BSA Submission
on the
Report by the Committee of Experts on
Non-Personal Data Governance Framework

Shri. Kris Gopalakrishnan,
Hon'ble Chairperson,
Committee of Experts on the Non-Personal Data Governance Framework,
Ministry of Electronics and Information Technology,
Government of India

Cc:

Shri. Ajay Prakash Sawhney
Secretary, Ministry of Electronics and Information Technology

Shri. Rajendra Kumar
Additional Secretary, Ministry of Electronics and Information Technology

September 10, 2020

Dear Sir,

Subject: BSA Submission on the Report by the Committee of Experts on Non-Personal Data Governance Framework

BSA | The Software Alliance (**BSA**)[1] appreciates this opportunity to comment on the Report prepared by the Committee of Experts (**Committee**) on a non-personal data (**NPD**) governance framework (**Framework**).[2]

[1] BSA is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy

BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Report by the Committee of Experts on Non-Personal Data Governance Framework accessible at: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

Le-Meridien
15th Floor, Room 1529
New Delhi 110001
India

P +91 11 4978 9066
W bsa.org

At the outset, we are grateful to the Committee for instituting a public consultation process on this important issue. A consultative approach will enable the Committee to understand the perspectives and concerns of crucial stakeholders, including data-intensive private enterprises that are driving job creation and economic growth in India.

In today's information-driven world, the collection and use of data has become a core component of effective global responses to complex challenges, from global health pandemics to climate change and beyond. Data will also be a key to growth in all sectors and will play an important role in helping India realize Prime Minister Modi's vision of a $5 trillion economy by 2024.[3]

BSA supports efforts to enhance the collective benefits of data by advancing responsible policies that facilitate sharing, collaboration, and experimentation with data resources while protecting privacy, security and the proprietary nature of data. As such, we support efforts to promote effective government-generated data sharing and the establishment of collaborative, and voluntary, data sharing arrangements among the private sector.[4]

However, the Committee's recommendations for a new law, a new regulator, and a compulsory data sharing architecture are premature, especially when there is little global precedent for the regulation of NPD. Additionally, the scope of the proposed framework is overly broad and will not assist India in achieving its objectives of attracting investment and promoting innovation and economic growth. Instead, forced data sharing policies will undermine innovation and investment, and risk stifling Indian businesses and startups. While we set out our detailed concerns and recommendations to the Framework in the annexure below, here are our key recommendations to the Committee:

1. Encourage ***voluntary*** data sharing arrangements and ***avoid proposing mandatory data sharing obligations***.
2. ***Recognize that mandatory obligations are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors,"*** including enterprise software and cloud service providers, which handle data only on behalf of their business customers and may be prohibited from accessing that data except to carry out their customers' instructions; and
3. ***Refrain from imposing restrictions on cross-border data flows and eliminate local storage requirements***, which can undercut the stated objectives of the Framework.

BSA supports a consultative, fact-based, flexible, and incremental approach based on a guiding framework for voluntary data-sharing and accountability that is designed to address targeted and empirically demonstrated challenges. This approach would better serve the needs of a dynamic and rapidly growing digital economy in India.

As the Committee considers stakeholder feedback to the Framework, BSA urges due consideration to the issues raised in these comments. While they do not account for all of BSA's concerns, they highlight proposals that, in BSA's view, would create the greatest difficulties for businesses that offer services in India as part of a dynamic, innovative, and global data-driven economy.

[3] Shri. Narendra Modi, Prime Minister of India, speaks at the fifth meeting of Governing Council of NITI Aayog, June 2019, accessible at: https://pib.gov.in/PressReleasePage.aspx?PRID=1574696
[4] BSA's Open Data Agenda – Open Data: Bridging the Divide, accessible at: https://www.bsa.org/files/policy-filings/061120bsaopendata.pdf

Sincerely,

Venkatesh Krishnamoorthy
Country Manager
BSA | The Software Alliance

Annexure: BSA Submission on the Report by the Committee of Experts on Non-Personal Data Governance Framework

Annexure

BSA Submission on the Report by the Committee of Experts on Non-Personal Data Governance Framework

1. Data Sharing Recommendations

The Committee proposes three categories of NPD — public NPD, community NPD, and private NPD, and corresponding mandatory data sharing obligations for each.[5] Beyond this, the Committee recommends compulsory sharing mandates for 'important NPD'[6] and 'high-value' NPD datasets.[7]

BSA supports initiatives to promote effective government data sharing, foster greater industry collaboration by making it easier for organizations to voluntarily share their data, and ensure that data sharing efforts are undertaken in ways that enhance privacy and security. However, the Committee's proposed compulsory data sharing mandates would chill investments in the collection and utilization of data and could undermine the interests of innovative enterprises including Indian start-ups and Small and Medium Enterprises (**SMEs**).

a. Promote Effective Government Data Sharing

At the outset, BSA supports the Committee's proposal to facilitate the sharing of "public NPD", i.e., data collected or generated by the Government.[8] "Public NPD" can serve as a powerful engine for creating new jobs, promoting economic growth, and enabling innovation. It is estimated that Government open data initiatives could translate into USD $22 billion of socio-economic impact.[9] As the National Institution for Transforming India (**NITI Aayog**) highlights, government data is a critical asset for the development of new technologies such as artificial intelligence.[10] From global health pandemics to climate change and beyond, "public NPD" can help craft smart responses to the world'smost pressing challenges. In particular, the Government of India's Open Government Data (**OGD**) platform, built on the framework created by National Data Sharing and Accessibility Policy (**NDSAP**), is a welcome initiative.[11,12] These efforts will help provide open and proactive access to the data available from various Government departments.

Prioritizing the release of high-value government data assets is an important objective. We encourage the Committee to consider ways to further strengthen these initiatives. For instance, the quality of currently available data can be improved. Currently, such data typically requires rigorous processing before use and data interoperability challenges remain. Further, identifying particular data assets that would be most

---

[5] *See* Para 4.2, 4.3, 4.4.
[6] *See* Para 4.10 (iv).
[7] *See* Para 7.2 (ii).
[8] *See* Para 7.4 (i).
[9] Open Government Open Data, joint report by Yes Bank and MeitY, may 2018, available at: https://www.yesbank.in/beyond-banking/knowledge-reports/technology/inspiring-the-next-big-leap
[10] NITI Aayog, National Strategy for Artificial Intelligence, June 2018, available at https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf?utm_source=hrintelligencer.
[11] Open Government Data (OGD) Platform India, available at: https://data.gov.in/
[12] Ministry of Science and Technology, National Data Sharing and Accessibility Policy, 2012, available at https://data.gov.in/sites/default/files/NDSAP.pdf.

valuable to different sectors has proven difficult. To improve existing data open sharing mechanisms, the Committee could consider tools to identify and examine: (1) government data assets that would be most useful for industry, academic researchers, and the public to be made available with open access; (2) data assets the government controls that are currently underutilized; and (3) ways to make such data assets available for research and development (**R&D**) while ensuring that privacy is protected.[13] By using simple API's and interoperable formats, the government could enhance access to and use of data by innovative private sector actors, including Indian start-ups and SMEs.

b. Promote Voluntary Industry Data Sharing

BSA supports responsible policies that facilitate voluntary industry data sharing, collaboration, and experimentation with data resources while protecting privacy and security. However, ***BSA does not agree with the Committee's proposals for mandatory access and sharing of community and private NPD.***

Data is key to growth in all sectors of the economy. However, data has very little inherent value in raw form or in isolation. It is only when data is curated and used as an input to other value-added operations, such as artificial intelligence (AI), that it has the potential to contribute to the projected $15 trillion addition to global GDP by 2030.[14] Businesses create value from data when they invest resources into organizing and analyzing such data, driving competitive new insights and business models. ***The proposed mandatory data access policies will likely deter investment and innovation in the Indian market, raising the costs of acquiring such data in the first place while also disincentivizing data collection activities, resulting in increased costs for end-users and reduced incentives for developing new technology.***

Instead, ***the Framework should promote a voluntary approach for enabling the sharing of data.***

We outline the following key concerns with the proposed mandatory data sharing regime:

i. Impact on Innovation

The Committee suggests that Indian businesses will not be able to create high value digital products without having access to data.[15] However, creating and structuring data sets is resource intensive (including for raw data sets) and requiring businesses to share data will remove their incentive to invest in the collection, curation, and maintenance of databases and to develop new technologies. While innovation does not solely depend on data access, policies that undermine the return on investment on efforts to improve the quality of data could hamper economic growth. It could also discourage investment in data analytics, an area identified as a national priority.[16]

A compulsory access policy will also give new entrants and start-ups little incentive to invest in database construction, the development of unique curation capabilities, or the creation of alternative business models. This will be harmful to consumers in the long run, as it reduces incentives for innovative business

---

[13] BSA, Open Data: Bridging the Data Divide, available at https://www.bsa.org/files/policy-filings/061120bsaopendata.pdf.
[14] BSA, What's the Deal with Big Data, available at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf
[15] *See* Para 7.3(i).
[16] Para 2.8, Objective 2, National IPR Policy, Ministry of Commerce and Industry, Government of India, May 2016, available at: https://dipp.gov.in/sites/default/files/National_IPR_Policy_English.pdf.

solutions. ***Contrary to the Committee's goal of enhancing the benefits of a data-driven economy for India, a mandatory data sharing requirement would stunt innovation and creativity.***

ii. Security Concerns

We appreciate the Committee's recognition of potential harms arising from the re-identification of personal data and similar risks.[17] A mandatory data sharing requirement, however, will only exacerbate such privacy and security risks as businesses may be required to share data with companies that employ inadequate security, privacy, and data handling practices. Some companies requesting data may ignore necessary security requirements simply to achieve faster growth, or they may not have the technical know-how and expertise to handle the data securely.

Re-identification of personal data may occur if a recipient compiles datasets from various sources and attempts to identify individuals. Not all companies will be able to afford or will prioritize appropriate investments in strong privacy and security measures. ***Thus, a mandatory data sharing regime will increase privacy and security risks.*** In voluntary data sharing arrangements, companies can review, assess, and negotiate the implementation of adequate privacy and security controls with their business partners.

iii. Broadly defined and highly subjective data-sharing purposes

The Report suggests that compulsory data sharing requirements can be imposed in service of sovereign purposes, core public interests' purposes, and economic purposes.[18] The scope of these purposes are very broadly defined in the Report. For instance, sovereign purposes include the requirement of data sharing for "investigations and law enforcement", the public interest purpose can be invoked where there are "wide societal benefits including science, healthcare, urban planning etc.", and economic purposes include encouraging competition. Having such broad purposes for which data must be shared would result in essentially all data held by a company coming within the scope of mandatory sharing obligations. ***This risks undermining the trust and confidence of consumers and enterprises and raises concerns that the data they may be sharing could be misused.*** If the Committee retains recommendations for having mandatory sharing requirements, it should substantially narrow and refine the purposes for data sharing and recommend that the government engage in further industry consultations to define an objective threshold criteria or purpose test that should be completed to determine whether data can be shared for such purposes or not.

iv. Onerous Registration, Disclosure, and Sharing Requirements for Data Businesses

Although there is increasing recognition of the collective benefits of collaborative data sharing, the mechanism proposed in the Framework faces multiple technical, legal, and organizational challenges. Rather than enhancing the benefits of a data-driven economy, ***the Committee's proposals would create an excessive compliance regime that disincentivizes data sharing.*** The Committee proposes mandating registrations for "data businesses", requiring such businesses to disclose the types of data processed, and harmonizing data-related directories.[19]

---

[17] *See* Para 3.7 (vii).
[18] *See* Paras 7.1-7.3
[19] *See* Para 6.3.

The mandatory registration and substantial disclosure and sharing obligations imposed on "data businesses", which is a new category so broadly defined[20] as to capture almost any business, would create an unjustified compliance burden and would likely raise the cost of providing services to end-users in India. To avoid such costs and obligations, businesses might take steps, such as refraining from adopting advanced and secure software-enabled solutions, to avoid being categorized as a "data business". This would run counter to the goals of Digital India and would adversely impact investments in data processing and outsourcing services in India.

In this regard, BSA suggests that the Committee consider frameworks that enable participants to benefit from mutually agreed sharing of data, while preserving data security. For instance, data marketplaces allow buyers and sellers to exchange datasets, while common data pools can be established for voluntarily contributions of specific data categories. Investments in R&D and the creation of regulatory sandboxes could also help spur the development of such arrangements. Regardless of the specific mechanisms, ***it is critical that the Committee recognize the voluntary nature of such mutually agreed arrangements and avoid creating new bureaucratic categories and regulatory requirements upon a broad swath of the Indian economy.***

v. Intellectual Property Rights

BSA members are highly innovative companies which rely on intellectual property (**IP**) to secure their substantial investments in innovative technologies. We appreciate that the Committee recognizes the role of 'robust IP rights' in promoting data-driven innovation.[21] ***However, the mandatory data sharing recommendations in the Framework disregard these IP rights and their function in catalyzing innovation.*** Besides copyright that exists in databases, data belonging to companies, and the insights derived from such data, are often treated as "confidential information" or "trade secrets" and granted legal protection against unauthorized disclosure.[22]

vi. Costs Related to AI Training Datasets

The Committee proposes certain measures to facilitate access to AI training datasets. The Framework recommends that raw/factual data needs to be labelled properly as raw data alone is unsuitable for AI training.[23] It also suggests developing incentive mechanisms to enable sharing of AI training datasets.[24] Policies, such as the mandatory sharing requirements and the burdensome compliance mechanisms discussed above, that decrease investments in collecting and curating datasets used to train AI systems, will ultimately increase the costs of these technologies for customers and decrease the incentive to develop and use new technology — potentially reducing overall consumer welfare.

The Committee should avoid recommending policies that would stifle innovation and consumer benefits and instead focus on recommending policies, such as incentive schemes and voluntary data sharing frameworks, that facilitate the voluntary business-to-business exchange of data and boost the development of AI services.[25] The Framework should additionally make clear that there can be no obligations to share trade secrets or confidential information.

---

[20] *See* Para 6.1
[21] *See* Para 3.7 (vi).
[22] *See* Vogueserv International Pvt. Ltd. v. Rajesh Gosain and Ors., (2013) 203 DLT 613; Diljeet Titus, Advocate v. Alfred A. Adebare, 2006 (32) PTC 609 (Delhi).
[23] *See* Para 7.3(iv).
[24] *See* Para 7.3(iv).
[25] Spurring AI Innovation With Sound Data Policy, The Impact of Data Policy on AI Development by BSA | The Software Alliance, accessed here at: https://ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_DataPolicy.pdf

2. Privacy Related Recommendations

The Committee proposes to import obligations similar to those in the Personal Data Protection Bill, 2019 (**PDP Bill**) into the proposed Framework, including categorizing NPD as sensitive or critical based on the nature of the personal data it may have been derived from, and imposing local storage requirements and restrictions on cross border flows of NPD.[26]

We are concerned that the Committee's attention to privacy-related matters is misplaced, given the mandate to focus on NPD — which, by its very nature, does not relate to an identifiable individual. While one of the four objectives identified in the Framework is to address privacy concerns,[27] ***any concerns related to privacy and personal data protection should be addressed by the PDP Bill and the proposed Data Protection Authority (DPA).*** If the Framework is also used to address privacy issues, it will create conflicting obligations that reduce the ability of the DPA and PDP to comprehensively address privacy concerns.

For example, the Report focuses on concerns about the degree to which data is truly anonymized. This is an important issue — but one that is already addressed by the proposed PDP Bill. Under the PDP Bill, data is considered anonymized and therefore outside the scope of the PDP Bill when it is subject to an "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified" that meets standards to be created by the DPA.[28] In this way, the proposed PDP Bill already creates a threshold that ensures personal data is subject to appropriate data protection safeguards. This threshold is in line with global norms, which do not impose privacy requirements, such as consent, on uses of anonymous data. For example, the European Union's General Data Protection Regulation (GDPR) does not apply to anonymized data.[29] At the same time, the GDPR recognizes that data that has been "pseudonymized" — and thus could be linked to an individual if combined with additional information — should be treated as personal data and subject to certain data protection safeguards.[30]

The Committee's recommendation that appropriate standards of anonymization be defined[31] is therefore likely to conflict with guidance from the DPA. Given that the PDP Bill already grants the DPA the authority to develop standards of anonymization and de-identification,[32] ***the Committee should exclude references to privacy, consent, and anonymization standards from the Framework's scope.***

3. Cross-Border Data Flows and Data Localization

The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. Cross-border data flows are particularly important in the context of cybersecurity and data privacy, enabling distributed and compartmentalized data storage, as well as allowing correlation of threat data for more effective cybersecurity defense. Cross-border data flows are also essential to improve data analytics,

---

[26] The Personal Data Protection Bill, 2019; available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[27] See Para 3.8 (ii), (iv)
[28] Section 3(2), PDP Bill.
[29] See GDPR Recital 26.
[30] See GDPR Recital 26; GDPR Article 4(5).
[31] *See* Para 4.6 (v).
[32] Section 50 (6)(m), PDP Bill.

which can deliver socially and economically beneficial results in situations ranging from digital commerce to responses to natural disasters.

The Framework's recommendations to introduce restrictions on cross-border NPD transfers and to impose local NPD storage requirements are unrelated to the data sharing objectives of the Framework. Instead, they disrupt companies' operations, make it costlier to provide services in India, decrease opportunities for collaboration through data sharing, and increase barriers for competition that are key to ensuring Indian users have cost-effective access to the best products and services. As highlighted before, the Committee's proposal to import cross-border data flows restrictions and data localization requirements on NPD derived from personal data by anonymization based on the same proposed restrictions and requirements in the PDP Bill unnecessarily complicates the regulation of personal information, would raise costs to businesses in India and deter investment in data-related enterprises, and is inconsistent with global norms and practice.

Therefore, the Committee should remove restrictions on cross-border data flows and eliminate local storage and processing requirements, which can undercut the stated objectives of the Framework.

4. Beneficial Ownership and Community NPD

The Committee proposes a "community right" over data and the appointment of a "trustee" to ensure such data is utilized in the best interests of the community.[33] To operationalize the allocation of "primary economic and other statutory rights" over "community NPD", the Committee introduces the concept of "beneficial ownership", where the community in question would exercise its primary economic rights through a "data trustee".[34] Such a layering of rights would introduce tremendous uncertainty and undermine fundamental principles about the nature of rights (including rights in property) and obligations associated with, this data. Consequently, this would substantially inhibit the ability of the enterprises, including SMEs and start-ups, to use the data they have invested to collect and curate.

Further, in today's context, data is usually utilized in vast quantities coming from multiple sources to derive intelligence or new meaning from such data. Therefore, it is possible that a data set could contain multiple sets of community non-personal data from multiple communities, and this may subsequently result in a complex network of seemingly vested "beneficial ownership/ interests" between the data custodians and such communities. In such scenarios, it could become difficult for data custodians to align interests or determine with whom or in whose best interests the data should be shared/ utilized.

The Committee's recommendation to establish a "duty of care" for "data custodians" towards a community is also ambiguous.[35] To the extent that this contemplates the imposition of a common law "duty of care", this would introduce unwarranted legal risk and liability for companies in dealing with the data they collect, again introducing a chilling effect on innovation. To the extent that the "duty of care" under contemplation is to be defined in the future, this introduces even more legal uncertainty in the overall business environment in India, which will have a negative impact on investment. BSA submits that any rulemaking should be based on the principles of transparency, accountability, predictability, and fairness, mutually agreed terms and conditions, and governed by clearly defined and objective criteria.

Therefore, the Committee should eliminate any recommendations for creating legally binding rights or concepts related to concepts such as "community data" and "community ownership"

[33] *See* Para 4.8 (ii).
[34] *See* Para 4.9.
[35] *See* Para 4.8 (iii).

from the Framework. The Committee may consider recommending the facilitation of a multi-stakeholder consultative process to discuss how the use of data, and improvements in the facilitation of voluntary sharing arrangements, can better benefit all communities, regardless of the particular source of particular data sets.

Furthermore, the Committee should remove the concepts of "beneficial ownership" and "duty of care" from the Framework.

5. Global Datasets

BSA is concerned by the proposal to classify "global datasets" collected by businesses/individuals overseas, including datasets relating to non-Indians, as "private NPD".[36] This would effectively extend the scope of the proposed Framework to any dataset collected by any entity in any jurisdiction, raising potential conflicts of law and imposing a heavy compliance burden on businesses. Moreover, imposing compulsory data access (including with respect to the data of non-Indians held by foreign businesses) may violate international treaties established to protect the IP rights of businesses, such as the WTO's Trade Related Agreement on Intellectual Property Rights (TRIPS Agreement)[37] and the World Intellectual Property Organization Copyright Treaty, among others.

Therefore, the Committee should delete references to "global datasets" from the definition of "private NPD".

6. Multiplicity of Regulators

Proposing a new regulator for the governance of NPD will result in regulatory overlap, creating legal uncertainty and adversely impacting the business and investment climate of India. Personal data protection related issues are already covered under the PDP Bill and will be enforced by the DPA. Further, the Competition Commission of India (**CCI**) has a sector-agnostic remit to govern issues of competition and promote the interests of consumers. Proposing an additional regulator for NPD creates two risks: (1) increased costs to businesses due to duplicative compliance measures of overlapping regulators; and (2) delays and uncertainty caused by jurisdictional conflict of separate regulators.

Therefore, the Committee should remove the proposal to create a new authority to oversee the governance of NPD.

7. Recognize That the Framework is Inappropriate for Data Processors, Including Enterprise Software and Cloud Service Providers

BSA is concerned with the potential applicability of the Committee's proposed NPD Framework to data processors, including enterprise software and cloud service providers (**CSPs**), which frequently act as data processors.

Any Framework addressing NPD should recognize the unique role of data processors, and ensure they are not subject to obligations designed to fit businesses that decide how data will be collected and used.

---

[36] *See* Para 4.4.

[37] Art. 10(2) of the TRIPS Agreement provides that "compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such." See also TRIPS Article 39.2, which requires WTO members to protect undisclosed information, including information that "… is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question."

In addition to our concerns and recommendations above, we urge the Committee to recognize that many of the proposed obligations, which are counterproductive throughout the data ecosystem, present additional complications if applied to data processors.

a. Data Processors are not "Data Custodians" or "Data Businesses", and May Lack the Technical Ability or Legal Right to Share Data They Hold On Behalf of Other Companies

The Committee proposes certain new stakeholders, namely "data custodians"[38] and "data businesses",[39] and places sharing, consent, and anonymization obligations on them. We have raised our concerns with imposing such obligations on such entities in our comments above.

However, in addition to these concerns, we are concerned that the Framework does not recognize the distinctive role of data processors (as distinct from "data controllers" or "data fiduciaries") in the overall data economy.

Data processors store and process data (whether personal or non-personal) on behalf of their clients, i.e. data controllers, and are obligated to follow their clients' instructions in handling that data. In many cases, data processors are often contractually prohibited from accessing that data, to increase the privacy protections afforded to the data — and would accordingly lack the legal right to share data they hold on behalf of other companies. As a result, data processors often engineer their systems so that they do not have access to the content of the data that is stored or processed via their services.

It would therefore be technically and legally infeasible for many data processors to comply with the proposed data sharing, consent, anonymization, and disclosure obligations set out in the Framework. We are very concerned that this would then lead to data processors finding themselves in the impossible situation where they are forced to choose between breaching their legal obligations to their clients or breaching the proposed obligations under the Framework. This would create significant harm to the data processing industry in India, which is one of the largest contributors to Indian IT sector revenues and, as noted above, could have severe negative impacts on the willingness and ability of companies in general to continue investing in innovative approaches.

b. Sharing Requirements May Create Security and Privacy Risks, Especially If Applied to Data Processors

To the extent any sharing requirements fall on data processors, it may create additional privacy and security concerns — besides the technical and contractual concerns raised above. Because data processors have limited visibility into the nature, scope, and purpose of processing activities they conduct on behalf of their customers (i.e., data controllers), they are unlikely to be the entity best situated to ascertain the likelihood of harm that could result from sharing particular data sets and the appropriate security controls for doing so.

c. Practical Challenges with Applying Consent Requirement to Data Processors

The Framework provides that NPD derived from personal data that has been anonymized remains under control of the individuals to whom the underlying personal data relates.[40] While collecting personal data, the Committee recommends that the data custodian or data business take the individual's consent prior to

[38] *See* Para 4.8, Report by the Committee of Experts on Non-Personal Data Governance Framework.
[39] *See* Para 6.
[40] *See* Para 4.6.

anonymizing it.[41] As noted above, this consent requirement is unnecessary because privacy-related concerns should already be addressed by the PDP Bill to the extent data is not properly anonymized. Furthermore, to the extent any such requirement is imposed on data processors, it would be extremely difficult if not impossible for them to meet it as the processor generally has no direct relationship or interface with the data subject, and indeed may have no way of identifying the data subject.

Therefore, the Committee should recognize that mandatory data sharing and other requirements on enterprises handling NPD are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors", including enterprise software and cloud service providers, which handle data only on behalf of their business customers and may be prohibited from accessing that data except to carry out their customers' instructions.

We thank you for the opportunity to provide recommendations and hope our submission is useful to the Committee during this consultation process. We look forward to participating in this important discussion and would be happy to answer any questions you may have.

[41] *See* Para 4.6.