once the same has been shared with the central government, and has complied with its obligations; **(d) A clear process has been laid out down for data fiduciaries to challenge a request by the government for access to non-personal data;** **(e) Central Government's access to NPD shall be on the principles of purpose limitation, storage limitation, and data minimisation.**

3. Conclusion

The gamut of lacunas discussed above, pertaining to including NPD in the draft DPB'21, warrant a relook on the issue. This would require another round of stakeholder consultation, which may further delay India getting a dedicated personal data protection law.[87] Also, the final report of the Gopalakrishnan Committee is yet to be made public,[88] and it would be premature to include aspects of NPD regulation within the ambit of the DP Bill'21, without adequate stakeholder consultation, as was done for the PDPB'19. Accordingly, it becomes imperative to make the final report of the Gopalakrishnan Committee public, invite stakeholder comments on it and enact the PDPB, without making any reference to NPD.

Notably, combining NPD and personal data under a single bill is globally unprecedented. While other jurisdictions have also begun contemplating on a legislation for governing NPD, they have kept such possible legislations separate from personal data protection or privacy laws. For instance, in the European Union (EU), NPD is not regulated under the General Data Protection Regulation (GDPR), but vide other legislations such as the Free Flow of Non-Personal Data Regulation,[89] and the EU Data Governance Act,[90] which addresses the use and sharing of data. There is also a need to invest in detailed studies, examine private sector data sharing regimes, publishing informative guidelines, and answering FAQs on the interaction between personal data and NPD. Notably, Article 8 of EU's FFD expressly requires the European Commission to publish informative guidance on the subject.[91]

As suggested above, the following action points must be considered and adopted:

- ***Action Point 1:*** *Exclude NPD from the applicability ambit of the bill*
- ***Action Point 2****: Narrow down the scope and definition of NPD, recognise different types of NPD and publish informative guidance*
- ***Action Point 3****: Operationalise two separate frameworks for personal data and NPD and continue developing a nuanced understanding of different data sets*
- ***Action Point 4****: Recommended changes in draft DPB'21 for restricting powers of DPA to personal data breach and removing references to NPD breach*
- ***Action Point 5: (Arguendo to Action Point 1)*** *Recommended alterations in the draft DPB'21 to provide a few checks and balances on the unfettered government access to NPD.*

87 Shri Gaurav Gogoi's Dissent Note, annexed with the JPC report

88 Kris Gopalakrishnan panel calls for national NPD authority, available at: https://economictimes.indiatimes.com/tech/technology/kris-gopalakrishnan-panel-calls-for-national-npd-authority/articleshow/87637119.cms

89 Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN

90 Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

91 Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

Annexure 1: Recommendations of the JPC on including NPD in the draft DPB'21

Part-II of the report (draft DPB'21)		Part-I of the report	
C. No.	**Suggested Changes**	**R. No.**	**Recommendations/ Rationale**
1(1)	This act may be called The Data Protection Act, 2021.	2	To define and restrict the new legislation to personal data protection or to name it as PDPB is determinantal to privacy. Since the bill is dealing with two types of data sets, different layers of protection and security are necessary. The JPC opines that it is impossible to distinguish between personal data and NPD, when mass data is collected or transported. Further, a large volume of NPD is essentially derived from one of the three sets of data: personal data, sensitive personal data and critical personal data, which has either been anonymised or has been in some way converted into re-identifiable data. Therefore, the committee opines that if privacy is the concern, non-personal data has to be dealt with in the Bill Any further policy/ legal framework on non-personal data may be made a part of the same enactment instead of any separate legislation.
Marginal heading of Clause 2	Application of the Act to processing of personal data and non-personal data.		
2(d)	The provisions of this act shall apply to the processing of NPD, including anonymised data.		
3(28) & Deletion of explanation in erstwhile 91(2)	Non-personal data means the data other than personal data.		
3(14), 3(29) & 25(6)	Data Breach includes personal data breach and non-personal data breach. Non-personal data breach means any unauthorised including accidental disclosures, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the	2	To avert contradiction, confusion and mismanagement, a single administration and regulatory body is necessitated. In Committee's view, all the data has to be dealt with by one Data Protection Authority (DPA). Since the Bill provides for the establishment of one DPA, we cannot have two DPAs one dealing with privacy and personal data and the other dealing

Part-II of the report (draft DPB'21)		Part-I of the report	
C. No.	**Suggested Changes**	**R. No.**	**Recommendations/ Rationale**
	confidentiality, integrity or availability of such data. The authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed.		with non-personal data. JPC opines that it is actually simpler to enact a single law and single regulator to oversee all the data that originates from any data principal and is in the custody of any data fiduciary. This will also restrict grey area in terms of anonymisation and re-identification.
		4	The Authority should ask data fiduciaries to maintain a log of all data breaches (both personal and NPD), which shall be reviewed periodically, irrespective of likelihood of harm to data principal.
92(1)	Noting in this Act shall prevent the Central Government from framing any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, and handling of non-personal data including anonymised data.	2	As soon as the provisions to regulate NPD are finalised, there may be a separate regulation on non-personal data in the Data Protection Act to be regulated by the Data Protection Authority.
92(2)	The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.		

Annexure 2: Changes in the PDPB'19 to include NPD

The JPC at various instances in the draft DPB'21 has recommended the deletion of the term 'personal' in order to expand the scope of the bill to include NPD, and added the term NPD. The table given below serves as a comparison matric to highlight and maps the deletion of the term 'personal' from the PDPB'19 text and addition of the term NPD in the DPB'21 text.

DPB'21 Clause	Marginal Heading	PDPB'19 Text	DPB'21 Text
	Long Title	To provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.	To provide for protection of the digital privacy of individuals relating to their personal data, to specify the flow and usage of (***) data, to create a relationship of trust between persons and entities processing the (***) data, to protect the rights of individuals whose (***) data are processed, to create a framework for organisational and technical measures in processing of data, to lay down norms for social media platforms, cross-border transfer, accountability of entities processing (***) data, remedies for unauthorised and harmful processing, to ensure the interest and security of the State and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto
1	Short title and commencement.	(1) This Act may be called the Personal Data Protection Act, 2019.	(1) This Act may be called the (***) Data Protection Act, 2021.
2	Application of Act to processing of personal data and non-personal data.	The provisions of this Act, — (B) shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91	The provisions of this Act shall apply to, – (d) the processing of non-personal data including anonymised personal data.

DPB'21 Clause	Marginal Heading	PDPB'19 Text	DPB'21 Text
3(14)	Definitions		"data breach" includes personal data breach and non-personal data breach;
3(28)	Definitions	Erstwhile Explanation in Clause 91(2) has been incorporated in DPB'21 as Clause 3(28). Relevant clause is reproduced hereunder- Explanation— For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data.	"non-personal data" means the data other than personal data;
3(29)	Definitions		"non-personal data breach" means any unauthorised including accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the confidentiality, integrity or availability of such data;
25(6)	Reporting of (***) Breach		(6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed.
49(2)(b)	Powers and functions of Data Protection Authority	(b) taking prompt and appropriate action in response to personal data breach in accordance with the provisions of this Act;	(b) taking prompt and appropriate action in response to (***) data breach in accordance with the provisions of this Act;
50(6)(o)	Codes of Practice	appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 25;	appropriate action to be taken by the data fiduciary or data processor in response to a (***) data breach under section 25;
92	Act to promote framing of	(1) Nothing in this Act shall prevent the Central	(1) Nothing in this Act shall prevent the Central

DPB'21 Clause	Marginal Heading	PDPB'19 Text	DPB'21 Text
	policies for digital economy, etc.	Government from framing of any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policy do not govern personal data. Explanation to sub-clause (2) has been incorporated as Clause 3(28) in the Definitions clause of the DPB'21.	Government from framing any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, and handling of non-personal data including anonymised personal data.
94(2)(e)	Power to make rules		(e) the steps to be taken by the Authority in case of breach of non-personal data under sub-section (6) of section 25;

Annexure 3: Dissent and Concerns of Select Members of the JPC

While the JPC has recommended including NPD aspects in the draft DPB'21, the same has not been done unanimously. It is to be noted that many members of JPC have raised concerns on the issue in their dissent notes. These have been given in the table below.

C. No.	JPC Member	Perspective not adopted
92(1)	Manish Tewari, MP, Lok Sabha	NPD needs to be defined precisely in the Act. The open-ended definition in Clause 3(28) leaves the entire field open to myriad interpretations of what constitutes NPD.
2, 92 & 94	Derek O' Brien, MP, Rajya Sabha; and Mahua Moitra, MP, Lok Sabha	The Committee made a number of recommendations for the inclusion of NPD within this legislation, however, a detailed study and separate framework for regulation of NPD is required. Exclude NPD from the application of the provisions of PDPB and remove power vested in CG to make rules or issue directions regarding NPD.
3(14), 3(28) & 91	Gaurav Gogoi, MP, Lok Sabha	Including personal and NPD in PDPB shall be counterproductive for two reasons: ● Personal and NPD implicate privacy and data protection concerns very differently, therefore, extensive consultation and deliberation shall be necessary. To include NPD without comprehensive consultation and deliberation, as was done for personal data, would fail to acknowledge nuances of NPD regulation. Currently, legislation refers to NPD selectively in a piece meal manner, which is reflected by loose and exclusionary definition of NPD under Clause 3(28). ● By casting a premature regulatory framework in stone, there is a foreclosure of the possibility of future techno-legal regulatory innovations. ● The legal, institutional and technical frameworks reflected in the PDP bill provide enough safeguards to protect 'inference cycle' uses of data. NPD encompasses data used by public and private entities for 'training cycle' uses, i.e., training algorithms to draw inferences from markers within the data. Therefore, several policy considerations arise with respect to training data, especially how data will be carefully anonymised, and algorithms made accountable to data protection regulation while preserving confidentiality of training models for Artificial Intelligence and Machine

C. No.	JPC Member	Perspective not adopted
		Learning. Rapid advancements in computing shall soon make it possible to effectively balance the considerations and design an NPD regime that is user and business-friendly. ● Since the nature of personal and NPD is different and preserving business confidentiality is necessary for NPD, policy prescriptions without careful appreciation of societal and market considerations in the Indian context may undermine Indian technology companies. Measures such as mandatory sharing of NPD may contribute to a regressive business environment. Comprehensive consultations with public and stakeholders is necessary for inclusion of NPD in PDPB.

Annexure 4: International Good Practices - A Jurisdictional Comparative

Definition of NPD

European Union	Singapore	India
EU's General Data Protection Regulation (GDPR) attempts at playing a balancing role to protect data and allow free flow of data for the legitimate interests of businesses and public. In furtherance of the same, GDPR goes to great lengths to define what is and is not personal data.[92] GDPR differentiates personal data from NPD on the basis of the origin of such data and includes: • *data which originally did not relate to an identified or identifiable natural person, such as data on weather conditions generated by sensors installed on wind turbines, or data on maintenance*	Singapore's data protection law does not particularly employ the term NPD but defines various data sets, including: • Personal data[93] • Derived personal data[94] • Publicly available data[95] • User activity data[96] • User-provided data[97] This degree of granular classification and precise definitions enable regulation to be more specific. Accordingly, different	The JPC Report Recommendation No. 25 provided for the inclusion the definition of NPD. As per the draft DPB'21, NPD is defined in Clause 3(28) as: *"non personal data means the data other than personal data"* And, personal data is defined in clause 3(33) as: *personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling."*

92 https://gdpr.eu/eu-gdpr-personal-data/

93 "personal data" means data, whether true or not, about an individual who can be identified — (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access, Singapore's Personal Data Protection Act, 2012 , Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

94 "derived personal data" (a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but (b) does not include personal data derived by the organisation using any prescribed means or method; Singapore's Personal Data Protection Act, 2012 , Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

95 "publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event — (a) at which the individual appears; and that is open to the public. Singapore's Personal Data Protection Act, 2012. Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

96 "user activity data", in relation to an organisation, means personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation; Singapore's Personal Data Protection Act, 2012 , Available at¨ https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

97 "user-provided data", in relation to an organisation, means personal data provided by an individual to the organisation.

European Union	Singapore	India
needs for industrial machines; or *data which was initially personal data, but later made anonymous.*	obligations and exemptions can be placed as per the sensitivity of the data set.	

Treatment of Mixed Datasets

Europe	India
EU recognises that splitting a dataset to process personal data and NPD separately may be challenging and impractical, if not impossible. In furtherance of Article 8 of the EU Regulation on NPD, an informative guidance note lays down the governance of a **mixed dataset**. Recognising that splitting a dataset to process personal data and NPD separately may be challenging and, the Commission clarifies that: "*The GDPR provision guaranteeing free flow of personal data will apply to the personal data part of the set, and the free flow of non-personal data principle will apply to the non-personal part."* [98] Consequently, • *the Free Flow of Data (**FFD**)*[99] *Regulation applies to the non-personal data part of the dataset* • *the **GDPR's***[100] *free flow provision applies to the personal data part of the dataset*[101] To clarify any overlaps of datasets, it is provided that "*if the non-personal data part and the personal data parts are 'inextricably linked', the*	The JPC report identifies that different layers of protection or security are required for personal data and NPD, but goes on to cite that due to the administrative impossibility to differentiate personal data and NPD, both should be regulated in the same enactment. Effectively, there has been a blanket imposition of the draft DPB'21 on all data sets. Therefore, there is no separate treatment of mixed datasets as such. The entire universe of data is subjected to the provisions of the draft DPB'21.

98 Digital Single Market: Commission publishes guidance on free flow of non-personal data, 29 May 2019, Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2749

99 Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

100 Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

101 European Commission, Commission publishes guidance on free-flow of non-personal data- Questions and Answers, Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2750

Europe	India
data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset."	

Framework for Re-identification of Data

Germany	Singapore	United Kingdom
As regards anonymisation of data, Germany places a very high standard for determining that data is anonymous, however, the BDfI recognises that the risk of re-identification is still not zero. In 2020, Germany published a consultation paper[102] to identify Data Anonymisation safeguards and highlights on the importance of stricter standards.	According to Section 48E of the Personal Data Protection Act, 2012,[103] there is a provision on unauthorised re-identification of anonymised information. If an individual knowingly or recklessly takes an unauthorised action to re-identify or cause re-identification, the individual shall be guilty of an offence and be liable on conviction to a fine not exceeding US$5000 or to imprisonment for a term not exceeding 2 years or both.	UK's Data Protection Directive clearly states that principles of data protection shall not be applicable to data rendered anonymous in such a way that the data subject is no longer identifiable. Where there is evidence of re-identification taking place, with a risk of harm to individuals, the Information Commissioner will be likely to take regulatory action, including the imposition of a civil monetary penalty of up to £500,000.[104]

[102] BfDI Press Release, Available at: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/16_Konsultationsverfahren_erfolgreich.html

[103] Section 48E, Singapore Personal Data Protection Act, 2012; Available at: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P19B-#pr48F-

[104] United Kingdom, Anonymisation: Managing data protection risk - Code of Practice, Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf

Annexure 5: Other Relevant Regulations and Initiatives

1. Draft Data Accessibility Policy, 2022[105] and draft National Data Governance Framework Policy

GoI's initial version of the National Data Sharing and Accessibility Policy 2012[106] (NDSAP) recognised the public value of non-sensitive data. NDSAP focused on making data collected or developed through public investments, publicly available for full realisation of their potential value.[107] This was based on the understanding that due to the deployment of substantial level of investment of public funds in collection of data and the untapped potentials of benefits to society, it has become important to make available non-sensitive data for legitimate and registered use.[108]

As per experts, rather than implementing a new policy framework, it may have been more suitable to consider laws on open data or publicly held NPD, as highlighted by Committee of Experts on NPD Governance.[109]

The now withdrawn draft Data Accessibility Policy, 2022[110] set out in its objectives that it would maximise access to and use of quality NPD available with the public sector.[111] However, the protocols laid down in the draft policy for sharing of NPD seemed to be ambiguous, had no minimisation principles and vested excessive discretionary power with the India Data Office and GoI.

Further, since the policy was also applicable to "*information created/generated/collected/archived by the Government of India directly or through authorised agencies by various Ministries/Departments/Organisations/ Agencies and Autonomous bodies",* it also brought personal data under its ambit. In doing so, the erstwhile

[105] Draft India Data Accessibility and Use Policy, 2022 https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022

[106] National Data Sharing and Accessibility Policy, 2012, available at: https://geoportal.mp.gov.in/geoportal/Content/Policies/NDSAP_2012.pdf

[107] Preamble, National Data Sharing and Accessibility Policy, 2012, available at: https://geoportal.mp.gov.in/geoportal/Content/Policies/NDSAP_2012.pdf

[108] National Data Sharing and Accessibility Policy, available at: https://dst.gov.in/national-data-sharing-and-accessibility-policy-0

[109] Rishab Bailey, Brinda Lashkari, Urvashi Aneja, Comments on the National Data Sharing and Access Policy, available at: https://deliverypdf.ssrn.com/delivery.php?ID=736013002124028103104073000026104006049071008034054034076085120076112027014101096011028039028119052022051074098083004093079004040038068062019126099091110065027103005014036080116091125090020026100090118112006103118119018071086094115116068067080126118078&EXT=pdf&INDEX=TRUE

[110] Supra Note 106

[111] *Ibid*

draft policy raised concerns regarding the monetisation of public data[112] and was also termed as 'dangerous'[113] by experts.

Noting stakeholder feedback and criticism, a new framework for governance of citizen data that would set standards for its storage, collection and use solely by the government, was formulated.[114] This draft National Data Governance Framework Policy seeks to enable catalysation of Artificial Intelligence (AI) and data led research and start-up ecosystem as well as access to anonymised NPD.[115] Most recently, experts suggested that it is a stamp of approval to monetisation of data as it portrays that the government could monetise citizens' data as part of its larger plan to use data as a public good.[116] The justification for the same was that data is generated by the people, of the people and should be used for the people to the best possible use. But concerns have been raised that this approach may lead to monetisation of data without adequate safety measures.

2. Open Network of Digital Commerce (ONDC)

ONDC[117] is a first-of-its-kind initiative that globally paves the way for reimagining digital commerce in India. Reportedly, the open network seeks to empower both consumers and sellers by democratising the e-commerce space. All seller and buyer platforms shall operate through one open protocol and be connected through ONDC. However, there have been concerns around the "tech" layer. Thought leaders opine that GoI should restrict their role to the facilitation of standards and protocols that provide open access and collect minimal amounts of data (especially personal data) so that a honeypot for hackers is not created.

3. Reserve Bank of India's (RBI) Account Aggregator (AA) Framework

The framework[118] is also relevant in this regard. AAs are financial data intermediaries armed with the task of collecting users' financial information and sharing the same with a range of enlisted entities, upon receipt of consumer consent. It has been argued that even though AAs

---

112 Understanding the Draft India Data Accessibility and Use Policy, 2022, available at: https://deliverypdf.ssrn.com/delivery.php?ID=736013002124028103104073000026104006049071008034054034076085120076112027014101096011028039028119052022051074098083004093079004040038068062019126099091110065027103005014036080116091125090020026100090118112006103118119018071086094115116068067080126118078&EXT=pdf&INDEX=TRUE

113 Why draft data accessibility policy is dangerous, available at: Our Data, not for Sale, available at: https://indianexpress.com/article/opinion/columns/draft-data-accessibility-policy-privacy-suveillance-7801714/#:~:text=The%20government%20may%20very%20soon,to%20harness%20public%20sector%20data%E2%80%9D.

114 Govt to float new data governance framework: Rajeev Chandrashekhar, Available at: https://economictimes.indiatimes.com/tech/technology/govt-to-float-new-data-governance-policy-framework/articleshow/90738066.cms

115 Draft National Data Governance Framework Policy, Available at: https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf

116 Economic Survey suggests govt can monetise citizen's data as a public good, available at: https://www.business-standard.com/article/economy-policy/economic-survey-suggests-govt-can-monetise-citizen-s-data-as-a-public-good-119070401558_1.html

117 How Open Network for Digital Commerce could disrupt India's e-commerce space, available at: https://indianexpress.com/article/opinion/columns/how-open-network-for-digital-commerce-could-disrupt-indias-e-commerce-space-7417683/

118 Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, available at: https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

appear to be an exciting new infrastructure, there are several disjoints in the framework wherein user privacy is not necessarily being prioritised.

4. Proposed Health Data Retention Policy

Even in responses by leading experts on the Consultation Paper on the proposed Health Data Retention Policy[119], it was highlighted that the focus should remain on the protection of an individual's privacy interests and that the policy should not devolve into a method to justify unfair use of an individual's data by either the State or private entities.[120]

5. Cybersecurity and breach reporting directions by the Indian Computer Emergency Response Team

The directions by the Indian Computer Emergency Response Team (under the aegis of the Ministry of Electronics and Information Technology) provides for strict reporting measures in case of cybersecurity incidents. There may be an overlap between reporting of data breaches under the said directions and the draft DPB'21. It is yet to be seen how the difference in timelines for data breach notification under the draft DPB'21 and the directions will be harmonised by the GoI.[121]

[119] National Health Authority, Ministry of Health and Family Welfare, Government of India, Consultation Paper on Proposed Health Data Retention Policy, available at: https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation_Paper_on_Health_Data_Retention_Policy_21.pdf

[120] Comments on the proposed Health Data Retention Policy, available at: https://deliverypdf.ssrn.com/delivery.php?ID=502127090083065024019095123081095089097086084036020059023084071071008118118083027119033028006123050113058083066013091109012021062005008023034103025100125026080012116021035085100084078122019125066016093117108127102108076092011010089065085025102004007098&EXT=pdf&INDEX=TRUE

[121] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, available at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).