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

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

January 29, 2021

Dear Sir,

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

BSA | The Software Alliance (**BSA**)[1] appreciates this opportunity to provide inputs on the revised report prepared by the Committee of Experts (**Committee**) on the Non-Personal Data Governance Framework (**Framework**).[2]

At the outset, we are grateful to the Committee for addressing and accepting some of BSA's recommendations on the previous version of the Framework.[3] Instituting a consultative approach to policymaking will support India's forward-looking efforts to build a modern data-driven economy. Specifically, we are thankful to the Committee for the following recommendations:

- Excluding data processors from the mandatory data sharing proposals;[4] and
- Excluding NPD from the scope of the Personal Data Protection Bill, 2019 (**PDP Bill**).

[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, Cisco, CNC/Mastercam, DocuSign, 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] Revised Report by the Committee of Experts on Non-Personal Data Governance Framework, accessible at: https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

[3] Earlier Report by the Committee of Experts on Non-Personal Data Governance Framework, accessible at: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf. BSA Comments (September 10, 2020) accessible at: https://www.bsa.org/files/policy-filings/09102020indiabsanpd.pdf

[4] See Para 7.5 (ii)

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

P +91 11 4978 9066
W bsa.org

Continuing to hold broad and meaningful public consultations on the Framework will allow the Committee to propose policies that drive job creation and economic growth. It will also empower market participants to contribute to and benefit from unlocking the economic value of data in India and encourage the uptake of innovative technologies such as AI and data analytics by Indian enterprises.

BSA supports efforts to enhance the collective benefits of data while preserving consumer privacy, data security, and protections for commercially sensitive information. However, several issues continue to remain unaddressed under the revised Framework. For instance, the revised Framework continues to recommend imposing mandatory data sharing with government entities and other businesses on enterprises that collect and analyze data (referred to as data custodians or data business in the revised Framework). While the revised Framework now limits these data sharing requirements to purposes of "public good", the concept of "public good" covers a very wide range of objectives and would subject affected enterprises to an overly expansive set of requirements that would undermine their legitimate business interests and therefore their ability to substantially invest in the innovative technologies, services, and business models. This would undermine investments in innovation and risk stifling Indian businesses and start-ups which are so essential for India's objectives for the digital economy.

While we set out our detailed concerns and recommendations to the revised Framework below, our key recommendations to the Committee are:

1. Avoid recommendations for a new NPD regulation and new NPD regulator
2. Remove recommendations to impose mandatory data sharing requirements, for "public good" purposes or otherwise;
3. Remove recommendations to require consent for anonymization and using anonymized data; and
4. Refrain from recommendations to restrict cross-border data flows and require local storage of NPD.

The Committee can play an important role in fostering the development of a framework that makes it easier and less expensive for government entities and private enterprises to share data in ways that are consistent with rigorous data governance expectations. In this context, BSA would like to submit the following recommendations:

1. Remove Recommendations to Mandate Data Sharing

We appreciate that the Committee has sought to narrow the scope and purposes for data sharing. However, the proposed revised data sharing mechanism would still effectively impose a data sharing requirement on businesses for "public good" purposes. As noted above, "public good" purposes can be very broadly interpreted. **We recommend that the Committee remove all recommendations to establish a mandatory data sharing regime.**

Our three main concerns on this issue are:

i. Negative Impact on Innovation

There is a lack of evidence that supports the concept encapsulated in the revised Framework, that a mandatory data sharing requirement will encourage local innovation, entrepreneurship and benefit the

public.[5] A data sharing requirement would raise the costs of acquiring data in the first place while also disincentivizing investment in data processing activities resulting in increased costs for end-users and reduced incentives for developing new and innovative technology.

ii. Violation of Internationally Recognized Intellectual Property Rights

Despite its acknowledgement of concerns regarding intellectual property rights (**IPR**) protection associated with datasets,[6] the revised Framework fails to adequately address how it will preserve those key protections. In fact, the revised Framework appears to minimize the scope of potential IPR that might be implicated by the revised Framework's proposed data sharing requirements. For instance, the revised Framework presupposes that data stored in "pre-set fields" is ineligible for copyright protection and suggests that "eminent domain" could be relied upon to compel sharing of data subject to trade-secret protection.[7] These bold assertions should be revisited. Without the addition of safeguards for protecting IPR that may be implicated by the broad compulsory data sharing requirements, the revised Framework would place India out of step with international norms regarding the protection of copyrighted works and proprietary data.

iii. Security Concerns

The revised Framework's data sharing requirements will exacerbate data security risks, as businesses could be required to share data with other companies that may 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 data securely. For example, a data sharing obligation could require companies to share data with other businesses even if they cannot establish that those companies will not seek to re-identify anonymized non-personal data shared with them. Indeed, not all companies interested in receiving data may be able to afford or prioritize appropriate investments in strong privacy and security measures. In contrast, voluntary data sharing arrangements would permit companies to review, assess, and negotiate the implementation of adequate privacy and security controls with companies receiving non-personal data.

Therefore, BSA recommends that the Committee remove the revised Framework's recommendations to impose mandatory data sharing requirements, even for "public good" purposes. Instead, the Committee should recommend that the Government of India work closely with the industry stakeholders to develop and promote voluntary sharing arrangements and help identify "high value datasets" (**HVDs**) for the public interest.

2. Conduct Industry Consultation for Identifying HVDs and Promote Voluntary Data Sharing

In the revised Framework, HVDs that are beneficial to the community at large can be shared for broadly defined "public good" purposes.[8] The Committee describes a wide list of purposes for which

[5] See Para 3.4

[6] *See* Para 8.6(i).

[7] *See* Para 9.3(iv) and 9.4(iv).

[8] *See* Para 7.8 (i).

HVDs can be identified, including objectives such as creating new businesses and encouraging innovation.[9] Based on this definition, most types of datasets would qualify as an HVD. For example, completely distinct and unrelated datasets such as road traffic data and data held by a search engine could qualify as HVDs. This means that businesses may be compelled to share all such datasets and more with the government and other businesses, depending on how HVDs are identified under these broad "public good" purposes. Instead, **the Committee should develop an accountability-based governance framework to facilitate a fair and transparent consultation process with the industry for identifying HVDs to support public objectives to be made available on a voluntary basis.** Leveraging the experience of industry will help better advance voluntary data sharing for "public good" purposes, given that the private sector is well placed to understand the value of particular datasets.

Further, BSA suggests that the Committee consider promoting the development of different voluntary data sharing arrangements or mechanisms to enable data sharing for "public good" purposes. This will allow data sellers and buyers to benefit from mutually agreed data sharing, while preserving data security. For instance, data marketplaces might allow buyers and sellers to exchange datasets, while common data pools could be established for voluntary contributions of specific data categories. Government investments in research and development (**R&D**) and the creation of regulatory sandboxes could also help spur the development of such arrangements. Technical tools, such as application programming interfaces (**APIs**), can facilitate data exchanges that are faster and more secure than traditional transfers and create opportunities for empowering the public with greater access to their own data. The Committee may also look to promote the development and use of standardized data licensing models. Similarly, the Committee may consider promoting public-private collaborations as a means for Government and private organizations coming together to work on data-related areas on a voluntary basis. In this regard, please refer to BSA's Open Data Agenda[10] which aims to enhance the collective benefits of data through responsible policies that promote voluntary data sharing and foster opportunity, collaboration, and growth.

3. Remove Inappropriate Privacy and Data Protection Requirements for NPD

We fully support the Committee's recommendation to remove NPD completely from the scope of the PDP Bill.[11] However, the Committee continues to propose importing into the Framework concepts related to data categorization and related obligations from the PDP Bill. Categorizing NPD as sensitive or critical based on the nature of the underlying personal data from which it may have been derived makes little sense and imposing local storage requirements and restrictions on cross border flows on NPD[12] are both unnecessary and counterproductive. The revised Framework also requires entities to obtain a data principal's consent to anonymize personal data through an opt-out mechanism.[13]

---

[9] *See* Para 7.6.

[10] BSA's Open Data Agenda, dated June 2020 accessible at: Open Data: Bridging the Data Divide (bsa.org)

[11] *See* Para 5.1, 5.3.

[12] *See* Para 8.15(i)

[13] *See* Para 5.4.

This structure is likely to create substantial overlap between the two legal frameworks, introducing confusion for both companies and regulators. 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 Bill to comprehensively address privacy concerns. This recommendation is also contrary to the Committee's objective of streamlining and separating the regulatory regimes for NPD and personal data, given that consent and anonymization are already addressed under the proposed PDP Bill.

Moreover, the requirement to obtain consent to anonymize data may actually undermine the goal of storing data in privacy-protective ways. Anonymization helps to protect the identity and personal information of the data principal. Requiring users to consent to anonymization may disincentivize companies from implementing anonymization processes for services that might otherwise anonymize users' data — and limit the circumstances in which consumers and companies can reap the privacy benefits that come with anonymization.

Further, requiring consent for anonymizing personal data may hamper anonymization operations necessary to provide specific services to users. For instance, companies often need to anonymize data in a timely manner for cyber-security purposes, so that they can better process the data to understand threats against their products and services and protect their consumers from data breaches or fraud. A consent requirement for anonymizing personal data could impede processing personal data necessary to ensure the security of a data principal's data.

Thus, requiring consent for anonymizing personal data may prompt individuals to withdraw their consent or opt-out of anonymization without understanding the security or privacy risks involved.

We therefore recommend the Committee delete the requirement to obtain data principals' consent for anonymization and for using anonymized data.

4. Eliminate Local Storage Requirements

The Committee has retained local storage recommendations for NPD qualifying as "sensitive" or "critical" information.[14] This will disrupt the operations of companies, make it costlier to provide services in India, decrease opportunities for collaboration through data sharing, and increase barriers for competition, undermining efforts to ensure Indian consumers and businesses have cost-effective access to the best products and services. Local storage requirements do not advance data security or privacy. Indeed, such requirements may in fact increase privacy and security vulnerabilities by requiring storage in a single centralized location that may be more vulnerable to intrusion by making it susceptible to a single point of failure.[15] Such a requirement will also raise costs for business in India, deter investment in data-related enterprises and is inconsistent with global norms and practices.

The Committee should therefore remove restrictions on cross-border data flows and eliminate local storage requirements.

[14] *See* Para 8.15(i).

[15] Cross-Border Data Flows, BSA | The Software Alliance, accessible at: https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

5. Avoid Creating a Separate "Data Business" Category

The Committee should remove recommendations to create a broadly defined "data business" category,[16] along with associated mandatory registration[17] and meta-data disclosure requirements.[18] These recommendations, if adopted, will create disincentives to invest in India's digital ecosystem and will raise the cost of providing services to end-users in India. For instance, due to uncertainty on the classification and compliance obligations of a "data business", enterprises might be disincentivized to invest in the Indian market or refrain from providing value-add services (for example, security protection) to Indian businesses. This would run counter to the goals of Digital India and would adversely impact investments in data processing and outsourcing services in India. Further, the thresholds used to define a "data business" will be aligned to those of "significant data fiduciaries" under the PDP Bill.[19] This means that data businesses will be subject to a dual-regulation system i.e., as significant data fiduciaries under the PDP Bill and as data businesses under the Framework. **Therefore, BSA recommends that the Committee avoid creating new bureaucratic categories such as a "data business" and refrain from imposing additional regulatory requirements upon a broad swath of the Indian economy.**

6. Remove the Concept of a "Community Right" and a "Data Trustee"

The Committee should eliminate any recommendations to create legally binding exclusive "community rights" to NPD. [20] Such a layering of rights would introduce tremendous legal uncertainty for individuals, businesses, and other organizations. Consequently, this would substantially inhibit the ability of the enterprises, including SMEs and start-ups, to use the data in which they have invested time, money, and effort to collect and curate.

Further, the concept of "community" is vaguely defined. In the revised Framework, members of a community would be required to self-identify (as member of a community) and form a collective to assert their community rights. The revised Framework does not adequately explore how such a system would be implemented and how it could be designed to benefit such broadly conceived "communities." Further, it is also possible — and likely — that datasets will contain data related to multiple communities. This will result in a complex network of vested interests between data custodians and communities that make it more difficult for companies to share data in practice.

Moreover, to operationalize the allocation of a community right over NPD, the Committee has expanded upon the role played by a "data trustee". According to the revised Framework, a data trustee will be either a "Government organization or a non-profit private organization" that will create, maintain, and undertake data-sharing of HVDs in India.[21] Entities or individuals claiming to be part of a community (i.e., data requestors) will ask data custodians for access to HVDs, which can then be

[16] *See* Para 6.1

[17] *See* Para 6.2

[18] *See* Para 6.1(v)

[19] *See* Para 6.2(ii)

[20] *See* Para 7.1, 7.2.

[21] *See* Para 7.7.

made available to data requestors.[22] This is concerning because the Committee does not address the necessary checks and balances that a data trustee must put in place to ensure the security of the data it handles. Handling datasets currently maintained by private entities with sufficient infrastructure and experience in managing data in a safe and responsible manner is a major responsibility. Many not-for-profit private entities, and indeed some Government organizations, may not be sufficiently equipped in terms of infrastructure, expertise, or experience to handle high value NPD datasets.

Therefore, in addition to refraining from proposing the creation of "community rights", the Committee should also remove the concept of a "data trustee".

7. Avoid Recommendations on Creating a New NPD Regulator

The Committee should remove the proposal to create a new NPD Authority (**NPDA**) to oversee the governance of NPD.[23] While the revised Framework notes that the powers and functions of the NPDA should be harmonised with regulators such as the Competition Commission of India and the proposed DPA,[24] concerns over regulatory overlaps have not been addressed. For instance, the proposed NPDA is empowered to address privacy and to re-identification related harms. This will encroach upon the remit of the proposed DPA, which the PDP Bill would empower to address personal data protection related issues under the PDP Bill. 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.

We thank the Committee for the opportunity to provide our recommendations on the revised Framework 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.

Sincerely**,**

Venkatesh Krishnamoorthy
Country Manager, India
BSA | The Software Alliance

[22] *See* Para 7.7(iv).

[23] *See* Para 7.10, 7.11, 7.12.

[24] *See* Para 7.10 (i).