The Digital Personal Data Protection Bill, 2022

Comments from BSA | The Software Alliance

December 2022

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Ministry of Electronics and Information Technology (**MEITY**) on the draft Digital Personal Data Protection Bill, 2022 (**Bill**).[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Enterprise software companies support organizations across the world, including SMEs and large companies; local and central governments; hospitals, schools and universities; and non-profits. By offering trusted and responsible business-to-business software, enterprise software companies enable other organizations to serve their customers.

Businesses entrust some of their most sensitive data — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy, and security protections are fundamental parts of BSA members' operations. Businesses depend on BSA members to help them protect the privacy of data they handle, and our companies compete to provide privacy protective and security-protective products and services. BSA members recognize that companies must earn consumers' trust and act responsibly with their data and BSA members' business models do not depend on monetizing users' personal information.

We have extensive experience engaging with governments around the world to promote effective, internationally interoperable legal systems that protect personal information and provide strong consumer rights while supporting responsible uses of data-driven technologies. BSA has closely engaged with the Government of India for several years in its efforts to formulate a robust personal data protection law for India. We value our engagements with MeitY and are providing you this letter with additional context on our views of on the Bill, in addition to submitting our comments on the MyGov.in portal.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] See:https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

At the outset, we commend the MeitY for revising the Bill to more closely focus on personal data protection. We appreciate the following aspects of the Bill:

1. The omission of non-personal data from the Bill's scope. This will help meet the MeitY's objective of providing robust privacy protections to Indian consumers and citizens that focus on protecting their personal data.
2. The removal of data localization provisions and the Bill's support for transferring data across international borders, which can and should be further strengthened.
3. The objectives of the Bill's 'deemed consent' provisions, which recognize the need for organizations to process personal data for certain purposes when consent is either impracticable or inadvisable.

These changes will help to create a strong foundation for businesses operating in India to protect and safeguard consumers' personal data, helping to advance India's 1-trillion USD digital economy goals.

At the same time, several aspects of the Bill would benefit from improvements. Revising the Bill to address these concerns could help companies better adopt measures that implement the Bill's goals of protecting individual's personal data. Several of our recommendations would also increase incentives for developing secure and trusted technologies on which millions of Indian companies and consumers increasingly rely. To this end, we highlight below BSA's most significant recommendations. Our detailed recommendations, which were filed on the MyGov.in portal, are also contained in the Annexure appended to this letter.

1. Adopt an accountability-based approach to support cross-border data transfers

BSA welcomes the removal of data localization requirements from the Bill. However, Section 17 may inadvertently lead to local storage requirements. To address this concern, we recommend that the Bill should be revised to further support cross-border data transfers, while ensuring organizations remain accountable for protecting the privacy and security of personal data after transfer. This can be done by revising Section 17 to adopt the accountability model, under which entities that process personal data remain responsible for its protection, regardless of where the data is processed.

BSA recommends:

1. Section 17 should be revised to state that international transfers of personal data are permitted when a data fiduciary or data processor uses contractual or other means to provide a comparable level of protection to the data, regardless of where it is processed.

2. If the Bill retains the 'white-list' approach, we ***strongly recommend*** it recognize other transfer mechanisms, including transfers made with consent of the data principal and transfers based on interoperable mechanisms such as model contracts, intra-group schemes, and certifications like the APEC Cross-Border Privacy Rules (CBPR) system. If the 'white-list' is retained, the list should be notified well before the Bill's effective date.

2. Provide greater flexibility in grounds for processing personal data

BSA appreciates the goal of the Bill's 'deemed consent' provisions, which recognize the need for organizations to process data for certain purposes when consent is either impracticable or inadvisable, including for employment and 'public interest' purposes such as fraud detection, network and information security, among others. In our view, these may be best recognized as standalone grounds for processing, rather than treating them as 'deemed consent.'

BSA recommends:

1. Section 8(9) should be revised to permit Data Fiduciaries to self-determine if processing is for a "reasonable purpose" rather than requiring the Central Government to identify reasonable purposes by rulemaking.

2. A new subsection should be added to Section 8, expressly permitting processing necessary for the performance of contract to which a data principal is party.

3. Section 8(3) should be expanded to address processing necessary for compliance with laws.

3. Amend provisions on personal data breach

BSA supports reasonable and appropriate personal data breach notification requirements that provide incentives to ensure robust protection for personal data and enable data principals to take protective actions in the event their data is compromised.

BSA recommends:

1. Revising Section 9 to create a risk-based threshold for reporting breaches. Specifically, a breach should be reportable to the Data Protection Board (**DPB**) only if it creates a significant risk of material harm to principals.

2. Revising the definition of personal data breach, which should not include the phrase "unauthorized processing of personal data." This language inadvertently implies that that a violation of personal data protection obligations is a breach, in contrast to how a breach is understood in data protection laws internationally.

3. Revising Section 9 to avoid requiring Data Processors to report data breaches to the DPB or data principals. This obligation conflates the distinct roles of Data Processors and Data Fiduciaries. Instead, Data Processors should be required to notify an affected Data Fiduciary without undue delay if the processor becomes aware of a breach, so the Data Fiduciary may make further notifications as appropriate.

4. The Central Government should consult with stakeholders before prescribing breach regulations.

4. Ensure that rules are subject to stakeholder consultations and harmonized with sectoral regulations

The Bill provides broad powers to the Central Government to prescribe rules to implement several critical aspects of the legislation, including prescribing data breach notification requirements, identifying a 'white-list' of countries or territories to which data may be transferred, prescribing reasonable purposes that constitute deemed consent, among others. However, the Bill does not specify if those implementing rules will be adopted after a consultative process that involves robust stakeholder consultations.

BSA recommends:

1. The Bill should be revised to require the Central Government to consult with stakeholders prior to formulating any subordinate legislation or implementing regulations.

5. Provide a clear timeline for transition period and effective date

While the Bill states that different provisions may come into force on different dates, it does not provide clarity on the timeline for implementation of its various provisions or an overall effective date.

Ambiguity on these timelines for compliance creates significant concerns, because organizations require adequate time to put in place systems and processes to meaningfully implement the Bill's requirements.

BSA recommends:

1. The Bill should provide a clear transitional period of at least two years for implementation.

2. All implementing regulations should be finalized at least 12 months before they take effect, to ensure that companies have sufficient time to operationalize their requirements.

Conclusion

We commend Government of India's consistent commitment to safeguarding the privacy of Indian citizens and consumers. BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide our recommendations on the draft Bill. We support the Government of India's efforts in formulating the Bill successfully and look forward to continuing to work with the MeitY on privacy and personal data protection policies.

Please do not hesitate to contact the undersigned at venkateshk@bsa.org if you have any questions or comments regarding our suggestions.

Regards,

BSA | The Software Alliance

Annexure: BSA Submission to The Ministry Of Electronics And Information Technology on India's Digital Personal Data Protection Bill, 2022

Annexure

BSA SUBMISSION TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY ON INDIA'S DIGITAL PERSONAL DATA PROTECTION BILL, 2022

1. Transfer of Personal Data Outside India, Section 17

Recommendation: The Bill should be revised to further support cross-border data transfers while ensuring organizations remain accountable for protecting the privacy and security of personal data after transfer. We recommend revising Section 17 to adopt the accountability model, under which entities that collect personal data remain responsible for its protection, regardless of where the data is processed. Specifically, the bill should be revised to state that international transfers are permitted when a Data Fiduciary or Data Processor uses appropriate contractual or other accountable mechanisms to provide a comparable level of protection, regardless of where the data is processed.

More broadly, if the Bill retains the white-list approach, we strongly recommend it recognize other transfer mechanisms, in addition to any white-list. The Bill should permit transfers made with consent of the data principal and transfers based on interoperable mechanisms such as model contracts, intra-group schemes, and certifications like the APEC-CBPR & PRP systems. If the 'white-list' is retained, the list should be notified well before the Bill's effective date.

Justification: BSA welcomes the removal of data localization requirements from the Bill. However, Section 17 may inadvertently lead to local storage requirements by permitting overseas data transfers only after the Central Government 'white-lists' a country or territory. This undermines the intent of the Bill — captured in the explanatory note — which acknowledges the importance of cross-border data transfers. The white-list approach also creates considerable work for the Central Government to approve and operationalize the list, as the Justice Srikrishna Committee report noted that adequacy requirements have proven cumbersome. Moreover, relying solely on a white-list leaves companies without back-up mechanisms for transferring personal data across borders, meaning any disruption to the white-list could shut down the flow of data and India's ability to participate in the global digital economy.

Section 17 should instead be revised to adopt the accountability model, which was established by the Organisation for Economic Co-operation and Development (OECD) and later integrated into legal systems and privacy principles including the APEC Cross-Border Privacy Rules System (CBPR).

If the accountability model is not adopted and Section 17 instead requires companies to adopt specific mechanisms to transfer data, we strongly recommend it recognize multiple transfer mechanisms, in addition to any white-list. At minimum, companies should be permitted to transfer data on the basis of consent, pre-approved model contracts, intra-group schemes and international certifications.

Any "white-list" should be publicly consulted upon and published well before the Bill's effective date.

2. Deemed Consent, Section 8

Recommendation: We recommend: (1) revising Section 8(9) so that Data Fiduciaries are allowed to self-determine if processing is for a "reasonable purpose"; (2) adding a new subsection expressly permitting processing necessary for the performance of contract to which a data principal is party, and (3) expanding Section 8(3) to address processing necessary for compliance with laws.

Justification: BSA appreciates the goal of the Bill's 'deemed consent' provisions, which recognize the need for organizations to process data for certain purposes when consent is either impracticable or inadvisable. We suggest several revisions to better achieve this goal.

Revising Approach to Reasonable Purposes. We appreciate the Bill's recognition that a residuary ground for processing activities is needed, i.e., reasonable purposes. However, the Bill appears to

empower the Central Government to determine those reasonable purposes by regulation, rather than permitting organizations to self-identify such purposes. That is contrary to the goal of a residual ground for processing that is designed to permit flexibility. Because it may not be possible to predict and enumerate every "reasonable" purpose for which personal data may be processed, this provision may not create the flexibility intended. This approach also significantly departs from leading data protection laws which permit organizations to process data necessary for "legitimate interests." Assigning this reasonableness determination to Data Fiduciaries, rather than to regulations, reflects that organizations are well positioned to understand the benefits and risks of their processing and are accountable for those determinations. The Bill should revise its more burdensome approach.

Additional Ground for Processing Based on Contract. The Bill should add a new provision expressly permitting processing that is necessary to perform a contract to which a data principal is a party. In practice, this ground for processing is routinely used in day-to-day business transactions and, for that reason, has been explicitly recognized in data protection frameworks across the world.

Expanding Section 8(3) on Processing Necessary for Compliance with Laws. The Bill should broaden Section 8(3) to permit processing necessary to comply with legal obligations. The current is limited to processing necessary to comply with judgements or orders, which may not capture other situations where processing is necessary to comply with laws.

3. General Obligations of Data Fiduciary, Data Breach, Section 9(5)

Recommendation: We urge several revisions to Section 9(5): (1) breaches should only be reported if they create a significant risk of material harm to data principals; (2) the definition of breach should not include "unauthorized processing of personal data"; (3) Data Processors should not be required to report breaches to the DPB or data principals; and (4) the Government should consult with stakeholders before prescribing breach regulations.

Justification:

First, the Bill does not create a risk-based threshold for reporting breaches. Requiring notice of *every* breach creates a substantial risk of over-notification, particularly considering the expansive definition of data breach. To reduce over-notification and to ensure focus on high-risk or high-impact breaches, the Bill should require breaches be reported only if they create a significant risk of material harm to data principals.

Second, the Bill's definition of breach implies that a personal data protection violation — i.e., unauthorized processing of personal data — is a breach. This conflates a personal data protection violation with a data breach. This should be excluded from the definition.

Third, the Bill should not require Data Processors to report breaches to data principals or to the DPB. This conflates the responsibilities of Data Fiduciaries, which decide how and why to collect a data principal's information, and Data Processors, which process data on behalf of Data Fiduciaries and often lack a direct relationship with data principals. Given their role, Data Processors are generally not positioned to assess the impact of a breach on users, since they often lack access to or visibility over end-user data. Instead, the end-user facing entity — the Data Fiduciary — is generally best positioned to assess the impact of a breach and share information with the DPB and end-users. Placing this obligation on Data Processors can confuse both individuals and regulators, who may receive two notices of the same breach, one from each entity. Instead of requiring a Data Processor to notify the DPB and data principals, a Data Processor should be required to notify an affected Data Fiduciary without undue delay if it becomes aware of a breach, so the Data Fiduciary may make further notifications as appropriate.

Fourth, the Government should consult stakeholders before prescribing breach regulations, including to ensure any breach reporting timelines align with global best practices (i.e., at least 72 hours).

4. General Obligations of Data Fiduciary, Security Safeguards, Section 9(4)

Recommendation: Data Fiduciaries should have the primary responsibility for identifying and implementing reasonable safeguards to prevent data breaches. Data Processors should also have a responsibility to adopt reasonable safeguards that reflect their distinct role in handling personal data. We recommend revising Section 9(4) to state: "Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach, *in light of their role in processing that personal data*."

Justification: Both Data Fiduciaries and Data Processors have important obligations to safeguard personal data. However, Data Processors often lack visibility into personal data processed on their services and may not be aware of the risks associated with that processing unless informed by the Data Fiduciary, which is the entity that decides how and why to process a data principal's information. Because of their limited insight into personal data, Data Processors are often not in a position to determine the full range of standards and safeguards that should be employed to protect the data. The Data Fiduciary, on the other hand, is best placed to understand the benefits and risks of their processing activities and to provide instructions to the Data Processor based on their knowledge of the data principal, the personal data collected and processed, and the risks associated with that processing. Accordingly, Data Fiduciaries should have primary responsibility for adopting data protection safeguards while Data Processors should adopt reasonable safeguards in light of their distinct role in processing personal data.

5. Right to Correction and Erasure of Personal Data, Section 13(2)(d)

Recommendation: Section 13(2)(d) concerning Data Principals' right to erasure should be amended to: (1) subject the right of erasure in that section to the Section 9(6) flexibilities for data retention; and/or (2) clarify that "erasure" can be achieved by removing "the means by which the personal data can be associated with particular Data Principals."

Justification: To ensure that there is no ambiguity or conflict between the rights of data principals, Data Fiduciaries, and Data Processors, a consistent set of provisions should apply to data retention and removal.

We commend the Central Government for recognizing, in Section 9(6) that there are legitimate scenarios in which personal data will need to be retained by organizations (e.g., for accurate invoicing, and billing records reconciliation). We also appreciate the recognition that these retention obligations may be satisfied by removing "the means by which the personal data can be associated with particular Data Principals."

We suggest clarifying this same standard may be used in responding to requests by data principals to exercise their right of erasure pursuant to Section 13(2)(d). That section requires that personal data be "erased" unless retention is "necessary for a legal purpose." This provision could be read broadly to require complete destruction of data. To avoid such ambiguity, and to avoid adopting two separate standards for retaining data, we recommend that the right of erasure in Section 13(2)(d) be made subject to the standards of deletion/data retention in Section 9(6).

6. Engagement of Processors and Subprocessors, Section 9(9)

Recommendation: Section 9(9) should be revised to ensure Data Fiduciaries are not required to obtain a data principal's consent to engage processors. If the Bill is not revised to eliminate this requirement, Section 9(9) should be revised to expressly clarify that deemed consent satisfies any such obligation.

Justification: We support creating safeguards that ensure personal data is protected when it is handled by a Data Processor, including requiring the Data Processor to process personal data pursuant to a valid contract with the Data Fiduciary, as recognized in Section 9(9). However, this

section also suggests that a data principal must consent to a Data Fiduciary's use of Data Processors — a requirement that could flood individuals with dozens of consent requests without meaningfully improving their privacy protections. Indeed, Section 9(1) already ensures that personal data remains protected when it is handled by a Data Processor, because it requires a Data Fiduciary to remain responsible for complying with the Bill when personal data is processed on behalf of the Data Fiduciary by a Data Processor.

In today's economy, each Data Fiduciary is likely to rely on an extensive network of Data Processors to store, analyse, and process data on their behalf — and the Data Fiduciary may frequently add and drop those Data Processors to provide new services, or to engage a new Data Processor when an existing one is no longer able to provide a given service, or in instances where redundancy is required. Individual data principals should not be required to consent to each of these uses, which would create a significant burden. Instead, the Bill should be revised to require Data Fiduciaries to engage Data Processors pursuant to a valid contract, without also requiring consent of a data principal. Under this approach, personal data would remain protected under Section 9(1) and would be subject to contractual protections agreed to between the Data Fiduciary and the Data Processor.

7. Short title and Commencement, Section 1(2)

Recommendation: The Bill creates a range of new safeguards for companies handling personal data. We recommend that organizations be allowed sufficient time to come into compliance with the Bill's requirements by adopting a phased implementation approach. We suggest a minimum transition period of 24 months. In addition, we strongly that recommend any implementing regulations be finalized at least 12 months before taking effect and beginning enforcement.

Justification: Organizations require adequate time to put in place systems and processes to meaningfully implement the Bill's requirements. For example, if the Bill retains a white list approach to data transfers, organizations may need to revisit their contracts and processes to comply. Data Fiduciaries will also need time to implement appropriate technical and organizational measures, and to adopt security safeguards to prevent breaches in line with the Bill's requirements and regulations that are to be issued by the Central Government under the Bill's authority. Also, for several aspects, the granular details are to be prescribed by rules that will be developed once the law is in force.

Currently, the Bill does not specify a transition period, which creates uncertainty for organizations. Notably, the 2021 version of the Bill (recommended by the Joint Committee of Parliament) provided for a clear transition period of 24 months. We recommend a minimum transition period of 24 months. In addition, we strongly recommend ensuring any implementing regulations are finalized at least 12 months before they take effect, to ensure that companies have sufficient time to operationalize the requirements that will be imposed by implementing regulations.

8. Additional Obligations of Significant Data Fiduciaries, Section 11

Recommendation: We recommend deleting the Significant Data Fiduciary categorisation. However, if this categorisation is not deleted, we recommend that the Bill provide sufficient objective criteria for determining when an organization is a Significant Data Fiduciary instead of relying on the Central Government to notify an organization after applying a broad set of subjective factors.

We recommend revising Section 11(2)(a) to delete the requirement for a DPO to be based in India.

Justification: The criteria for designating an organization as a Significant Data Fiduciary are broad and many factors do not focus on the risks associated with the entity's processing activities. Using broad and vague factors such as public order, the security of the State, risks to electoral democracy and the potential impact on the sovereignty and integrity of India do not put companies on notice that they are likely to be deemed significant data fiduciaries — making it much more difficult for businesses to identify and adopt additional obligations in a timely manner. Moreover, the Bill creates the ability for the Central Government to specify any other factors that it considers necessary, exacerbating the lack

of notice to businesses. We recommend removing the Significant Data Fiduciary classification. However, if this category is not removed we strongly recommend the Bill be revised to specify objective factors for determining when an organization is a Significant Data Fiduciary, to ensure entities are on notice they may reach such a threshold. At minimum, Section 11(1)(g), which would permit notifying a Significant Data Fiduciary based on "other factors," should be deleted.

In addition, we are concerned with the potential to require independent data auditors for significant data fiduciaries. Requiring audits may create both privacy risks, by requiring additional companies be given access to personal data about a set of data principals, and business risks, because audits can implicate trade secret or business confidential information. The Bill already places other obligations on Significant Data Fiduciaries, including the appointment of a DPO and the requirement to conduct data protection impact assessments, that can achieve the goals of this provision without creating such risks. We therefore recommend deleting this requirement.

Finally, a DPO should be capable to act on behalf of entities in multiple jurisdictions and need not be physically based in India.

9. Data Protection Board of India, Sections 19, 20 and 21

Recommendation: The Bill should be revised to define the criteria for the membership and composition of the DPB and the selection committee that nominates members to the DPB. The selection committee should consist of the Chief Justice of India (or a judge nominated by him), the Cabinet Secretary and an expert nominated by the Chief Justice in consultation with the Cabinet Secretary.

Justification: BSA recognizes the importance of effective enforcement by an independent, fair, and transparent data protection authority to ensure efficiency and proportionality. However, in its current form, the Bill fails to create an institutional framework that achieves these goals. We focus on two concerns:

First, the Bill empowers the Central Government to establish a DPB and to prescribe the terms of the DPB, including its members and chairperson, through rules. The Central Government will also appoint the Chief Executive of the DPB. This gives the Central Government significant control over the DPB, which should be an independent sectoral regulator. Importantly, the Bill does not set out procedural checks and balances to ensure the independence of the DPB. The Bill also does not create baseline qualifications for members of the DPB. We recommend returning to the structure of the 2018 Bill, which clearly identified members of the selection committee, to better enable the creation of an independent regulatory body.

Second, several powers that were granted to the data protection authority in past versions of the Bill are now provided to the Central Government. The authority in past versions could issue regulations on several issues, including determination of reasonable purposes and adequacy findings. However, the Bill now empowers the Central Government to issue regulations implementing the Bill. To the extent that implementing regulations are needed, a specialized regulator like the data protection authority under past versions of the Bill may be better placed to make regulations. As noted below, any regulations should also be developed through a consultative process, ensuring that stakeholders can provide comments on draft regulations before they are adopted.

We also recommend that there should be a mechanism for submissions to the DPB to be kept confidential. Organizations will be making submissions on matters such as technological and operational measures, and these will include matters that are critical to network and information security of the company, as well as their financials, personnel, customer and other business information.

10. Power to Make Rules, Section 26

Recommendation: The Bill should require the Central Government to consult with stakeholders prior to formulating any subordinate legislation or implementing regulations.

Justification: The Bill provides broad powers to the Central Government to prescribe rules to implement several critical aspects of the legislation, including prescribing data breach notification requirements, identifying a white list of countries or territories to which data may be transferred, prescribing reasonable purposes that constitute deemed consent, identifying obligations of a significant data fiduciary, creating rules around children's privacy obligations, and setting out procedures for the removal and appointment of members of the DPB, among others. However, the Bill does not specify if those implementing regulations will be adopted after a consultative process that involves robust stakeholder consultations. Public consultations are an essential regulatory tool that can contribute to a predictable policy environment. We strongly recommend specifying that any regulations or subordinate legislation implementing the Bill be adopted only after a robust consultative process that allows all affected stakeholders to comment on proposed regulations or legislative text.

11. Additional Obligations in Relation to Processing of Personal Data of Children, Section 10

Recommendation: We recommend revising the definition of child to mean an individual under the age of 13.

Justification: The upper age limit of 18 for defining "child" clashes with other data protection frameworks such as the GDPR and the Unites States' Children's Online Privacy Protection Act. This could prevent some children — particularly teenagers — from accessing services. It could also increase the cost for Data Fiduciaries to provide these services.

12. Rights of Data Principals, Section 12

Recommendation: We recommend three changes to Section 12: (1) revising Section 12(1) to require a Data Fiduciary only to confirm whether it 'is processing' a data principal's personal data, but not whether it 'has processed' her data in the past; (2) revising Section 12(3) to require Data Fiduciaries to inform individuals of the *categories* of Data Fiduciaries with whom personal data has been shared, rather than the identity of each such company, and (3) adding a new provision to Chapter III permitting Data Fiduciaries to deny individual rights requests in certain instances.

Justification: First, Section 12(1) creates a right for individuals to confirm whether a data fiduciary "is processing or has processed" her personal data. The "has processed" language is problematic because it implies that Data Fiduciaries must indefinitely retain records to identify any data principal whose data they process. This sort of retention obligation is contrary to important principles of data protection, including the principle of data minimization.

Second, Section 12(3) should be revised to require Data Fiduciaries to inform individuals about the categories of Data Fiduciaries with whom personal data is shared, rather than naming those specific Data Fiduciaries. Providing the identities of each individual Data Fiduciary with whom personal data has been shared will prove burdensome and will not meaningfully assist the individual in exercising control over her data. We recommend that organizations be required to specify only categories of recipients.

Third, we suggest revising Chapter 3 to add a new provision recognizing instances in which Data Fiduciaries may deny individual rights requests. For example, Data Fiduciaries should be allowed to refuse to respond to a request that is a misuse of the Data Principal's rights such as where the request is a misuse or violation of other laws, would impede the rights and freedoms of third parties, including other Data Principals, or would involve divulging trade secrets or other business confidential information.

13. Notice, Section 6(3)

Recommendation: We recommend two changes. First, the Bill should be revised to recognize that the requirement in Section 6(3) to provide notice to a data principal in a range of languages may not be appropriate in situations such as employment or in business-to-business transactions, where all communication between the parties has taken place in a particular language. Second, we recommend revising Section 6(2) to avoid requiring new consent notices be provided to data principals for consent that was obtained prior to the Bill taking effect.

Justification:

First, Section 6(3) requires Data Fiduciaries to provide data principals with notice either in English or in another language in the Eighth Schedule. While we appreciate the objective to make notices accessible in local languages, this requirement would be onerous in certain situations and we suggest revising the Bill to recognize appropriate exceptions to this notice requirement. We also recommend revising the Bill to clearly state that companies are not required to translate notices into *each* language identified in the Eighth Schedule, which can significantly increase the amount of time and resources it takes to develop notices to consumers.

Second, Section 6(2) should be revised to avoid requiring companies provide new consent notices to data principals when consent was already obtained prior to commencement of the Bill. This may only result in more consent requests to consumers, which creates confusion and fatigue — and may cause data principals to pay less attention to consent requests rather than to focus on new consent requests for data processing they have not already approved.

14. Consent Manager, Section 7(6)

Recommendation: We recommend the removal of this concept from the Bill. In the alternative, if this provision is retained, we strongly recommend adding additional guardrails that protect the privacy of information collected and processed by consent managers.

Justification: The Bill and explanatory note envision the concept of a "consent manager" or "consent manager platform" to manage data principals' consent to Data Fiduciaries. However, the Bill provides little clarity on how consent managers will operate, creating significant uncertainty for both Data Fiduciaries that must obtain consent from consumers for processing and for individuals seeking to utilize consent managers.

Because consent managers are expected to function as intermediaries between Data Fiduciaries and data principals, it is critical to ensure their role is defined in a manner that carries out an individual's choices with respect to providing and withdrawing her consent. If this concept is retained, we strongly recommend revising this provision in two ways. First, any future regulations implementing requirements for consent managers should be subject to robust public consultations that focus on practical aspects addressing how Data Fiduciaries and data principals will engage with these entities in practice. Second, the Bill should create additional guardrails focused on ensuring the privacy of information collected and processed by consent managers, to ensure that a data principal's information remains protected when held by these Data Fiduciaries.

15. Financial Penalty, Section 25

Recommendation: We recommend a graded approach to penalties. We also recommend that 'significant' non-compliance be defined as instances in which actual harm to data principals has occurred, and financial penalties be imposed only in such cases.

Justification: The Board's resources and attention should be focused on the most consequential areas of noncompliance, where there has been actual harm to individuals. We suggest that 'significant' be determined in the context of instances where actual harm has occurred to individuals.

16. Exemptions, Section 18

Recommendation: We make two recommendations on revisions to Section 18. First, Section 18(1) should be revised to clarify the scope of exemptions in this provision. Specifically, we recommend adding parentheticals, so that this provision states: "The provisions of Chapter 2 (except sub-section (4) of section 9), Chapter 3, and Section 17 of this Act shall not apply where:" Second, we recommend expanding Section 18(2)(b) to expressly recognize processing for "commercial" research.

Justification:

Revisions to Section 18(1). Section 18 creates important exemptions to the Bill, including for processing necessary to enforce a legal right or claim; the processing of personal data by certain courts or tribunals; processing to prevent, detect, investigate, or prosecute certain offenses; and processing the personal data of data principals not within India pursuant to a contract entered into by a person outside of India. We strongly recommend revising Section 18(1) to clarify the scope of these exceptions. This is particularly important for Section 18(1)(d), which addresses the processing of personal data of data principals not within India – since that data would be transferred into India pursuant to a contract with a person located outside of India and, upon completion of the processing, would be transferred from India back to such a person. Our recommendation is intended to clarify Section 18(1) to ensure that Section 17's provisions on cross-border transfers are not inadvertently read to apply in such circumstances.

Revising Section 18(2) to expand processing for research. The Bill recognizes that use of personal data for research is critical for bringing new innovations to Indian citizens and for India's global competitiveness. We recommend expanding Section 18(2)(b) to expressly include "commercial" research.

17. Consent, Section 7(5)

Recommendation: Section 7(5) should be revised to recognize that if a data principal withdraws her express consent for processing personal data, the data may still be processed pursuant to the deemed consent provisions in Section 8. We recommend revising Section 7(5) to state: "If a Data Principal withdraws her consent to the processing of personal data under sub-section (4), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing of the personal data of such Data Principal unless such processing without the Data Principal's *express* consent is required or authorized under the provisions of this Act *(including processing permitted under Section 8)* or any other law."

Justification: Section 7(5) recognizes the importance of allowing data principals to withdraw their consent to processing, while also recognizing that organisations may need to process data for purposes permitted by the Bill. We recommend clarifying that those purposes include the purposes covered by the deemed consent provisions in Section 8, which addresses processing for purposes such as compliance with legal judgments, employment purposes, and certain processing in the public interest is appropriate, even when the data principal has not provided express consent.

Here are the 'submission ID' numbers corresponding to the submission made on the mygov.in portal:
81672294, 81674064, 81684294, 81712654, 81746764, 81758414, 81782364, 81788894, 81800084, 81827484, 81832724, 81836414, 81839514, 81907364, 81933794, 81942574