February 25, 2020

Director,
Room No. 152, Ground Floor,
Lok Sabha Secretariat,
Parliament House Annexe,
New Delhi-110001

Cc:
Shri Ajay Prakash Sawhney, Secretary, MeitY
Shri S. Gopalakrishnan, Additional Secretary, Meity

Dear Sir/Madam,

Subject: BSA Submission to the Joint Parliamentary Committee on India's Personal Data Protection Bill, 2019

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

P (91 11) 4978 9066
W bsa.org

BSA | The Software Alliance (**BSA**)[1] appreciates this opportunity to present its views to the Joint Committee (**Committee**) on the Personal Data Protection Bill, 2019 (**Bill**).[2]

BSA recognizes that growth of the data economy is key to India realizing its vision of a $5 trillion economy. Data-driven services support innovation and present huge economic opportunities by empowering consumers to make better decisions and enabling merchants to optimize their services. At the same time, robust data protections are an important part of the digital economy, as they ensure respect for individuals' fundamental rights and strengthen the trust that is necessary to promote full participation in digital society.

Although many aspects of the Bill would lay a strong foundation for a robust data protection framework in India, several provisions pose substantial challenges to BSA members and other organizations that operate globally without advancing the objectives of the Bill.

As the Committee considers revisions to the Bill and moves towards enacting it into law, BSA urges due consideration of the issues raised in these comments. In this letter, we highlight some of BSA's most significant concerns and provide our recommendations to the Committee. The attached annex provides a more detailed and comprehensive explanation of our concerns with and recommendations for the Bill.

---

[1] BSA | The Software Alliance (www.bsa.org) 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] The Personal Data Protection Bill, 2019 (December 2019), available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

1. Non-personal data

Clause 91 grants the Central Government sweeping authority to require "any data fiduciary or data processor" to provide "any personal data anonymized or other non-personal data" for government purposes. This raises substantial concerns on several levels.

First, the scope is far too broad, essentially encompassing any data other than non-anonymized personal data. This would appear to grant the Central Government the authority to gain access to all manner of data which could significantly harm the interests of business entities.

Second, the legislation is primarily designed to enhance and protect the personal information of data subjects in India, and expanding the scope of this Bill to all data goes far beyond that core, and essential purpose.

Finally, we understand that the Central Government, under the leadership of the Ministry of Electronics and Information Technology (**MeitY**) has organized a committee of experts (**MeitY Committee**) to deliberate on a "data governance framework" and issues relating to non-personal data.[3] While BSA and our members have substantial concerns with this exercise itself, a deliberative process designed to consider the policy objectives at hand, the definitions of the information under question, and the possible approaches the Government might take to address its objectives is far preferable to simply introducing sweeping authority with little public debate into this Bill.

RECOMMENDATION: The Committee should eliminate Clause 91 from the Bill and defer discussion of whether and how the government should regulate non-personal data to a more deliberative and consultative process, such as the MeitY Committee.

[3] Constitution of a Committee of Experts to deliberate on Data Governance Framework (September 2019), available at: https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf

2. Data localization

Chapter VII lays out proposed restrictions to the transfer of personal data outside India. Specifically, Clause 33 (1) states that "sensitive personal data may be transferred outside India (subject to conditions), but such sensitive personal shall continue to be stored in India." Clause 33(2) states that "critical personal data shall only be processed in India".

We are deeply concerned about these proposed restrictions on international data transfers and requirements to localize certain data in India. Limitations on data transfers, and requirements to store data in particular locations do not advance data protection goals. Rather, they disrupt companies' operations and increase the costs of providing services in India.

Rather than restricting data transfers and focusing on data localization, good regulation and practice will focus on ensuring data fiduciaries (**DFs**) are required to handle data according to reasonable consumer expectations, and both data fiduciaries and data processors are obligated to ensure the highest standards of data security.

We are also concerned about the narrow grounds for processing data, including for international data transfers. Consent is one basis for acquiring, storing, transferring, and processing data, but in the modern digital economy, it cannot be the only legal grounds for managing such data.

In addition, we are concerned about the invention of an entirely new class of personal information, so called "critical personal data". This is inconsistent with international practice and will likely cause confusion on the part of consumers and businesses and impose additional costs and burdens on the data protection authority (**Authority**).

RECOMMENDATIONS:

1) Remove Clause 33 and the data localization requirements it imposes, and focus instead on strengthening practices that will secure data.
2) Remove references to "critical personal data". At the very least, ensure that the concept of "critical personal data" is defined in a manner that is narrowly tailored based on highly sensitive national security considerations to create more predictability for companies that may process such data.
3) Include exhaustive definitions of any categories of sensitive or critical personal data subject to the Bill. Any new categories should be added by amending the law, not through government notifications.

4) Revise Clause 33 and its restrictions on data transfers, to focus providing accountability for cross-border data flows and recognizing the role of private contractual arrangements in strengthening accountability mechanisms. To the extent an adequacy requirement is used for data transfers, the Bill should maximize consistency with existing mechanisms under other data protection frameworks.

3. Grounds for processing

Chapter III describes the available grounds for processing personal data without consent. While the enumeration of additional grounds for processing is helpful and consistent with international practices, we make the following recommendations to further enhance the Bill's functionality while maintaining high levels of personal information protection

RECOMMENDATIONS:

1) DFs should be allowed the discretion to self-determine if processing is for a "reasonable purpose" rather than requiring the DPA to issue regulations identifying each "reasonable purpose".
2) Revise Clause 14(2) to expressly recognize that all the purposes listed under that section each considered a "reasonable purpose" and include processing necessary for the performance of contract to which a data principal is party as a "reasonable purpose".
3) To the extent the DPA retains authority to specify "reasonable purposes," the Bill should require the DPA to solicit and incorporate input from stakeholders before issuing regulations specifying such purposes.
4) Extend the employment purpose as a valid ground for processing to sensitive personal data (**SPD**) by applying Clause 13 to SPD as well.

BSA appreciates the Committee's solicitation of feedback on the Bill and would be very happy to serve as a resource as development of the Bill continues. BSA would be honored to appear before the Committee to explain our recommendations in person.

Kind Regards,

Venkatesh Krishnamoorthy
Country Manager - India
BSA | The Software Alliance

BSA SUBMISSION TO THE JOINT PARLIAMENTARY COMMITTEE
ON
INDIA'S PERSONAL DATA PROTECTION BILL, 2019

The Personal Data Protection Bill, 2019 ("**Bill**") was introduced in Parliament in the winter session and referred to a Joint Parliamentary Committee ("**JPC**") on December 12, 2019. The table below highlights provisions of the Bill that are of concern to BSA, and proposed recommendations.

Provision	Requirement	Concerns	Recommendations
Data localization: Clause 33	• The Bill imposes data localization requirements for two types of data: sensitive personal data and critical personal data. • Sensitive personal data: Must be stored in India, but may be transferred outside India. o "Sensitive personal data" is defined to include a broad range of data types, including financial and health data. o The Central Government may add new data types to this definition. • Critical personal data: Shall only be processed in India. o "Critical personal data" is not defined. Rather, then Bill allows the Central	• Data localization requirements do not advance data protection goals. Rather, they disrupt companies' operations and increase the costs of providing services in India. • *Sensitive personal data.* This is defined broadly and, in many cases, could not be separated from other types of data. As a result, the practical effect of the bill is likely to be requiring nearly all types of data to be stored in India. This would severely disrupt operations of both data fiduciaries ("**DFs**") and data processors ("**DPs**"), including limiting services available to DFs. Moreover, allowing the Government to add new categories of "sensitive personal data" increases regulatory uncertainty for businesses. • *Critical personal data.* The absence of any clear criteria for classification of "critical personal data" creates more	• We recommend deleting Clause 33 and instead focus on strengthening practices that will secure data. • Alternative approach. The Bill should instead recognize the role of private contractual arrangements, internationally-recognized certification mechanisms, and other transfer mechanisms in strengthening accountability mechanisms and promoting cross-border data flows. For example, creating a general obligation for processors and fiduciaries to be accountable – as is the case under Canada's Personal Information Protection and Electronic Documents Act – is a more effective way to achieve the goal of ensuring high levels of data protection than

Provision	Requirement	Concerns	Recommendations
	Government to designate categories of data as critical personal data without specifying any criteria for such designations.	uncertainty for businesses and negative consequences for commercial operations, R&D, and continued investment.	imposing data localization requirements. • Sensitive personal data should be reserved for categories of data that carry special risks in relation to discrimination and abuse of fundamental rights. Given that sensitive personal data is broadly defined and includes financial data, official identifiers, health data, and other broad categories of data, the Bill would place unreasonable restrictions on cross-border data flows that could hurt key industries, including the digital payments and healthcare industry in India • We recommend that the Bill remove references to "Critical personal data." At the very least, if this category is retained, the Bill should ensure that the concept of "critical personal data" is defined in a manner that is narrowly tailored based on highly sensitive national security considerations to create more predictability for companies that may process such data. Additionally, the Bill should define

Provision	Requirement	Concerns	Recommendations
			all categories of critical personal data (to the extent that the Bill retains the concept of "critical personal data") and sensitive personal data. Any new categories should be added by amending the law, not through government notifications.
Restrictions on cross-border data flows: Clause 34	• Sensitive personal data: May only be transferred outside India for the purpose of processing, when both: (1) explicit consent is given by the data principal and (2) the transfer is made either: o pursuant to a contract or "intra-group scheme" approved by the Authority; o pursuant to an adequacy determination; or o with approval of the Authority for a transfer "necessary for any specific purpose." • Critical personal data: May only be transferred outside India when such a transfer is: o for the purpose of "prompt action" in the provision of health or emergency services	• 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 electronic growth. As the Justice Srikrishna Committee's initial White Paper recognized, data localization measures have negative economic impact on GDP. • Sensitive personal data. This term captures a broad range of data types that are vital to India's digital ecosystem and necessary to provide services such as medical diagnosis and peer-to-peer digital payments. Restricting the cross-border flow of sensitive personal data could slow down economic growth and hurt key industries, including the financial sector and healthcare businesses. o Even where a provider has hosting facilities in India it is likely	• *Alternative approach.* For both sensitive personal data and critical personal data, we recommend revising the Bill to: o Focus on accountability for cross-border data flows, rather than requiring adequacy and/or consent for all international transfers. Under the accountability model, entities that process personal data should remain responsible for its protection, regardless of where the data is processed. o Make "explicit consent" one basis for cross-border transfers, without including consent as an additional requirement when other

Provision	Requirement	Concerns	Recommendations
	o to a person/entity in a country or international organization pursuant to an adequacy determination where the transfer does not prejudicially affect the security and strategy interests of the State.	that some features or functionality will require certain data to be stored outside of India. o Requiring explicit consent as a prerequisite to transferring any sensitive data is not practical. For example, in the GDPR, consent it is presented as one of multiple options rather than a necessary condition. o Allowing transfers based on an adequacy determination does not resolve these concerns. The Justice Srikrishna Committee, in its report ("**Report**") noted that adequacy requirements for conducting international transfers have proven cumbersome. Such requirements impose a significant regulatory burden, and the capacity to make such determinations is currently lacking. • *Critical personal data.* The Bill appears to contemplate transfers of critical personal data only when case-by-case determinations are made by the Central Government. This creates considerable uncertainty for businesses, which would	legal mechanisms for cross-border transfers are invoked. o Allow organizations to transfer data pursuant to grounds such as certifications, which are incorporated in other global data protection frameworks (including the EU's GDPR and Brazil's newly enacted data protection law). o Specify "reasonable purposes" such as cybersecurity and fraud prevention as a permissible basis for transfers. • *Adequacy.* To the extent an adequacy requirement is used, the Bill should maximize consistency with existing mechanisms under other data protection frameworks. For example, it should recognize as adequate transfers made pursuant to APEC's Cross-Border Privacy Rules, EU standard contractual clauses, and binding corporate rules, and should not create national versions of these same mechanisms.

Provision	Requirement	Concerns	Recommendations
		be prohibited from transferring the data altogether if it is deemed critical. Moreover, those case-by-case determinations may come only after an adequacy decision. That structure puts significant pressure on the Indian government's ability to conclude such decisions, and the capacity to make such determinations is currently lacking.	• *Critical personal data*. We recommend removing the additional requirement that cross-border transfer of "critical personal data" is permissible only when it does not prejudicially affect the security and strategic interests of the state, in the opinion of the Central Government.
Penalties and Compensation: Clause 57-61, Clause 64, Clauses 82-85	• Criminal penalties can be imposed for the offence of re-identifying personal data that has been de-identified, without consent of the data principal. Employees may also be deemed guilty of a company's offense under Clause 84. • Monetary penalties are imposed for a range of other violations. For instance, DFs may be subject to a penalty of up to fifteen crore INR or four percent of total annual turnover for failing to adhere to security safeguards or transferring data outside India in violation of the Act. • In determining the amount of a monetary penalty, the Adjudicating Officer is to consider a number of	• *Criminal liability* for data protection violations is contrary to international best practices. Criminal liability can chill beneficial and harmless data practices – and the current language imposing broad liability on employees also discourages individuals from working for companies subject to the Act. Rather, privacy laws should ensure that remedies and penalties for violations should be structured to be effective and proportionate to the harm resulting from violations. Criminal penalties are not proportionate remedies for violations of data protection laws and do not have a useful role to play in enforcing them. • *Monetary penalties* should also be proportionate and reflect cooperation with the DPA as a mitigating factor. This	• *Criminal liability*. We strongly recommend removing the possibility of criminal liability. • *Monetary penalties.* The Bill should explicitly include degree of cooperation with the data protection authority ("**DPA**") as a mitigating factor.

Provision	Requirement	Concerns	Recommendations
	factors, including the nature, gravity and duration of the violation, the number of data principals affected, intent or negligence of the violator.	provides an important incentive for cooperation that can help substantially reduce harms to data principals. In addition, considering cooperation helps to ensure that penalties are structured to be effective and proportionate to the harm resulting from a violation. Notably, the GDPR provides that monetary fines are to be imposed "in each individual case" if "effective, proportionate, and dissuasive."	
Relationship between data processors and data fiduciaries and allocation of liability: Clause 31, Clause 64	• Contracts required for data processors. DFs are not to use DPs to process data on their behalf without a contract. • Subprocessors. DPs are not to engage subprocessors "except with the authorisation" of the DF and "unless permitted in the contract" between the DF and the DP. • Data processors act on behalf of DFs. The Bill prohibits DPs from processing data except "in accordance with the instructions" of the DF and are to treat such information as confidential. • Liability. Two provisions address liability of DPs:	• *Subprocessors*. The Bill does not clarify what authorization is required from a DF to engage a subprocessor, and whether general authorization is permitted. Requiring explicit consent would be a restrictive standard that disallows DPs sufficient flexibility to conduct their operations. For example, Article 28(2) of the GDPR permits a general written authorization in which a processor may inform a controller of intended changes or replacements for subprocessors and enable the DF to object. This approach provides needed flexibility to a DP while offering a reasonable opportunity to a DF to object. • *Recognition of processing required by law*. It is critical to ensure that data processors may process data as they are required to do by law. The 2018 Bill did	• *Subprocessors*. Clause 31 should be revised to clarify that the authorization to engage subprocessors is a general written authorization. • *Processing required by law.* The Bill should be revised to expressly state that DPs may process personal data as required by law, even if not instructed to do so by a DF. It may do so by including language from section 37(3) of the 2018 bill. • *Liability*. We recommend that the Bill should be revised to clarify that only DFs are responsible for compensating data principals for any violation relating to their obligations under the Bill. However, DFs and DPs may enter into

Provision	Requirement	Concerns	Recommendations
	o DPs are only liable for actions "outside or contrary to the instructions of the data fiduciary" or negligence. Clause 64(1). o Where more than one DF or DP "are involved in the same processing activity," either company must pay the entire amount of compensation to a data principal for harm caused. That company may then claim compensation from the other entity, corresponding to their role in the harm caused. Clause 64(5)-(6). • Security safeguards: The Bill mandates DPs and DFs to undertake the implementation and review of security safeguards.	so, recognizing in section 37(3) that a DP is to process information at the instruction of a DF "unless they are required to do otherwise under law." The Bill removes this language. • *Liability*. The Bill muddles a clear separation between DFs' and DPs' responsibilities by creating a confusing structure for compensating data principals. • *Security safeguards* – Both DFs and DPs have important obligations to safeguard data. Often the DP may not have visibility to the personal data and may not be aware of the particular risks unless informed by the DF. The DF is in the best position to understand the benefits and risks of their processing activities and provide instructions to the DP based on the DF's knowledge of the data subjects, personal data collected and processed, and the risks associated with processing. Therefore, contracts should necessarily identify the applicable security safeguards and standards to be adopted by the DP.	agreements that allocate liability differently among themselves. In addition, the explanation to Clause 64 should be revised to remove the reference to imposing liability on DPs for negligence. Rather, it should be limited to where the DP acts against the DF's instructions or fails to provide adequate safeguards. • *Security safeguards*- Consistent with an accountability model, we recommend that the primary responsibility for identification and implementation of applicable standards and safeguards should vest with the DF. The DF in turn will be contracting with the data processor for services based upon the DF's assessment of the nature of the processing (and any associated risks) based on its own understanding of the nature of the personal data collected, *purpose for collection etc.*

Provision	Requirement	Concerns	Recommendations
Grounds for processing: Clause 11-14	• Personal data may be processed without obtaining consent if it is necessary for "reasonable purposes", which are to be specified by the DPA. • Data may be processed without consent if necessary for a "reasonable purpose," after considering: o Interest of the DF; o Whether the DF can be reasonably expected to obtain consent of the data principal; o Any public interest; o The effect of processing on rights of the data principal; o Reasonable expectations of the data principal with regard to the processing. • DPA is to issue regulations identifying "reasonable purposes," which may include: o prevention and detection of unlawful activity; o whistle blowing; o mergers and acquisitions; o network and information security;	• *Primacy of consent.* Consent has been given primacy, with all the other grounds essentially being framed as exceptions. It is not helpful to give the impression that consent is the favored grounds for processing as practical experience from other jurisdictions demonstrates that the market and regulators are prone to become over reliant on it, which can result in consent fatigue for consumers. • *Need for residual ground of processing.* As the Committee's report recognizes, there is a need for a residual ground for processing activities that are not covered under other grounds of processing. By way of an example, the GDPR recognizes the concept of "legitimate interest" as a residual ground for processing. Requiring the DPA to identify "reasonable purposes", rather than allowing DFs the discretion to do so, creates at least two concerns: o Requiring the DPA to set out a specific list of "reasonable purposes" is contrary to the need to ensure a residual ground that permits flexibility in processing data.	• *Equal grounds for processing.* The grounds for processing should be presented on an equal footing, as opposed to exceptions from consent. • *Determination of "reasonable purposes."* We recommend that DFs be allowed the discretion to self-determine if processing is for a "reasonable purpose" rather than requiring the DPA to issue regulations identifying such purposes. • *List of "reasonable purposes."* Clause 14(2) should also be revised to expressly recognize processing necessary for the performance of contract to which a data principal is party as a "reasonable purpose". • *Stakeholder input on "reasonable purposes."* To the extent the DPA retains authority to specify "reasonable purposes," the Bill should require the DPA to solicit and incorporate input from stakeholders before issuing regulations specifying such purposes.

Provision	Requirement	Concerns	Recommendations
	o credit scoring; o recovery of debt; o processing of publicly available personal data; and o operation of search engines.	o DPA approval could be cumbersome in practice, posing substantial burdens to both DPA and industry. • *Processing for purposes of employment.* It is helpful that Clause 13 recognizes several grounds for processing employee data, however it is overly narrow because it excludes sensitive data. That creates concerns because employee data may need to be processed in a context that includes sensitive personal data (SPD), such as making available insurance or processing special leave like maternity benefits. As a result, Clause 13 may not be sufficiently broad to enable such processing, unless it is extended to cover SPD.	• *Processing for purposes of employment*- We recommend that employment purposes as a valid ground for processing should be extended to SPD as well. Therefore clause 13 should be made applicable to SPD as well.
Transparency and accountability measures: Chapter VI	• Significant DFs: The Bill would allow the DPA to classify "significant data fiduciaries" and impose additional obligations on them. *Classification*. The DPA may classify DFs as significant DFs on the basis of: o volume of personal data processed; o sensitivity of data;	• *Designation of Significant DFs*: The "significant data fiduciary" classification is problematic because it is based on factors that bear little relation to the risks of processing or the sensitivity of data processed. For example, it is unclear how "turnover of the data fiduciary" and the "use of new technologies" relate to heightened data processing risks.	• *Significant DF classification.* We recommend removing the "significant data fiduciary" classification. Instead, the Bill should impose stricter obligations on DFs undertaking activities that carry greater risk to data principals. • *Data protection impact assessments*. We recommend revising the Bill so that significant

Provision	Requirement	Concerns	Recommendations
	o turnover of DF; o risk of harm through processing by DF; o use of new technologies; and o any other factor causing harm. *Obligations*: Significant DFs are subject to at least three significant obligations: o *Data Protection Impact Assessments*. Significant DFs are required to conduct a data protection impact assessment ("**DPIA**") before undertaking any processing that has the potential to cause significant harm to data principals. The DPIA is to be submitted to the DPA, which may direct the Significant DF to cease the processing or impose conditions on it on a low showing, when it has "reason to believe that the processing is likely to cause harm to the data principals."	• *Data protection impact assessments.* While DPIAs are an important part of data protection programs, the Bill treats them as a tool of precautionary regulation that could overwhelm the DPA with paperwork. Consistent with the notion that DPIAs are an accountability tool, the Bill should require them to be kept on record and provided to the DPA on request. • *Audits.* Annual audits create a significant new and burdensome element to global privacy programs, which typically do not include routine audits. Moreover, a "data trust score" derived from such audits is unlikely to be meaningful to a Significant DF's complex considerations on processing data and could create misleading impressions for consumers on the trustworthiness of Significant DFs. • *Data protection officers*: While DPOs are now an established part of global data protection programs, requiring a DPO to be in India undermines global compliance efforts by designating DPOs who are not otherwise part of more centralized efforts to address global data protection and privacy issues.	DFs are required to keep DPIAs on record, and only provide them to the DPA on request. • *Audits*. We recommend revising the provision on audits, to focus on allowing the DPA to conduct data audits only under appropriate circumstances. In addition, the "data trust score" should be removed from the bill. • *Data Protection Officers*. We recommend revising this provision to eliminate the requirement that DPOs be located in India. • *Privacy by design policies.* We recommend clarifying that a DF's decision to submit its policy to the DPA is voluntary.

Provision	Requirement	Concerns	Recommendations
	o *Audits.* Significant DFs are required to engage an independent data auditor to conduct annual audits of their policies and processing activities. o *Data Protection Officers*. Significant DFs must appoint India-based data protection officers ("**DPO(s)**"). • Privacy by design policy: Every DF shall prepare a privacy by design policy. Subject to regulations, a DF may submit its policy to the DPA for certification.	• *Privacy by design policies*: While the requirement to submit the privacy by design policy to the DPA appears to be voluntary, the provision begins with "subject to the regulations made by the Authority", creating uncertainty on whether the provision is voluntary or mandatory.	
Powers of Central Government: Clause 15, Clause 33, Clause 42, Clause 43, Clause 91	• Non-Personal Data. The Central Government may "direct any" DF or DP to "provide any personal data anonymized or other non-personal data" for certain purposes. • In addition, the Bill gives the Central Government significant authority, often including open-ended authority. This includes: o Creating new categories of sensitive personal data, after	• *Non-Personal Data.* Empowering the Central Government to demand non-personal data from companies is a cause for significant concern, as it could require companies to share their proprietary data with the government. This will hurt the business confidence of companies. • *Defining sensitive and critical data.* The Central Government's ability to define "critical personal data" and "sensitive personal data" raises critical concerns	• *Non-personal data*. We recommend removing provisions pertaining to non-personal data. • *Sensitive and critical data*. We recommend that the Bill remove references to "critical personal data." At the very least, if this category is retained, the Bill should ensure that the concept of "critical personal data" is defined in a manner that is narrowly tailored

Provision	Requirement	Concerns	Recommendations
	consultation with the DPA and the sectoral regulator concerned, based on certain factors. o Determining what constitutes "critical personal data." The Bill does not identify any factors or other criteria for such determinations. o Appointing members of the DPA, based on recommendation by a selection committee of government officials. o Removing members of the DPA, including for abusing their position.	about a lack of certainty for businesses, which are heightened by requirements to limit the transfer and storage of such data. • *Appointment of DPA.* The committee to select members of the DPA consists solely of Central Government officials. This suggests that the Central Government will have significant control over the DPA, which is meant to be an independent sectoral regulator.	based on highly sensitive national security considerations to create more predictability for companies that may process such data. Additionally, the Bill should define all categories of critical personal data (to the extent that the Bill retains the concept of "critical personal data") and sensitive personal data. Any new categories should be added by amending the law, not through government notifications. • *Appointment of Chairperson and Members of the DPA*. We recommend that Clause 42(3) of the Bill should be revised to reflect the position under the 2018 Bill, in which the selection committee consisted 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.

Provision	Requirement	Concerns	Recommendations
Personal data breach: Clause 25	• "Personal data breach" means any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal. • Breach notification. The Bill requires DFs to report a breach of personal data to the DPA, if it is "likely to cause harm to any principal". • Timing of notification. The DF must notify the DPA "as soon as possible" and within any period specified by regulations issued by the DPA following the breach after accounting for any period that may be required to assess its potential impact on data principals. • Content of notice. The notice is to include: (1) nature of the data, (2) the number of data principals affected, (3) possible consequences, and (4) actions taken by the DF to remedy the breach.	• The current definition includes "loss of access" to personal data as a personal data breach. This inclusion is very broad and could also be interpreted to include temporary loss of access to personal data which may for instance be due to authorized and planned system maintenance carried out by a DF which is lawful and does not have adverse impact on the data principals. • *Trigger for notification to DPA.* The reporting trigger for breach is set too low at "likely to cause harm." This creates a significant risk that the DPA will be over-notified, resulting in a volume of notices that make it difficult for the DPA to identify the most significant breaches. • *Timing of notice*. Reporting a breach "as soon as possible", or a time period specified by the DPA, leads to unrealistic and inflexible timelines. DFs should ensure they ascertain relevant facts prior to notification, to avoid confusion and lessen the need for follow-up notifications.	• *Definition of breach.* Clause 3(29), defining "personal data breach" should expressly require either an unauthorized "loss of control" or a permanent "loss of data", to constitute a breach. • *Trigger for notification*. The Bill should only require notice to the DPA of personal data breaches that are reasonably likely to cause a significant risk of material harm to data principals. • *Timing of notice*. Instead of relying on the DPA to set an explicit deadline for notification, the Bill should require notification "as soon as practicable" or "without undue delay." This timeline should only begin when the team within the DF is aware of the breach, not when the breach occurs, and has sufficient time to assess its impact on data principals. Therefore, the Bill should also expressly add that the notification should be following the "awareness" or "discovery" of the breach and the DF has had

Provision	Requirement	Concerns	Recommendations
	• Action by DPA. Upon receipt of a notice, the DPA is to determine whether the DF is to report a breach to the data principal. The DPA may also require the DF to take appropriate remedial action and post details of the breach on its website.		sufficient time to assess its potential impact on data principals. • *Notification to data principals.* Regardless of the DPA's power to determine whether a breach is notifiable to data principals, DFs should have the right to voluntarily notify data principals prior or in parallel to notification of the DPA in order to minimize the impact of a breach.
Personal data of children: Clause 3 (8), Clause 16	• Child. A child is defined as person under the age of 18. • General obligations. Each DF is to process personal data of a child "in such manner that protects the rights of, and is in the best interests of, the child." • Consent required. DFs must verify the age and obtain consent of the child's parent or guardian before processing any personal data of a child.	• *Age limit*. 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 increase the cost for DFs to provide services and prevent some children—particularly middle and older teenagers—from accessing services.	• *Age limit*. We recommend revising the definition of child to mean an individual under the age of 13.

Provision	Requirement	Concerns	Recommendations
	• Regulations for obtaining consent. The manner of obtaining consent will be specified by the DPA, taking into consideration: o volume of personal data processed; o proportion of such data likely to be that of children; o possibility of harm to child due to processing; o and other factors that may be prescribed.		
Transitional provisions	• Effective date. There are no provisions in the Bill specifying the transitional period before it takes effect. • *2018 Bill*. In contrast to the Bill, the 2018 Bill provided several effective dates, including: (1) the Central Government would establish the DPA within 3 months of the notified date, (2) the DPA was required to identify "reasonable purposes" for processing within 12 months of the effective date.	• *Transition period*. The lack of specificity about when the bill would take effect creates significant uncertainty for businesses.	• *Transition period*. We recommend that the Bill not take effect until companies have had sufficient time to ensure they are in compliance with its requirements. For example, a two-year transition period would be consistent with GDPR and would enable companies to design compliance solutions that meaningfully implement the Bill's requirements.
Exemption for processing of data of foreign nationals: Clause 37	• Processing of data of non-Indian persons. The Central Government may exempt certain processing from requirements of the Act, when it	• *Processing of data of non-Indian persons*. This exemption is overly narrow, because it appears to contemplate only case-by-case exceptions determined by the	• *Processing of data of non-Indian persons*. The Bill should provide

Provision	Requirement	Concerns	Recommendations
	involves processing data of non-Indian persons, including by companies incorporated outside of India.	Central Government. Moreover, the process for seeking such an exception is unclear. Without an upfront exemption for such processing, the Bill will create serious concerns, particularly in the context of the localization requirements.	clear exemptions for the processing of foreign nationals' data.
Definition of personal data: Clause 2(28)	• Personal data is defined as data about or relating to a natural person who is "directly or indirectly identifiable," with regard to any characteristic, trait, attribute, or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information and "shall include any inference drawn from such data for the purpose of profiling."	• *Treating inferences as personal data*. By including inferences within the definition of personal data, the Bill meaningfully expands the scope of data covered by data protection laws. Such an expansion is contrary to efforts to ensure that global data privacy regimes are interoperable and creates disincentives for companies seeking to serve the Indian market.	• *Personal data*. We recommend the definition of personal data is revised, to exclude inferences drawn for profiling purposes.
Data portability: Clause 19	• Right to data portability. Data principals have the right to receive the following in a structured, commonly used and machine-readable format, and also have it transferred to another DF: (a) the personal data provided by DF; (b) the data which has been generated in the course of provision of goods/ services by the DF; and	• *Scope*. The scope of the data portability requirement is exceptionally broad, and extends beyond personal data provided by the DF. As a result, it could require DFs to transfer data that is proprietary in nature, offering a competitive advantage to other companies. This concern is exacerbated by the broad definition of personal data, which includes inferences drawn from such data for the purpose of profiling.	• *Scope of right to data portability.* This right should be revised, to extend only to personal data that a data principal has provided to a DF.

Provision	Requirement	Concerns	Recommendations
	(c) the data which forms part of any profile of the data principal or which the DF has otherwise obtained.		
Transparency in processing of personal data: Clause 23 (3)-(5)	• Consent managers. Data principals may give or withdraw, review and manage consent through consent managers through an interoperable platform.	• *Consent managers.* The Bill provides little clarity on how consent managers will operate, creating significant amounts of uncertainty for businesses that must obtain consent from consumers to certain processing. The concept was also introduced without being tested in practice and may cause operational challenges.	• *Consent managers*. We recommend that this concept be removed from the Bill.