# Recommendations on Personal Data Protection Bill - 2019

Date of Submission – 25th February 2020

American Chamber of Commerce in India
PHD House, 4th Floor, 4/2, Siri Institutional Area, August Kranti Marg, New Delhi-110016
Tel: 91-11-26525201 Fax: 91-11-26525203 Email: amcham@amchamindia.com
www.amchamindia.com

| Sl. No. | Area of Challenge | Nature of Issue | Proposed Change |
|---|---|---|---|
| | | **Member 1** | |
| 1 | Clause 2; 37 | An adequate time period to be provided for implementation in the Bill itself. It must be noted that around 2 years' time was provided for the implementation of GDPR. even when the privacy directive was being enforced. In India, the implementation of the privacy regime would be a much-needed fresh start for regulators and for domestic Industry. This bill has cross sectoral impact and will require variety of Industry ranging from Automotive, Retail, Oil& Gas PSUs, Power companies, Health services and many others to learn and comply. | It would discourage the use of India-based service providers because the provisions would cover Personal Data that are originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable privacy laws, and sent to India for processing. It could clash with other privacy legislations. Unless the exact verbiage of the exemption (under section 37) is clear – it will not be possible to assess the impact. Clarity must be sought. |
| 2 | Chapter I- Preliminary<br>Section 2 (20)<br>"harm" includes loss of employment | Indian employment law permits termination on medical grounds in combination with several other factors, that may be considered by employer. | For the purpose of employment, related services / benefits to employee, companies need to process Sensitive personal data including Financial data and Health Data, and such processing, and decisions resulting from such processing, shouldn't come under the definition of "harm".<br>Processing of sensitive personal data necessary for various purposes related to employment (including fraud prevention, immigration, termination of employment, etc) should be a valid ground. |
| 3 | Chapter II - Obligations of Data Fiduciary<br>Section 9 (4)<br>Personal data to be deleted "as specified by regulations" | Regulations should be outcome based. This is all the more important, given the dynamic nature of technology, and therefore regulators prescribing 'manner of deletion' may be counterproductive. | The sections should be modified to clearly state the objectives and should permit the data fiduciary to implement its own systems and procedures, provided the objectives are met.<br>There should be no requirement of DPA approval. |

| Sl. No. | Area of Challenge | Nature of Issue | Proposed Change |
|---|---|---|---|
| 4 | Grounds for processing Sensitive personal data<br>Section 11(3)<br>The consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained…. | While Chapter III recognizes employment as a valid ground of processing personal data without consent, this excludes sensitive personal data.<br>Employee health data is often processed to make available essential services like Insurance, but also process and offer special leave like maternity benefits and other facilitations. Information on health data and other preferences also aids manpower planning. This may include SPD. | We recommend that Chapter III employment purposes as a valid ground for processing should be extended to SPD as well. Therefore clause 13 be modified to be made applicable to SPD as well. |
| 5 | Chapter III Grounds for Processing Personal Data without consent<br>Section 14 (1) and (3)<br>Processing of personal data may be permitted for such reasonable purpose "as may be specified by regulations"<br>Section 15 (2)<br>Additional safeguards may be specified by regulation for processing of sensitive personal data | Having these obligations be subject to regulations, or subject to the approval of the DPA, may be too prescriptive, and discounts the dynamic nature of technology. | Processing should be permitted to protect the legitimate interests of the data subject (it is currently permitted only to process it in case of medical or health emergencies), or the data fiduciary/ processor (unless these legitimate interests are overridden by the fundamental interests of the data subject). |

| Sl. No. | Area of Challenge | Nature of Issue | Proposed Change |
|---|---|---|---|
| 6 | Chapter VI Transparency and Accountability Measures<br>S. 24 (2)<br>Periodic review of security safeguards "as may be specified by regulations"<br>Chapter VIII - Exemptions<br>S 38 (Exemptions for research purposes) | Security safeguards are dynamic. Making these over prescriptive can hinder organization's ability to apply appropriate security safeguards.<br>Exemptions from research purposes only after review by the DPA could stifle innovation. | We propose that broad guidelines be given as to the adequacy of the security safeguards, and organizations be permitted to apply their own technology solutions to these.<br>We propose that such processing for legitimate research purposes be permitted under the Act itself, subject to reasonable safeguards as may be stipulated in the Act. This could include the self-certification by the organization against the conditions in S. 38, or the filing of regular reports by the research organization, specifying how the data is being used, and the kind of research being undertaken. |
| 7 | Chapter VI Transparency and Accountability Measures<br>Section 22 (1) and (2)<br>Privacy by Design Policy<br>- Such a policy should contain business practices and technical systems of the data fiduciary<br>- Such a policy should be certified by the DPA | As technology companies develop products, privacy and security by design are essential features of offerings that offer significant competitive advantage. Disclosures of technical systems that ensure privacy by design could in effect lead to disclosure of trade secrets and confidential information.<br>With significant technical content, there are concerns on how the regulator would certify and the privacy policy. | It is recommended that the requirement of disclosure of technical system details and certification be done away with, as this may lead to disclosure of trade secrets and confidential business information and a complex process for approvals that may lead to delays. The DPA should issue broad guidelines and specify the objectives and should permit data fiduciaries to formulate their own policies, as long as such objectives are met. |

| Sl. No. | Area of Challenge | Nature of Issue | Proposed Change |
|---|---|---|---|
| 8 | Chapter VI Transparency and Accountability Measures<br>Section 24<br>24. (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—<br>(a) use of methods such as de-identification and encryption;<br>(b) steps necessary to protect the integrity of personal data;<br>(c) steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.<br>(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly. | Data processors and data fiduciaries are expected to undertake implementation and review of security safeguards. It appears that there is a joint obligation on the fiduciary and processor to implement 'security safeguards. Often the data processor may not have visibility to the personal data and may not be aware of the particular risks unless informed by the data fiduciary. The data fiduciary is in the best position to understand the benefits and risks of their processing activities and provides instructions to the data processor based on their knowledge of the data subjects, personal data collected and processed, the risks associated with processing. Therefore, contracts should necessarily identify the applicable security safeguards and standards to be adopted by the data processor. | Consistent with an accountability model, we recommend the section be modified to impose the primary responsibility for identification and implementation of applicable standards and safeguards on the data fiduciary.<br>The data fiduciary in turn will be contracting with the data processor for services based upon the data fiduciary'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.<br>Recommendations<br>Section 24 - be modified to reflect that the primary responsibility for the identification of relevant security standards, and safeguards under the law and its implementation is on the Data Fiduciary based upon the Data Fiduciary's assessment of the risks associated with the processing. Data Fiduciary must ensure that these are enshrined in the contract (ref 31(1)) for the Data processor to implement as per instructions. |

| Sl. No. | Area of Challenge | Nature of Issue | Proposed Change |
|---|---|---|---|
| 9 | Chapter VI Transparency and Accountability Measures<br>Section 25<br>Data Breach Notification | It should be clarified that only breaches with a possibility of material harm should be reported. Further, data breaches that are sensitive and could expose technical details of the data processor, and publicizing details of these could also undermine public confidence in the data processor, maybe carefully evaluated before making it public. | t is recommended that Data Breaches should only be reported if they meet a materiality threshold. Sufficient clarity should be provided as to the kind of data breaches that should be reported to the DPA.<br>Details of data breaches may be confidential, and carefully evaluated before making it public if it can expose technical details and undermine public confidence. Further, It must be considered that a failure to comply with this section would lead to stiff fines. |
| 10 | Chapter VI Transparency and Accountability Measures<br>Section 26<br>Significant Data Fiduciary | This should be based on specific sectors (finance, healthcare), and not on factors such as turnover and employee strength.<br>IT companies deal with a variety of clients, and not all projects or engagement have the same risk profile. Therefore, the volume of data being handled and nature of technology deployed will differ from | t is recommended that factors such as turnover and employee strength be deleted. Large employers should not be imposed with additional compliance obligations and penalized for creating employment.<br>Clarity should also be provided that an entity classified as a Significant Data Fiduciary may also act as a processor to entities that are not Significant Data Fiduciaries. In such instances, provisions related to Significant Data Fiduciaries should not apply. |
| 11 | Chapter VII Restriction on Transfer of<br>Personal Data Outside India<br>Section 33<br>(1) Subject to the conditions in subsection<br>(1) of section 34, the<br>sensitive personal data may be transferred outside India, but such<br>sensitive personal data shall continue<br>to be stored in India. | Personal data that is collected by Industry, in many cases, is a mix of both personal and sensitive personal data. Therefore, the mandate to store sensitive personal data (SPD) will data processors in India to either store all data in India or disaggregate the data free of SPD and then transfer the subset abroad. Such data storage practices will not be efficient for businesses. Therefore, the proposed data localization requirements will have the same effect of mandating localization for all data in the medium to long run. | Localization/local storage norms can disrupt businesses, add to cost of compliance and also deprive Indian industry of the cloud economy and its inherent efficiencies, without adding to the ability to offer enhanced privacy and protection of data. We suggest<br>• Data localization requirements should not be enshrined in the Data Protection law. As per needs of specific sectors and Government, Data Protection Authority on the request and in consultation with sectoral regulators as well as stakeholders including Industry notify local data storage requirements. This will ensure there is no blanket localization requirements imposed on personal data, as a rule.<br>• The Data Protection Authority be strengthened to develop and implement strong security safeguards with clear, unambiguous processes for Law Enforcement agency access to data. |

| | | | |
|---|---|---|---|
| | | | • Government to Government dialogue for data sharing and access should be expedited |
| 12 | Chapter VII Restriction on Transfer of Personal Data Outside India Section 33 (2) The critical personal data shall only be processed in India. Explanation.—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data. | There is no clarity on what could be notified as Critical Personal Data. The provisions introduce considerable uncertainty in business for the following reasons If a broad class of personal data is classified as critical personal data, this could lead to stringent data localization norms, thereby disrupting businesses. Globally, we have learnt that the process of recognizing destinations to be adequate for data transfers is time consuming requiring several rounds of Government to Government discussions, that could last for more than a year. Therefore, such time that destinations are recognized as adequate, transfer of critical personal data may be completely prohibited, posing challenges for businesses in India. | The classification of Critical Personal Data be such that it is closely linked to the requirements of National Security. This will limit the impact of stringent localization and also offer certainty to businesses in their data processing activities. Till such time countries / destinations are not recognized as adequate, critical personal data transfers maybe approved basis standard contractual clauses, with additional safeguards. |
| 13 | Chapter VII Restrictions on Transfer of Personal Data Outside India Section 34 (1) (a) Transfers may be done pursuant to intra-group schemes or contracts approved by the DPA | This is overly prescriptive and onerous, and could lead to government scrutiny of commercial contracts, some of which could have confidential technical details. | The Bill should provide for certain mandatory provisions in such contacts, and such contracts and schemes should not be required to seek certification or approval. |
| 14 | Chapter VIII Exemptions Section 37 The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any | The provision for notified exemption for processors dealing with foreign national data is inadequate. In the absence of upfront exemptions, sensitive personal data and critical personal data, being processed in India, will need to be stored in India with provisions for transfer notified as per category (Ref clause 33, 34) Government can access data from both data fiduciaries and data processors, that includes nonpersonal data/ anonymized data (Ref 91). This | The revised draft of the Data Protection bill raises serious concerns on localization requirement, Government access that maybe applicable to Foreign National Data and its consequent impact on the IT sector. Suggestion - Upfront exemptions, for organizations' processing foreign national's data in India, from select provisions, should be considered. This will suitably ring fence the applicability of the law, without any discretionary powers and process uncertainty e.g. exemptions from data localization/storage provisions, Government access to data. This could be |

| | | | |
|---|---|---|---|
| | person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law. | will have a huge impact on business confidence of overseas clients and foreign nationals, as they would be apprehensive of Government of India's access to Foreign national data<br>Process is uncertain. Notification on a case to case basis will disrupt ongoing and upcoming contract finalization and will impact confidence of clients outsourcing data processing to India. | important for India to achieve adequacy status from EU. |
| 15 | Chapter VIII Exemptions<br>S. 40- Sandbox | A clear path forward needs to be provided at the end of the Sandbox/ exemption period, otherwise innovators may be forced to revert to existing laws, negating the purpose of the Sandbox. | One suggestion is to have a mandatory review process, where the DPA will give a recommendation on whether or not any changes to law / rules/ standards are required, as an outcome of the sandbox initiatives. |
| 16 | Chapter IX Data Protection Authority of<br>India<br>S. 50 Codes of Practice<br>50(4) …shall not be issued unless …consultation with sectoral regulators,<br>public… | These may be prescriptive, may reduce flexibility, and could rapidly become outdated with the advent of new technology.<br>Further there is a need for consultations with Industry and Public before any standard, code of practice and rules are notified. While this has been specified for the purpose of code of practice, it should be extended to be a best practise for DPA to adopt. | Codes of practice should be recommendatory and/ or persuasive. Data fiduciaries and data processors should have sufficient flexibility to implement their own systems and practices, as long as the objectives behind the codes of practice are met.<br>It must be noted that a similar approach has been followed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data) Rules 2011, where the Government stated that ISO27001 was one such standard that entities could follow. These Rules stated that personal data was to be protected using managerial, technical, and other measures commensurate with the nature of the data being protected. |
| 17 | Chapter IX Data Protection Authority of<br>India<br>Section: 50(6)(k), 50(6)(l))<br>The code of practice under this Act may include the following matters, namely:—<br>….<br>(k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries | With technological evolution, standards and codes of practices are constantly evolving, with respect to data privacy and security. The Personal Data Protection Bill has given the Authority the responsibility to develop, approve and issue standards/codes of practice for protection of privacy and enforcement of the provisions of the bill. However, there is no flexibility to adopt a new and a better, more appropriate standard specific to a niche technology, that may not have been notified by the authority. This flexibility to demonstrate adherence to better and higher standards has been removed from the | The Data Protection Authority should allow a data fiduciary or data processor to demonstrate before the Authority, or any court, tribunal or statutory body, that it has adopted an equivalent or a higher standard than that stipulated under the relevant code of practice, and therefore will be considered compliant. Such flexibility is important for business innovation and efficiency. |

| | | | |
|---|---|---|---|
| | and data processors under Chapter VI;(l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 24 | Personal data protection Bill 2019 and needs to be reinstated. | |
| 18 | Chapter X, Penalties and Compensation<br>S. 57, Penalties | Given the nature of technology, there may be significant ambiguity around data fiduciaries and processor's obligations under the Act.<br>Hence, a phased approach can be considered where the DPA can build up a body of precedents and jurisprudence, and where lower fines and penalties may be imposed for some time. | The quantum of penalties should be lower at the start, and can be revised in due course, once sufficient clarity has emerged. |
| 19 | Chapter X, Penalties and Compensation<br>S 64(5) & 64(6))<br>(5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same<br>processing activity and are found to have caused harm to the data principal, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to ensure effective and speedy compensation to thedata principal.<br>(6) Where a data fiduciary or a data processor has, in accordance with sub-section<br>(5) paid the entire amount of compensation for the harm suffered by the data principal, such | The bill correctly makes data fiduciary primary liable, recognizing that data processors can only act on behalf of the data fiduciaries (S. 10)<br>However, while penalties and compensation levied on data processors is limited to the processor liability (64(1)) if they act contrary to the instructions of the data fiduciary pursuant or outside of the contract or not incorporated adequate security safeguards, clause 64(6) imposes obligation on the data processor to pay the entire amount of compensation, on behalf of data fiduciary and others.<br>In effect, the bill allows a data processor to be penalized, despite their neither having a full visibility or understanding on why and how personal data was collected, the purpose and objective of such collection, nor any control over the acts or omissions of the data fiduciary or other data processors. | There must be Clear separation of liability of Data Processor from Data Fiduciary<br>• The accountability principle in the bill should be consistently applied to Rules, SOPs and Standards being developed by the Data Protection Authority, Government, Sectoral regulators.<br>• Primary liability to comply with all provisions of the Bill and to pay compensation to Data principal rest with the data fiduciary, and any compensation payable by the processor should be limited to the harm caused due to violation of contractual terms and conditions. |

| | | | |
|---|---|---|---|
| | data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused. | | |
| 20 | Chapter XIII Offences<br>S. 83, non-bailable and cognizable offences | Apprehension of stringent penalties in an uncertain technology environment | Such offences should provide for remedies such as bail, based on the discretion of the court, after considering bona fide deployment of technology.<br>Such offences should also be made compoundable offences. |
| 21 | Chapter XIV Miscellaneous<br>Section 91<br>91(2)<br>The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other nonpersonal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.<br>Explanation. —For the purposes of this subsection, the expression "non-personal data" means the data other than personal data. | Government can access data from both data fiduciaries and data processors, that includes nonpersonal data/ anonymized data<br>Further this clause undermines the existing business practices wherein the data processor is contractually bound by the data fiduciary and cannot share data (personal or non-personal) or any insights thereof, as they belong to the client of the data processor on whose behalf the data processing entity is conducting data processing activities as per instructions and contract. | This will have a huge impact on business confidence of clients and foreign nationals, of data processing companies in India as they would be apprehensive of Government of India's access to data.<br>This clause effectively can bypass the control of the data fiduciary and obligations of data processor under its contract with data fiduciary.<br>The draft bill does not cover non personal data under its ambit, and there is no reason to include this clause in a bill that seeks to protect personal data. There is also a concern that this could lead to disclosure of proprietary data/ trade secrets and other sensitive non-personal data.<br>Further, implications and concerns of the stakeholders should be evaluated carefully, before such requirements are imposed even if it is outside of this data protection bill. |

| MEMBER 2 | | | |
|---|---|---|---|
| 1 | Marketing and advertising | n/a | This will have a huge impact on business confidence of clients and foreign nationals, of data processing companies in India as they would be apprehensive of Government of India's access to data. This clause effectively can bypass the control of the data fiduciary and obligations of data processor under its contract with data fiduciary. The draft bill does not cover non personal data under its ambit, and there is no reason to include this clause in a bill that seeks to protect personal data. There is also a concern that this could lead to disclosure of proprietary data/ trade secrets and other sensitive non-personal data. Further, implications and concerns of the stakeholders should be evaluated carefully, before such requirements are imposed even if it is outside of this data protection bill. |
| 2 | Definitions | n/a | The definitions of personal data and harm are extremely broad and should be narrowed.<br>Definitions of personal data do not commonly include inferences, although depending on the circumstances, these may be linked to an identifiable person.<br>The definition of harm should not include ambiguous or subjective factors, such as "humiliation," "fear of being observed or surveilled," and unexpected observation or surveillance. Similarly, the denial of benefits or services based on an evaluative decision should not *per se* be considered a harm, absent discriminatory intent or similar factors. |
| 3 | Data principal rights | n/a | The right to erasure is extremely broad and should be subject to additional conditions, such as those contained in the GDPR Article 17. It is also unclear why the right to restriction, which appears narrower, is subject to many more conditions. We might suggest that these rights be harmonized and subject to appropriate limitations that allow companies to use personal data with safeguards for product development, fraud detection and prevention, etc.<br>The right to portability should be narrowed to personal data *provided to* the controller. This ensures the control of data principals over their photos, posts, and contacts while reducing compliance costs and the likelihood that data principals will transfer data in ways that advantage platforms that are already dominant. Similarly, industry has not |

| | | | |
|---|---|---|---|
| | | | developed interoperable methods for transferring data from one controller to another, and controllers should not be required to do this. |
| 4 | Audits | n/a | Mandatory annual audits for "significant data fiduciaries" are unnecessary in light of the requirement to conduct data protection impact assessments which must be submitted to the DPA. Such an onerous requirement does not appear to exist elsewhere in data protection law. |
| 5 | Data breach notification | n/a | The applicability of notification requirements to all personal data and the broad definition of harm create ambiguities that are not conducive to proper risk management. Data fiduciaries should be required to notify the DPA of breaches of sensitive personal data, and the definition of harm should be narrowed. The requirement to notify "as soon as possible" should be maintained, rather than converted to a specific period through rulemaking. |
| 6 | Directions | n/a | The DPA's broad capacity to issue "directions" is ambiguous and creates uncertainty. Similarly, the Central Government's power to direct any fiduciary or processor to provide it with any anonymized or non-personal data should be subject to some limitations, as this raises concerns regarding proprietary information. |
| 7 | Financial data | n/a | The classification of financial data as sensitive is appropriate, but it would be ideal to create exceptions for restrictions on the processing of this data in the employment context and in the cross-border transfer of personal data. Consent should not be required in these situations if other safeguards (such as the use of encryption) are used. |
| 8 | Publication of privacy by design policy | n/a | There is ambiguity surrounding this section, which may be resolved by rulemaking, but the mandatory publication of such a policy would provide information to hackers and other wrongdoers that significantly increases the risk of cybercrime. |
| 9 | Rulemaking authority | n/a | It is unnecessary to give the Central Government broad rulemaking authority, when the DPA also appears to have such authority. It creates a more predictable environment to centralize this function in one authority, and the DPA is well placed to do so. |

| | | | |
|---|---|---|---|
| 10 | Penalties | n/a | The fines, injunctive powers, and criminal penalties are extremely punitive. It is not necessary to impose criminal penalties in light of the fines that may be levied. The extension of liability broadly throughout the company is also likely to have a chilling effect and may even disincentivize proper oversight. |
| **MEMBER 3** | | | |
| | GENERAL RECOMMENDATIONS | n/a | Data localization measures: Companies are required to store all sensitive personal data in India, and any transfers of sensitive data outside India would be subject to conditions that are too restrictive. This would largely prevent the implementation of global initiatives involving flow of data cross countries and region. Definition of critical personal data needs more clarity and should be included in the Act itself rather than through a central notification.<br>Cross-Border Transfer Rules: Under Cross-Border transfer of personal data & sensitive personal data, approved clauses / schemes for transfer between the transferor and transferee must be specified within the legislation itself in the form of model clauses. Countries / organizations that meets adequate level of data protection and enforcement mechanism also needs to be specified upfront as done in parallel legislations such as GDPR. Cross-Border transfer of sensitive personal data should be allowed as well subject to compliance with the same conditions.<br>Definition of Health Data: Under the current definition of Health data within the Act, it would be helpful to further clarify the health-related information that would constitute sensitive personal data. This would help ensure that health data are not too widely construed to include information provided by individuals in the context of the purchase of a good or service that is unrelated to the provision of a health service – e.g., their height or weight or the fact they have dry skin. In order to provide such clarification, India may wish to consider a definition such as the following which is drawn from the definitions found in the Australian and Canadian laws: “Health data means: (a) information or opinion about the |

| | | | |
|---|---|---|---|
| | | | physical or mental health of the individual; (b) information collected to provide, or in providing health service provided to the individual; (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;(d) information that is collected in the course of providing health services to the individual; or (e) information that is collected incidentally to the provision of health services to the individual. |
| 1 | Chapter I - 2 | The extra 'territorial scope of the law is too broad as it applies to all Personal data originally collected from residents of foreign jurisdictions and sent to India for processing. | Foreign data should be exempt from application of the Bill. We recommend to amend article 2 A – (c ) (i) as follows:<br><br>'*In connection ~~with any business carried out in India, or~~ any systematic activity ….*'<br><u>Rationale</u><br>Extra territorial scope is today broader than GDPR and would deter foreign companies from outsourcing activities of processing PI in India or would force them to relocate their activities elsewhere. |
| 2 | Chapter I – 3 | Definitions of health data/ critical personal data need to be further clarified | 'Health data': need to clarify further what type of health-related information constitute sensitive personal information. Provide clear definition as to what constitutes critical personal data.<br><u>Rationale</u><br>For Multinational companies, purchase of good or services not related to the strict provision of a health service could be construed as sensitive personal information and subject to restrictions for cross border data flows. |
| 3 | Chapter II – 9 | The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. | The Retention period for data is not clear. The law should clearly classify the data retention period based on personal data, Sensitive personal data and Critical personal data.<br><u>Rationale</u><br>Once the retention period is clear, a standardized approach for collecting / retaining the data for specific period can be followed |

| | | | |
|---|---|---|---|
| 4 | Chapter III-14 | Personal data should be processed without consent for contractual necessity | Collection of personal data Performance of contract must be considered as 'necessary for reasonable purpose'.<br>Rationale<br>Such legal basis is recognized widely and in GDPR, the individual has already consented to the collection as per contract, so no further consent should be required. |
| 5 | Chapter VI-26 | No visibility on the criteria to define significant data | Provide more visibility and precision on the criteria for definition of significant data fiduciary<br>Rationale<br>Companies need to have more visibility on whether they will fall within the definition of significant data fiduciary as this draws further obligations (having an in country DPO/ compulsory registration/ mandatory DPIA). |
| 6 | Chapter VII -33 | Obligation to store one copy of sensitive personal data in India. Data localization requirements/ prohibition on processing certain categories of data outside of India | Remove the condition of the sensitive personal data to be stored in India at all time (article 33 (1));<br>Restrict the definition of critical personal data to be processed only in India to this critical information that can be qualified as sensitive government information ' (military/defense/government data/data that would harm national security)<br>Rationale<br>Such storage requirement would be too onerous for multinational companies as it would prevent any economy of scale and data storage in global CRM database or cloud storage, which would mean for our company revisiting our entire business model for a lot of projects and increasing the costs for customers.<br>Data localization would have a strong negative impact on multinational companies and prevent free flow of data as part of global projects, where business rely on cross border data transfer to provide services to customers based in India and would generally prevent any cloud computing data transfers. |
| 7 | Chapter VII- 34 | Cross -border transfer rules conditions are in addition of obtaining consent | Where transfer is made on the basis of standard contractual clauses, inter affiliated agreements, explicit consent for sensitive data should not be required in addition. Contract and Inter affiliated agreements should NOT be subject to pre-approval by relevant authority. |

| | | | |
|---|---|---|---|
| | | | **Rationale**<br>Data localization would have a strong negative impact on Multinational companies' business as preventing free flow of data as part of global projects, where business rely on cross border data transfer to provide services to customers based in India and would generally prevent any cloud computing data transfers. Explicit consent of the individual should be considered as sufficient basis to allow transfer cross border. Flow of data. |
| 8 | Chapter XIV-91 | Government has the right to direct any company to provide personal data anonymized to target delivery of services by central government | Remove this clause as the central government should not have free access to business intelligence and intellectual property of the company.<br>**Rationale**<br>There is no justification for central government to access data analytics and business intelligence of foreign companies. |
| **MEMBER 4** | | | |
| 1 | Usage of Personal Data | Currently, user has the right to obtain confirmation from the fiduciary on whether their personal data has been processed. | While we recommend that whenever anyone's personal data is used, individual should be immediately informed (automatically |
| 2 | Amendments to other laws | The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data | Currently, compensation payable to individual by companies is withdrawn (refer amendments to other laws). It should be retained and defined. |
| 3 | **Offences** | Offences under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, | There is a separate section for Offense, which will be payable to Government and not to individual whose personal data is used. As mentioned earlier there should be provision of compensation to individuals. |
| 4 | **Consent to use data** | Applicable for all social media intermediaries | We recommend that consent to use (or not use) personal data be taken on periodic basis. Further record of such consent is to be kept for three years for each individual users. |

| | | | |
|---|---|---|---|
| **MEMBER 5** | | | |
| 1 | 'Consent Managers' under the bill | The Personal Data Protection Bill defines 'consent managers' through an explanation under Clause 23(5) as: A "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform. | The role of consent manager is at present ambiguous and clarity is needed on:<br>- Whether there will be multiple consent managers and if yes, how will data fiduciary get into an arrangement with consent manager for obtaining consent of data principal. Further, getting into arrangement with multiple consent managers will increase cost of operation for data fiduciaries.<br>- Whether a consent manager will enable a data principal to communicate with all data fiduciaries with whom it has dealings.<br>**Recommendation**<br>Single consent manager (regulated entity) or a set of managers which a data principal can use for his dealings with it. Alternatively, separate consent management systems for specific industries, much like the account aggregators for the financial industry, must be considered. |
| 2 | **Liabilities of consent managers – Chapter X: PENALTIES AND COMPENSATION** | The Personal Data Protection Bill is unclear on is how liabilities will be determined with the use of consent managers. For instance, who is responsible if communication of consent fails, is incorrectly conveyed, or if there is a data breach at some point? | It needs to be clarified if Chapter X is considered to be applicable to 'consent managers' as well or will there be a need to separately cover them through an agreement between data fiduciary and consent manager. |
| **MEMBER 6** | | | |
| | GENERAL COMMENTS | N/A | Government should define what is "Critical Data" – under the current bill, "Critical Data" needs to be processed only in a server located in India. While the bill defines personal data and sensitive personal data, it has yet not defined what is Critical Data. Many MNCs would find it difficult to implement in absence of this clarity.<br>Recommend that government implements these regulations in phased manner. First time roll out could mean a significant implementation cost and time for some companies – cost of setting up hardware and processes, finding subject matter experts, training |

| | | | |
|---|---|---|---|
| | | | employees that gather data, ensuring that necessary consent has been taken etc. |
| **MEMBER 7** | | | |
| 1 | Section 33(1) | **Data Localization -** Data Localization requirement relaxed for PII Data. However Sensitive PII Data & Critical Data still need to be stored in India. | Recommend removal of Data Localization requirement for Sensitive PII Data (mirroring requirement. |
| 2 | Section 57(1) & 57(2) | **Financial Penalties** The bill provides for financial penalties to the tune of 2-4% of the worldwide turnover. | Penalties to be based on Indian Turnover vs Global Turnover. |
| 3 | Section 34 | **Cross Border Transfer of Data –**<br><br>**Sensitive PII** can be transferred outside of India for processing if the Data principal consents for it and where:<br><br>a) the transfer is made pursuant to a contract or intra group scheme approved by the Authority.<br><br>b) the Central Govt has allowed transfer to certain country or class on entities in a given country<br><br>Central Govt allows transfer of Sensitive PII necessary for a specific purpose. | Consent requirement over and above the other requirement poses a major hurdle for data processors operating cross-border.<br><br>Also, the bill mentions that "Sensitive PII" can be transferred outside of India for processing. This statement is ambiguous as this does not clarify whether we can store Sensitive PII Data outside India post processing. |
| 4 | Section 3(28) | "Personal Data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;"Anonymization" in relation to personal data, means such irreversible process of transforming or | We still recommend including a reasonable link b/w personal data & data principal and not make it so broad. If not, then Cookies, Device Ids, MAID's etc. everything will get included in definition of PII.<br><br>The definition of Anonymization has been amended to include all data which meets the anonymization standard prescribed by the Authority. This will help provide some flexibility on the standard for anonymization. But it would help if these standards are laid down |

| | | | |
|---|---|---|---|
| | | converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority | upfront. Also, the standards should not set a very high bar than needed. |
| 5 | Section 13(1)<br><br>Section 14(1) & (2)<br><br>Section 14(1) & (2) | **<u>Reasonable Purpose -</u>**<br><br>The bill recognizes recruitment & employment as a reasonable purpose for processing PII Data (excluding sensitive PII Data).<br><br>Bill also recognizes processing of PII Data (without consent) for such reasonable purposes as may be specified by regulations.<br><br>Currently the bill provides that "reasonable purpose" may include prevention and detection of fraud, whistleblowing, merger and acquisitions, network information security, credit scoring, recovery of debt, processing of publicly available data and operation of search engines. But these can be used only subject to notification / approval by Authorities. | Considering most of the employee data is sensitive, it is recommended that "reasonable purpose" for the recruitment & employment should cover Sensitive PII as well.<br><br>Would recommend clarifying "reasonable purpose" upfront in the bill vs notifying it later. Also, the current list does not include "contract". Would also recommend adding "contracts" under reasonable purpose. |
| 6 | Section 13 & 14<br><br>Section 3(36) and 93(1) | **<u>Sensitive PII -</u>**<br><br>"Reasonable purpose" cannot be used as a ground for processing Sensitive PII.<br><br>The Bill provides that the DPA would be responsible for identifying new categories of sensitive data. | Reasonable purpose should be allowed to transfer Sensitive PII Data.<br><br>Govt should clarify the list of sensitive PII in the Act itself vs leave it open. |

| | | | |
|---|---|---|---|
| 7 | Section 7 | **Privacy Notice*:***<br><br>The Privacy Notice should be given to Data Principal at the time of collection & should include the following:<br><br>the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable; | The Privacy Notice requirements are extremely onerous. The requirements should be relaxed and limited to the basic details that are necessary for a Data Principal.<br><br>If not possible, at least the requirement on giving details of individuals / entities as listed in (g) should be changed to categories of entities. |
| 8 | Section 3(8)<br><br>16(3) | **Data belonging to Children –**<br><br>The threshold for processing children's data without parental consent is kept at 18 years.<br><br>Mechanisms for verification of age of minors will now be prescribed under the regulations rather than be determined by Data Fiduciaries. | This age of children should be lowered to 13 – 16 years to bring it in line with the threshold set by US and GDPR.<br><br>Also, the new requirement of "mechanism for verification of age of minors" determination should be left with Data Fiduciary as provided in the earlier draft. If not, then the mechanism should be clarified upfront. |
| 9 | Section 26(1) | **Significant Data Fiduciary –**<br><br>The Draft Bill had put a lot of obligations on Significant Data Fiduciaries (Annual Audits, DPIA, appointing resident DPO etc.).<br><br>The authorities to notify the entities that will be covered by Significant Data Fiduciaries later.<br><br>Secondly "volume of personal data processed, turnover of the data fiduciary & new technologies used for data processing" to be considered as a relevant factor for deciding whether a Data Fiduciary is significant or not. | All these requirements/ obligations will put unnecessary burden on companies without providing any additional benefit. Hence this concept should be entirely removed.<br><br>We would recommend defining Significant Data Fiduciary upfront vs notifying it later. Also "volume of data processed, turnover, new technologies used" should not be considered relevant factors for deciding Significant Data Fiduciaries. |
| 10 | Section 30(3) | **Data Protection Officer (DPO) -**<br><br>The bill provides for Significant Data Fiduciary to hire DPO based out of India. | Recommend removal of residency requirement as this not in any way strengthen the protection of data / compliance with the law. |

| | | | |
|---|---|---|---|
| 11 | Section 27(4)) | **Data Protection Impact Assessment –**<br><br>The Draft Bill requires that significant data fiduciaries always submit DPIAs to the Authority for review. | The DPIA should only be reviewed by the internal DPO. The requirement of submitting it to Authorities for review should be removed. |
| 12 | Section 91(2) | **Anonymized Data:** The bill gives power to the Govt to ask Company's to share Anonymized PII data / any other data to enable better targeting of delivery of services or formulation of policies by the Central Government. | This bill is for "PII Data". Hence any clause related to anonymized data should not form part of this bill. |
| 13 | Section 91(2) | **Right to Erasure –** The bill provides data principal the "Right to Erasure" [i.e. Erasure of Personal Data which is no longer necessary for the purpose for which it was processed.] | Would recommend removal of right to erasure especially in light of research / analytics work where we draw conclusions & inferences from PII data because "inference drawn from such data", is now included as PII. And deletion of this data from research studies might not be possible. |
| **MEMBER 8** | | | |
| 1. | Applicability and Scope | **Section2:** Application of Act to processing of personal data.<br><br>**Section 91:** Act to promote framing of policies for digital economy, etc.<br><br>**Section 26:** Classification of data fiduciaries as significant data fiduciaries<br><br>**Section 28:** Maintenance of Records | PDPB provides clarity with regards to its application by focusing on processing of Personal Data and not territorial boundaries. Moreover, anonymized data continues to be out of the purview of PDPB, however an exception has been chalked out for anonymized data, which may need to be shared in order, enable it to better target delivery of services or formulate evidence-based policies. Additionally, significant data fiduciaries *(to be notified by the Data Protection Authority)* would be subjected to a higher compliance threshold such as conducting data protection impact assessments ("DPIA"), appointing a Data Protection Officer ("DPO"), record keeping and submitting to yearly audits. Clarity will be required on who will be a significant data fiduciary for organizations to initiate their compliance activities in a focused and streamlined manner. Furthermore, entities who primarily or solely enable online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services will be termed as *social media intermediaries.* The said entities with a certain high volume of users and ability to impact |

| | | | |
|---|---|---|---|
| | | **Section 29:** Audit of policies and conduct of processing, etc. | electoral democracy, India's security, sovereignty or public order, can be notified by the regulator as a significant data fiduciary (Entities processing high volumes of sensitive data). This will not include intermediaries, which primarily enable commercial or business oriented transactions; provide access to the Internet; in the nature of search-engines, on-line encyclopaedias, e-mail services or online storage services.<br>**Likely investments by organizations would be required to:**<br>□ Identify processing activities in relation to personal data, whether that data relates to an individual or can identify an individual<br><br>□ Understand the purpose and means of data processing activities to ascertain whether one is a data fiduciaries1 or an entity which is only processing data on behalf or another entity and hence, a data processor2<br><br>□ Identify if data processing activities are exempted by law. |
| | | **Section 28:** Maintenance of Records | |
| | | **Section 29:** Audit of policies and conduct of processing, etc.. | Understand if one's data processing activities will classify an entity as a "significant data fiduciary and consequential compliance activities with respect to DPIA, record keeping, appointment of a DPO and any compliance applicable on social media intermediaries. |
| | | **Section 91 (2):** Act to promote framing of policies for digital economy, etc. **(Non-Personal Data)** | Clarity will be required on the verification process for social media intermediaries, form and procedure of conducting audits, whether the requirement to conduct audits is applicable only on significant data fiduciaries or also on data fiduciaries and commercial & reputational disadvantages/advantages of data trust score.<br>**Likely investments by organizations would be required to:**<br>□ Identify the flow of data and the elements therein within all the functions of the entity and isolate the source, flow, transfer, access, retention and disposal in relation to the said data flow<br>□ Understand the different types of data flowing and transacting with the entity such as personal, sensitive, critical and non - personal data.<br>□ Create a data inventory using the identified flow |
| | | **Section 3:** Definitions | |

| | | | |
|---|---|---|---|
| | | **Section 22:** Privacy by Design Policy | ▯ Indulge in some degree of automation with regards to creation of data inventory depending on the scale and size of operations<br>▯ Develop processes to enable third party audits<br>▯ Develop and update internal processes to demonstrate compliance with provisions of PDPB |
| | | **Section 27:** Data Protection Impact Assessment (“DPIA”) | Clarity will be required on the verification process for social media intermediaries, form and procedure of conducting audits, whether the requirement to conduct audits is applicable only on significant data fiduciaries or also on data fiduciaries and commercial & reputational disadvantages/advantages of data trust score. |
| | | **Section 24:** Security Safeguards | **Likely investments by organizations would be required to:**<br>▯ Identify the flow of data and the elements therein within all the functions of the entity and isolate the source, flow, transfer, access, retention and disposal in relation to the said data flow<br>▯ Understand the different types of data flowing and transacting with the entity such as personal, sensitive, critical and non - personal data.<br>▯ Create a data inventory using the identified flow<br>▯ Indulge in some degree of automation with regards to creation of data inventory depending on the scale and size of operations<br>▯ Develop processes to enable third party audits<br>▯ Develop and update internal processes to demonstrate compliance with provisions of PDP |
| | | **Section 30:** Data Protection Officer | Clarification is required regarding this provision w.r.t to any form of compensation or remuneration for such data. Section 91(2) also provides the right of the Central Government to formulate policies for the digital economy so long as such policies do not govern personal data. Hence, the provisions of PDPB has to be read in conjunction with Draft National e-commerce Policy3 considering the interplay of rights and obligations under PDPB and the said Draft Policy, until legislative and judicial clarity is provided. |

| | | | |
|---|---|---|---|
| | | | **Investments by organizations would be required to:**<br>• Understand the various non-personal data elements they process<br>• Develop procedures to respond to directions by the Central Government regarding non-personal data<br><br>The term ***'financial data'*** is narrowly defined under PDPB and may be expanded<br><br>Data fiduciaries will be required to create 'Privacy by Design' policies that may be subjected to certification by the DPA. Once certified, the policies must be published on the data fiduciary's website. These policies should describe business practices and technical systems adopted to protect personal data, strategies to anticipate and avoid 'harm' to individuals, and how individuals' interests are accounted for at every stage of data processing.<br>**Likely investments by organizations would be required to:**<br>• Develop policies on privacy by design<br>• Ensure that obligations under PDPB such as purpose limitation, collection, data quality, data storage etc. are duly reflected in the business procedures and IT systems.<br>• Ensure embedding of privacy features in all aspects of the data lifecycle<br>• Employee commercially accepted or certified technology<br>• Develop procedures to identify risks of harm to data principals and create mitigation strategies<br><br>Clarity is required on what amounts to a 'new technology' and whether the requirement to conduct a DPIA is limited to only significant data fiduciaries or may extend to data fiduciaries as well.<br>**Likely investments by organizations would be required to:**<br>• Develop procedures to understand privacy risks within a business operation so as to identify the triggers of conducting a DPIA<br>• Develop procedures, questionnaires and reporting templates to facilitate DPIA'<br>Organizations will be required to implement security safeguards, including: (i) the use of de-identification and encryption; (ii) steps |

| | | | |
|---|---|---|---|
| | | | necessary to protect the integrity of personal data; and (iii) measures to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data. These safeguards must be implemented taking into account the nature and scope of processing, the risks associated, and the likelihood of harm that may be caused to the data principal and must be reviewed periodically.<br>**Investments by organizations would be required to:**<br>□ Develop procedures to assess and mitigate privacy related risks that the business operations may be prone to<br>□ Adopt techniques such as de-identification, encryption, identity and access management, data loss prevention on need and applicability basis<br>□ Undertake periodic reviews of security controls<br>□ Ensure comprehensive contractual relationships are maintained with third parties.<br><br>Clarity is required on whether DPO is to be appointed by a significant data fiduciary or even data fiduciaries may appoint one.<br>**Likely Investments by organizations would be required to:**<br>□ Understand whether they are significant data fiduciaries or are required to appoint a DPO nevertheless.<br>□ Appoint a DPO as the point of contact for all data related compliance activities and issues<br>□ Ensure that DPO resides in India |
| 2 | Processing of Data | **Section 12:** Grounds for processing of personal data without consent in certain cases<br>**Section 13:** Processing of personal data necessary for purposes related to employment, etc.<br>**Section 14:** Processing of personal data for other reasonable purposes. | PDPB allows personal data and sensitive personal data to be processed in the absence of consent under certain grounds, such as for the performance of certain State functions, for compliance with law or any order of a court, and for prompt action such as responding to medical emergencies, providing assistance during a disaster or breakdown of public order.<br>Additionally, personal data which is not sensitive personal data may be processed by an employer for purposes such as recruitment, termination or assessment of employees, where processing based on consent may not be appropriate. Processing may also be carried out for other reasonable purposes which could be fraud, whistle blowing, |

| | | | |
|---|---|---|---|
| | | | mergers and acquisitions, network and information security, credit scoring recovery of debt, processing of publicly available personal data and the operation of search engines.<br>The said grounds should be specified by a regulation under the aegis of DPA and hence, clarity will be required on whether to avail these grounds or refrain till DPA lists down the grounds explicitly.<br>**Likely Investments by organizations would be required to:**<br>▯ Identify the legal basis for data processing and document the same in policies and procedures<br>▯ Isolate and identify criteria's other than consent before beginning processing activities |
| | | **Section 11:** Consent necessary for processing of personal data<br><br>**Section 23:** Transparency in processing of personal data | Clarity is required on 'consent mangers' and the scale and nature of its probable adoption by organizations.<br>**Likely Investments by organizations would be required to:**<br>▯ Develop consent management procedures<br>▯ Maintain records of consent obtained<br>▯ Ensure that provisions of goods and services or performance of a contract is not conditional on consent<br>▯ Create mechanisms to allow data principals to withdraw or give consent *via* consent managers |
| | | **Section 7: Notice Requirement** | The data fiduciary has to provide notice to the data principal at the time of collection of personal data of the data principal, even if such personal data is not being collected from the data principal directly. This notice must contain (i) the various purposes for which personal data is to be processed; (ii) the nature and categories of personal data being collected; (iii) the identity and contact details of the data fiduciary (including its data trust score, if applicable) and DPO; (iv) the rights of the data principal; (v) information pertaining to sharing, cross-border transfer and retention of personal data; (vi) the procedure for grievance redressal; and (vii) any other information as specified by the regulations.<br>**Likely Investments by organizations would be required to:** |

| | | | |
|---|---|---|---|
| | | | Develop and update privacy notices in line with requirements of PDPB<br><br>Develop procedures and organizational culture around providing transparent and easily comprehensible privacy related information to customers, employees, third parties and regulators |
| | | **Section 16:** Processing or personal data and sensitive personal data of children. | Clarity is required on age verification mechanisms since the same will be stipulated by DPA as part of the regulations and organizations seeking to initiate their compliance activities might face difficulties in streamlining their policies and procedures around data processing and protection.<br>**Investments by organizations would be required to:**<br>Identify data elements flowing within their processes likely to be of children and assess the possibility of harm arising out of such processing activities<br><br>Develop appropriate age verification mechanisms<br><br>Create forms for seeking parental consent |
| | | **Section 17: Right to confirmation and access** | A data principal has the right to request a data fiduciary to confirm if it is processing or has processed his personal data. The data principal can also request the data fiduciary for the personal data being processed or that has been processed, or a brief summary of such personal data, as well as a summary of processing activities undertaken with respect to the personal data and with whom the personal data has been shared.<br>**Likely Investments by organizations would be required to:**<br>Create procedures and policies facilitating individuals to make requests pertaining to confirmation and access of/to personal data.<br>Develop templates to respond to data principal's requests<br>Indulge in automation to address rights of data principals. |

| | | | |
|---|---|---|---|
| | | **Section 18:** Right to correction and erasure | Clarity is required with respect to right to erasure of data since the PDPB now seems to provide for a direct right to seek erasure of irrelevant<br>Personal Data. Hence, data principals now have the ability to require such erasure directly, rather than after adjudication. Therefore, investments might be required to integrate technological tools to enable the right to erasure.<br>**Likely Investments by organizations would be required to:**<br>□ Create policies and procedures to enable right to correction and erasure of personal data<br>□ Develop mechanisms to notify all relevant stakeholders of any change to personal data<br>□ Develop templates to respond to data principals requests<br>□ Adopt technical solution to enable rights of data principals |
| | | **Section 19:** Right to Data Portability | When the processing is carried out by automated means, data principal has the right to receive its personal data in a structured, commonly used and machine-readable format. A data principal also has the right to have such data transferred to any other data fiduciary. This right is however not available where compliance with such request would reveal a trade secret of the transferor data fiduciary or would not be technically feasible, or where processing is required for functions of the State, or in compliance with a law or an order of a court.<br>**Likely Investments by organizations would be required to:**<br>□ Create policies and procedures to enable right to data portability<br>□ Identify personal data that is being processed through only automated means<br>□ Develop a safe channel for transfer of such data<br>□ Develop templates to respond to data principals requests<br>□ Adopt technical solution to enable rights of data principals |

| | | | |
|---|---|---|---|
| | | **Section 20:** Right to be forgotten | A data principal has the right to restrict or prevent continued disclosure of personal data by a data fiduciary, where such disclosure (i) has served the purpose for which it was collected or is no longer necessary for the purpose, (ii) was made on the basis of consent and such consent has since been withdrawn, or (iii) was made contrary to the provisions of PDPB or any other law made by Parliament or any State Legislature. To exercise this right, an application must be made by a data principal to an Adjudicating Officer.<br>Perhaps, the provision needs to be revisited since the user might face administrative challenges whilst exercising this right as it can only be enforced if an order by the adjudicating officer is made in this regard and not by the data fiduciary directly.<br>**Likely Investments by organizations would be required to:**<br>Develop procedures and policies facilitating data principal's right to be forgotten<br>Create mechanisms to notify stakeholders about data principals requesting their right to be forgotten |
| 3 | **Cross-Border Transfer of Data** | **Section 33:** Prohibition on processing of sensitive personal data and critical personal data outside India<br><br>**Section 34:** Conditions for transfer of sensitive personal data and critical personal data. | Critical personal data shall be elaborated<br>**Likely Investments by organizations would be required to:**<br>Identify the location of data and review the retention and disclosure requirements with respect to the said data<br>Create mechanisms to ensure local processing and storage of critical personal data<br>Create mechanisms to ensure local storage of sensitive personal data<br><br>Clarity is required regarding adoption of contractual basis since there seems to be a deviation from the 2018 draft of PDPB which permitted transfers based on standard contractual clauses, in line with frameworks such as the GDPR4. The 2019 draft of PDPB provides for contracts as a basis for transfers and it is unclear as to whether the requirement of approval by DPA will be extended to such contracts since this may raise the compliance cost for organizations who rely on contractual obligations for cross-border transfers.<br>**Likely Investments by organizations would be required to:**<br>Identify processes indulging in cross border transfer of data |

| | | | |
|---|---|---|---|
| | | | Identify the basis under which data will be transferred abroad<br>Create policies and mechanisms to facilitate transfer of data abroad such as consent mechanisms, contracts and intra-group schemes |
| 4 | Breach Notification and Grievance Redressal | **Section 25:** Reporting of personal data breach. | Clarity is required on the timelines for reporting the breach to DPA.<br>**Likely Investments by organizations would be required to:**<br>Develop procedures and mechanisms to notify DPA of a DPA within a reasonable period of time<br>Create templates for notifying DPA of data breaches<br>Review contracts with third parties to ensure indemnity or obligations with respect to data breaches |
| | | **Section 32:** Grievance redressal by data fiduciary | Data fiduciaries are required to put in place a mechanism that allows data principals to have their grievances addressed. Data principals may file a complaint to the DPO (in case it is a significant data fiduciary, or the officer authorised by the data fiduciary for data fiduciaries other than significant data fiduciaries) for any contravention of the PDPB that is likely to cause them harm. These complaints are to be resolved within 30 days. In case this timeline is not met, or if the data principal is not satisfied with the resolution of their complaint, they may file a complaint regarding the same with the DPA.<br>**Likely Investments by organizations would be required to:**<br>Create mechanisms for data principals to raise their grievances<br>Designate officers who will be point of contacts for handling such grievances |

| MEMBER 9 | | | |
|---|---|---|---|
| 1 | **Definition of Personal Data**<br><br>**Chapter 1 Clause 3(28)** | "Personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; | The definition of personal data should be pragmatic and risk-based. It should not include all data that is capable of re-identification by a person or set of persons but data for which a fiduciary or processor is reasonably likely to have and use the means to be able to identify the principal |
| | **Definition of Personal Data Breach**<br><br>**Chapter 1 Clause 3(29** | "Personal data breach" means any unauthorised 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; | The definition of a data breach should include permanent loss of data that may be accessible by third parties but not temporary loss of access to data by data principals. Otherwise, every time a system undergoes maintenance or is offline for other reasons it would constitute a breach. This does not impact privacy. |
| 2 | **Definition of Sensitive Personal Data**<br><br>**Chapter 1 Clause 3(36)** | "sensitive personal data" means such personal data, which may, reveal, berelated to, or constitute—(i) financial data;(ii) health data;(iii) official identifier;(iv) sex life;(v) sexual orientation;(vi) biometric data;(vii) genetic data;(viii) transgender status;(ix) intersex status;(x) caste or tribe;(xi) religious or political belief or affiliation; or(xii) any other data categorised as sensitive personal data under section 15<br><br>Explanation.— For the purposes of this clause, the expressions,—(a) "intersex status" means the condition of a data principal who is—(i) a combination of female or male;(ii) neither wholly female nor wholly male; or(iii) neither female nor male;(b) "transgender status" means the condition of a data principal whos esense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure; | Sensitive personal data should be reserved for categories of data that carry special risks in relation to discrimination and abuse of fundamental rights (3(36) and 15). While it is positive that passwords have been dropped from the list, official identifiers and financial data are regularly processed by fiduciaries and processors and while important, should not qualify for this special category. No other jurisdiction, including the EU has created sensitive status for these categories. |

| | | | |
|---|---|---|---|
| 3 | **Definition of Sensitive Personal Data**<br><br>**Chapter 1 Clause 3(36)** | "sensitive personal data" means such personal data, which may, reveal, berelated to, or constitute—(i) financial data;(ii) health data;(iii) official identifier;(iv) sex life;(v) sexual orientation;(vi) biometric data;(vii) genetic data;(viii) transgender status;(ix) intersex status;(x) caste or tribe;(xi) religious or political belief or affiliation; or(xii) any other data categorised as sensitive personal data under section 15<br><br>Explanation.— For the purposes of this clause, the expressions,—(a) "intersex status" means the condition of a data principal who is—(i) a combination of female or male;(ii) neither wholly female nor wholly male; or(iii) neither female nor male;(b) "transgender status" means the condition of a data principal whosesense of gender does not match with the gender assigned to that data principalat birth, whether or not they have undergone sex reassignment surgery, hormonetherapy, laser therapy, or any other similar medical procedure; | Sensitive personal data should be reserved for categories of data that carry special risks in relation to discrimination and abuse of fundamental rights (3(36) and 15). While it is positive that passwords have been dropped from the list, official identifiers and financial data are regularly processed by fiduciaries and processors and while important, should not qualify for this special category. No other jurisdiction, including the EU has created sensitive status for these categories. |
| 4 | **Limitation on purpose of processing of personal data**<br><br>**Chapter 2 Clause 5(b)** | for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected | Purpose limitation principle requires the data principal to consent to the purposes of processing – which is out of step with the broader array of grounds for processing available in the Bill |
| 5 | **Requirement of notice for collection or processing of personal data**<br><br>**Chapter 2**<br>**Clause 7(g)** | the individuals or entities including other data fiduciaries or data processors,with whom such personal data may be shared, if applicable | Fiduciaries should not be required to provide notice on entities with whom data may be shared as the vendor ecosystem – not just processors but also sub-processors – is fluid and changeable over time. More relevant to the principal is understanding the types of entities with whom their data may be shared – and hence this requirement should be to notify categories of such entities. |
| 6 | **Consent necessary for processing of personal data**<br><br>Chapter 2<br>Clause 11 | The personal data shall not be processed, except on the consent given by thedata principal at the commencement of its processing | Consent has been given primacy in this clause, with all the other grounds essentially being framed as exceptions. It is not helpful to give the impression that consent is the favoured grounds for processing. Necessity for performance of contract should be added to the list of grounds for processing (in line with GDPR) |

| | | | |
|---|---|---|---|
| 7 | **Processing of personal data necessary for purposes related to employment, etc.**<br><br>**Chapter 3**<br>**Clause 13** | Processing of personal data necessary for purposes related to employment, etc | Employment purposes (13) is very useful and recognizes the distinct application of privacy and data protection in that sphere.<br>However, given the broad definition of sensitive data, the limited available grounds for processing is troubling. For example, workplaces often process financial data and official identifiers (e.g. HR) limiting the usefulness of processing for employment purposes in section 13. We recommend narrowing the definition of sensitive data and introducing reasonable and employment purposes for the grounds for processing sensitive data |
| 8 | **Right to data portability**<br><br>**Chapter 3**<br>**Clause 19** | Where the processing has been carried out through automated means, the data principal shall have rights | The data portability right is expansively drafted and should apply only to raw data provided by the individual, as opposed to insights generated during the provision of the |
| 9 | **Privacy by design policy**<br>Chapter 4<br>Clause 22 | Every data fiduciary shall prepare a privacy by design policy | Multinationals tend to take global approaches to accountability measures, enabling them to handle data protection at scale with appropriate quality control and governance. As such, we welcome an objective or principle-based approach to such regulatory provisions – as demonstrated in the privacy by design section. |
| 10 | **Reporting of personal data breach**<br><br>**Chapter 4**<br>**Clause 25 (1)** | Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal | It is important that a filter is established to ensure that only breaches that represent a significant risk are notified to the DPA and individuals to avoid notification fatigue. As such, breaches should be notified to the DPA if there is a real risk of significant material harm to principals and there should be an explicit exemption for data that has been rendered unusable or illegible. |
| 11 | **Reporting of personal data breach**<br>**Chapter 4**<br>**Clause 25 (4)** | Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay | Due to the varying nature and complexity of breaches, it would be preferable not to set an explicit deadline for notification but to require notification "without undue delay". The timeline for notification should only begin when the responsible team within the fiduciary is aware of the breach and has a sense of its general significance – not when the breach occurs. Breaches may be well disguised (e.g. advanced persistent threats) or originate in third parties, such as the data processor. |

| | | | |
|---|---|---|---|
| 12 | **Reporting of personal data breach**<br>**Chapter 4**<br>**Clause 25 (5)** | Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm | Regardless of the DPA's power to determine whether a breach is notifiable to data principals, fiduciaries 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. |
| 13 | **Data protection impact assessment**<br><br>**Chapter 4 Clause 27 (4)** | Upon completion of the data protection impact assessment, the data protection officer appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations | We recommend that DPIAs are kept on record internally and provided to the DPA on request, as opposed to automatically submitted. Companies undertake hundreds of DPIAs and it is not clear what value would be brought by the DPA processing them en masse |
| 14 | **Audit of policies and conduct of processing, etc**<br><br>**Chapter 4**<br>**Clause 29 (1)** | The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act | The DPA should have the power to conduct investigations in the form of data audits, but there should not be a general obligation for fiduciaries to undertake annual audits conducted by registered auditors. This is neither targeted, nor does it reflect that data protection programmes are often managed globally. Results from independent data audits voluntarily conducted by fiduciaries may, of course, be useful documentation to the DPA during investigations |
| 15 | **Data protection officer**<br><br>**Chapter 4**<br>**Clause 30 (1)** | Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out specific functions | For a fiduciary established in India the DPO should not necessarily be located in India. Such roles are often embedded in corporate functions where they can have a clear impact in influencing the business, as well as making sure requirements are embedded in global privacy programmes. |
| 16 | **Prohibition on processing of sensitive personal data and critical personal data outside India.**<br>**Chapter 5**<br>**Clause 33** | Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to bestored in India | While we welcome the deletion of the general requirement to store a copy of personal data in India in the new Bill, the requirement to store sensitive data in India and the limitations on transferring sensitive and critical data outside India are still problematic. They do not serve on their own to improve data protection and severely disrupt operations of both fiduciaries and processors. Requiring explicit consent as a prerequisite to transferring sensitive data is not practicable and is rarely used as a mechanism for transfer of data under the GDPR, where it is presented as one of multiple options rather than a necessary condition. Whereas relying on adequacy decision as the primary mechanism for transfer for critical data puts too much pressure on the Indian government to conclude such agreements and leaves companies without private law mechanisms under which they |
| 17 | **Conditions for transfer of sensitive personal data and critical personal data.**<br>**Chapter 5**<br>**Clause 34** | The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer | |

| | | | |
|---|---|---|---|
| | | | guarantee the data protections. There is also uncertainty as to what will qualify as critical data, given it is not defined in the Bill. |
| 18 | **Conditions for transfer of sensitive personal data and critical personal data.**<br>**Chapter 5 Clause 34** | The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer | To the extent that India chooses to establish data transfer mechanisms, there is scope to leverage existing international mechanisms such as CBPRs (as recognized in the Japanese law) or EU model clauses and BCRs (recognized by Israel) rather than create local versions of such mechanisms.<br><br>Consent and notice requirements are onerous and could apply to employee data collection. It is however unlikely to apply to customers who are mostly in B2B segment.<br><br>Increased movement into telecom services or services ancillary to telecom services could be a concern under data localization norms if critical data definition covers personal information in this context. However, it is noted that telecom regulations already have some stringent provisions not just prohibiting certain kinds of data transfer but even remote access to data from abroad; |
| 19 | **Sandbox for encouraging innovation, etc**<br>**Chapter 5 Clause 40** | The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox | We welcome the new proposal for a regulatory sandbox |
| 20 | **Re-identification and processing of de-identified personal data**<br>**Chapter 13 Clause 82** | Any person who, knowingly or intentionally—(a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or(b) re-identifies and processes such personal data as mentioned in clause (a),without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both | It is inappropriate for the Act to establish criminal offences. To the extent that violations create criminal as opposed to civil liabilities they are better described under more specific areas of the Criminal Code (e.g. fraud or cybercrime). Moreover, to the extent that natural persons are acting in the official capacity of the legal person that employs them, they should not be held personally liable (84). |

| | | | |
|---|---|---|---|
| 21 | **Offences to be cognizable and non-bailable**<br>**Chapter 13Clause 83** | Notwithstanding anything contained in the Code of Criminal Procedure, 1973,an offence punishable under this Act shall be cognizable and non-bailable. | |
| 22 | **Offences by companies.**<br>**Chapter 13**<br>**Clause 84** | Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to,the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. | |
| 23 | **Offences by state**<br>Chapter 13<br>Clause 85 | Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. | |
| 24 | **Act to promote framing of policies for digital economy, etc**<br>**Chapter 13**<br>**Clause 91** | Nothing in this Act shall prevent the Central Government from framing of any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policy do not govern personal data. | The scope of the requirement for any fiduciary or processor to provide any non-personal data to the government to enable targeting of delivery of services or formulation of policies is unclear. At face value, this looks like a broad, compulsory data sharing requirement with the public sector, which could interrupt commercial offerings and potentially compromise trade secrets. |
| 25 | **Power to make regulations**<br>**Chapter 14 Clause 94** | The Authority may, by notification, make regulations consistent with this Act and the rules made there under to carry out the provisions of this Act.<br><br>(2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters | We recommend inclusion of a deadline for responding to requests of (at least) 30 days and an extension period of 30 days to comply, if justified. At the moment, the power to set deadline for complying with requests rests with the Authority |
| 26 | **General comments:** | N/A | - Support for the general approach and distinctions between fiduciaries, processors and principals<br>- Welcome the list of data principals' rights (17 – 20)<br>- Support for the range of different grounds for processing (11 – 14). |

# MEMBER 10

| | | | |
|---|---|---|---|
| 1 | **Localisation of sensitive personal data ("SPD") and critical personal data and restrictions on cross-border data flows:** | **1.** While the Bill does not place any restrictions on cross-border transfers of personal data, it requires the fulfilment of strict pre-conditions for transfers of SPD and critical personal data under Section 33 and 34 of the Bill. The Bill requires SPD to be stored in India and critical personal data to only be processed in India. These restrictions are of concern because of the following reasons:<br>a. Expansive definitions of SPD and critical personal data: The definition of SPD under the Bill includes categories of data that are routinely processed, such as financial data, details relating to caste/tribe and official identifiers. It is unclear if data that can be used to infer SPD (for eg., using a person's home address to infer their financial data) can also be considered SPD. Further, the Bill allows the central government to expand the list of SPD to include additional categories of personal data. Similarly, the central government is granted the power to notify categories of personal data as critical personal data, with no guidance on the kinds of data that could be classified as critical. The broad discretion granted to the central government to determine the scope of critical personal data and to add new categories of SPD creates ambiguity in the meaning of both categories of data. This ambiguity means that data fiduciaries will find it difficult to ascertain when they should seek explicit consent for processing data and implement local storage/ processing. This regulatory uncertainty can in turn affect commercial operations in the country. | ***(a) SPD should be defined in the Bill itself, and this definition should not be changed at the Government's discretion. In this regard, Section 3(36)(xii), section 15 and section 93(2)(a) should be removed in their entirety;***<br><br>***(b) we should remove the category of critical personal data as no comparable legislation globally has such a categorization and the categories of data which may be classified as critical are already subsumed under sensitive personal data;***<br><br>***(c) cross-border transfer of data should be allowed as long as the overall responsibility of protecting data remains with the data fiduciary ("DF");***<br><br>***(d) We recommend that section 33 be deleted in its entirety. In case localization requirements are imposed, additional grounds should be included under the Bill for enabling cross-border flows of SPD. Transfers outside India for 'reasonable purposes', such as mergers and acquisitions and network security, should be permitted. If retained, the revised language for Section 34 should be as follows:***<br><br>*(1) The sensitive personal data may only be transferred outside India for the purpose of processing if the transfer meets any of the following conditions~~, when explicit consent is given by the data principal for such transfer, and where~~*<br><br>*(a) the data principal has given explicit consent for such transfer;*<br>*(b) the transfer is made pursuant to a contract or intra-group scheme ~~approved by the Authority~~ which ~~Provided that such contract or intra-group scheme shall not be approved, unless it~~ makes ~~the~~ provisions for-*<br>*(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person;* |

| | | | |
|---|---|---|---|
| | | b. Negative impact on India's economic growth: India has benefitted immensely from cross-border data flows. The Indian Council for Research on International Economic Relations ("**ICRIER**") has found that a 1% increase in international internet bandwidth leads to an increase of USD 696.71 million in the total volume of goods trade for India. It is clear that data flows will play a big role in helping India achieve its goal of becoming a USD 5 trillion economy by 2024. Restricting cross-border flows of data prevent India from enjoying the benefits associated with free data flows. This is evidenced by a study of the European Centre for International Political Economy, which found that an economy-wide data localisation measure would have caused a GDP loss of 0.8% for India in 2014.<br>c. Data localisation does not enable law enforcement access to data: One of the driving factors behind the introduction of data localisation requirements under the Bill is that localisation will enable increased lawful access to data. However, the mere storage of SPD and critical personal data in India will not lead to control over that data. This fact was recognised by the report of the Srikrishna committee, which found that other countries may assert jurisdiction over data that is physically located in India. Additionally, data localisation does not enable access to encryption keys, without which encrypted data can be rendered incomprehensible. Conversely, the local storage of data is not a pre-requisite for enabling access to data. For instance, India can enter into executive arrangements with countries through laws like the United States' Clarifying Lawful | *and (ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or*<br>*(c) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that- (i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and (ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction:*<br>*Provided that any finding under this section shall be reviewed periodically in such manner as may be prescribed;*<br>*(d) the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose; or*<br>*(e) the transfer is in compliance with a legally binding and enforceable instrument issued from public authorities or bodies; or*<br>*(f) the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures taken at the data principal's request; or*<br>*(g) transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data principal between the data principal and the data fiduciary or another person; or*<br>*(h) the transfer is necessary for important reasons of public interest; or*<br>*(i) the transfer is necessary for the establishment, exercise or defence of legal claims; or*<br>*(j) the transfer is necessary to protect the vital interests of the data principal where their consent cannot be obtained; or*<br>*(k) the transfer is subject to appropriate safeguards such as legally binding instruments, or a relevant law.* |

| | | | |
|---|---|---|---|
| | | Overseas Use of Data ("**CLOUD**") Act. Since the imposition of data localisation does not meet its proposed objectives, better solutions to the problem of lawful access to data should be explored.<br>d. Impact on the health of the internet and healthy competition: By forcing companies to store data within India, data localisation risks isolating the Indian market, creating a fragmented 'Indian' internet. This in turn, will reduce competitiveness and innovation by reducing access to world-class technical infrastructure and emerging technologies. | *Provided that the data fiduciary has taken appropriate steps to ensure that the recipient will protect the personal data to a comparable standard of protection as required under the Act.* |
| 2 | **Expansive right to data portability and introduction of the consent manager framework:** | **2.** Section 21 of the Bill grants individuals the right to data portability, which allows them to receive or transfer personal data provided by them to the DF; data generated in the course of provision of services or use of goods by the DF; and data which forms part of any profile on such individuals. Such categories of data may include confidential/ proprietary information of an organization, and may be protected as a proprietary asset/intellectual property of the DF. This raises the following concerns:<br>a. Wide scope of data under the right to data portability: Under Section 19 of the Bill allows individuals to seek access to a wide range of data that may include business confidential/ proprietary information of an organization. This right is of particular concern since the Bill expands the definition of 'personal data' to expressly include "any inference drawn from… data for the purpose of profiling". A DF may generate data in the form of business insights or aggregated data from personal data by investing significant financial and technical resources. Such data may also qualify as a proprietary asset/intellectual property of the DF. In | ***We recommend that: (a) the scope of data covered under clause 19 should be restricted to only personal data concerning the data principal which the data principal provides to a DF. All other data categories should be removed, i.e. we should only retain Section 19(1)(a)(i) of the Bill;***<br>***(b) the necessity of creating a new class of entities as consent manager should be removed from the Bill. In this regard sections 21, 23 and 94 should be revised in the following manner:***<br><br>*Section 21. (1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary ~~either~~ directly ~~or through a consent manager~~ with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.*<br><br>*Section 23. ~~(3) The data principal may give or withdraw his consent to the data fiduciary through a consent manager.~~*<br><br>*~~(4) Where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.~~* |

| | | | |
|---|---|---|---|
| | | contrast, the EU General Data Protection Regulation ("**GDPR**") restricts the scope of the right to data portability to "*the personal data concerning him or her* (the data principal), *which he or she has provided to a controller*." As per the European Data Protection Board's guidelines on data portability, the data inferred or derived by the DF from the personal data is not required to be provided to the data principal. Similarly, in Philippines, the data portability right extends to only that data which is '*undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject*'. The rationale for such limitations is that the right to data portability should allow ease of transfer when a data principal wishes to switch service providers, and is an extension of an individual's control over the use of her personal information. The right to data portability is not intended to be a means for transferring business' proprietary information.<br>b. <u>Concerns with the consent manager framework</u>: Under Section 23, the Bill introduces a type of entity called 'consent manager', which is a DF that manages the consent given by the data principal for collection and processing of personal data by other DFs. This is an entirely new class of entities that is yet to be tested in the market. Introducing this through a law raises concerns especially since no details are available on their roles, functions and operations in the Bill. Combined with the broad scope of the right to data portability, a consent manager may potentially be used as a mechanism for transfer of proprietary data of a DF to another. While there are parallels drawn | ~~*(5) The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.*~~<br><br>~~*Explanation. —For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.*~~<br><br><u>Section 94</u>. *(1) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act.*<br><br>*(2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely: —*<br><br>*...*<br><br>~~*(h) the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under sub-section (5) of section 23;*~~<br><br>***(c) inferred data should not be included in the scope of the definition of 'personal data'. The definition of 'personal data' has been expanded to expressly include "any inference drawn from… data for the purpose of profiling". Other comparable regimes do not have such wide definitions of personal data, and while inferences drawn from attributes that are traced back to an individual, may be caught in the definition of personal data (even without the express inclusion), an express reference runs the risk of extending the scope of personal data to insights/ commercial information that go beyond the commonly understood meaning of personal data. In this regard Section 2(28) of the Bill should be revised to the following:*** |

| | | | |
|---|---|---|---|
| | | between the account aggregator concept and that of a consent manager, compared to an account aggregator, the consent manager has far wider powers and could potentially cause more damage than we anticipate, given that a consent manager is effectively another intermediary in the chain between the DF and the data principal who has access to all the data of the data principal and can exercise all powers of the data principal in relation to erasure of this information, modification of this information, confirmation and access, etc. A reference may be made to Section 21 of the Bill which bestows these wide powers on the consent manager. | *Section 2(28) "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the <u>physical, physiological, genetic, mental, economic, cultural or social</u> 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~~;* |
| 3 | **Wide powers of the government without sufficient safeguards:** | **3.** The Bill allocates sweeping powers to the central government, without accompanying checks and balances and enables wide government exemptions. This raises the following concerns:<br>a. <u>The regulation of non-personal data goes beyond the scope of the Bill</u>: Under Section 91, the Bill grants the Government the new power to direct companies to provide anonymized personal data and other non-personal data, for the purposes of better targeted delivery of services and creation of evidence-based policies. Non-personal data is defined in very wide terms, as being "*data other than personal data*". However, the Preamble of the Bill limits its scope to the governance of personal data. By allowing the government the power to direct companies to share their non-personal data, the Bill goes beyond this scope. In any case, expanding the scope of the Preamble to allow for the governance of non-personal data does not solve the fundamental | **We recommend that: (a) the Government's power to seek access to non-personal data should be removed from the Bill. In this regard, we recommend deleting section 91, section 2 (B) and section 93(2)(x) of the Bill; (b) the Bill must limit the scope of exemption that can be granted to government agencies from application of the Bill; (c) the Government must be subject to well-defined checks and balances to protect against abuse of power and to ensure regulatory certainty, this includes provision of a clear definition of sensitive personal data in the Bill itself without providing the Government the power to continuously modify this definition.** |

| | | | |
|---|---|---|---|
| | | problem associated with enabling government access to non-personal data, which is that it interferes with the intellectual property rights that companies enjoy over their proprietary information. In the absence of appropriate safeguards, such access also poses serious privacy risks, since aggregated and anonymized data-sets can be used to identify individuals through re-identification techniques.<br>b. <u>The central government's power to notify additional categories of SPD creates regulatory uncertainty and amounts to excessive delegation of power</u>: Under Section 15 of the Bill, the Government has the power to determine the scope of SPD, the Bill creates unnecessary regulatory uncertainty for commercial players, which affects the stability of the Indian economy. Furthermore, it allows the central government and its bureaucracy to take on a policy-making role, which is reserved for the legislature and the elected representatives of the country. It is arguable that this power amounts to an excessive delegation of powers to the government and violates the concept of separation of powers which is a part of the basic structure of the Indian Constitution.<br><u>The government's increased power to select the members of the DPA limits the regulator's independence</u>: The DPA must enjoy regulatory independence in order to discharge its functions objectively and effectively. By allowing the central government to select the members and chairperson of the DPA, the Bill limits this independence. This creates potential for abuse of the DPA's powers and can also interfere with the functioning of the DPA, both of which threaten the privacy of individuals. | |

| | | | |
|---|---|---|---|
| 4 | **DPA to issue codes of practice as regulations:** | Under section 50 of the Bill, the DPA shall specify codes of practice through regulations. Codes of practice are ordinarily intended to be practical guidance tools to aid organizations in implementing good practices and helping with compliance. The Bill equates codes with the law; non-compliance with the codes may attract penalties. This is an overly restrictive approach, against the commonly understood meaning of codes as operational tools. | ***We recommend that codes be developed through the industry and not be framed as prescriptive regulations.*** |
| 5 | **Designation of certain data fiduciaries as significant data fiduciaries** | **4.** Through Section 26 of the Bill, the Bill allows the DPA to designate certain data fiduciaries as 'significant data fiduciaries', on the basis of factors, such as volume of personal data processed, turnover of the DF, and the use of new technologies for processing. There are two concerns with provisions relating to significant DFs:<br>a. A significant DF is required to be registered with the DPA. This is an onerous requirement and will add to the DPA's capacity constraints because of administrative requirements related to registration.<br>Significant DFs have to appoint data protection officers that are based in India. Global DFs that are subject to the requirement of appointing data protection officers under the laws of several jurisdictions, may choose to appoint one officer per region, and will be impacted by this requirement. | ***We recommend the registration requirement be reconsidered, and global DFs be permitted to appoint one officer per region. In this regard, Section 26(3) of the Bill should also be removed.*** |
| 6 | **Reliance on consent and absence of other grounds for processing:** | The Bill places excessive reliance on consent, despite consent being criticized as a basis for legitimizing data processing. There are no grounds or bases that will allow routine data processing activities of DFs. Without other grounds for processing, individuals may receive innumerable privacy notices, resulting in over-notification of individuals and consent fatigue, challenges that were raised by the Srikrishna Committee in its report. While the 'reasonable purposes' ground is an attempt to allow processing for business | ***We recommend that DFs should be allowed to determine what reasonable purposes are, instead of such purposes being specified by the DPA. In this regard, Section 14 of the Bill can be modified in the following manner:***<br><br>*(1) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for ~~such~~ reasonable purposes ~~as may be specified by regulations~~, after taking into consideration-* |

| | | | |
|---|---|---|---|
| | | purposes, the Bill requires the DPA to specify such purposes and fails to serve a meaningful end. | *(a) the interest of the DF in processing for that purpose;*<br><br>*(b) whether the DF can reasonably be expected to obtain the consent of the data principal;*<br><br>*(c) any public interest in processing for that purpose;*<br><br>*(d) the effect of the processing activity on the rights of the data principal; and*<br><br>*(e) the reasonable expectations of the data principal having regard to the context of the processing.*<br><br>*(2) For the purpose of sub-section (1), the expression "reasonable purposes" ~~may~~ shall include, without limitation-*<br><br>*(a) prevention and detection of any unlawful activity including fraud;*<br><br>*(b) whistle blowing;*<br><br>*(c) mergers and acquisitions;*<br><br>*(d) network and information security;*<br><br>*(e) credit scoring;*<br><br>*(f) recovery of debt;*<br><br>*(g) processing of publicly available personal data;*<br><br>*(h) the operation of search engines;*<br><br>*(i) where processing is necessary to protect the vital interests of the data principal or of another natural person;*<br><br>*(j) where processing is necessary for the performance of a contract to which the data principal is party or in order to take steps at the request of the data principal prior to entering into a contract;*<br><br>*(k) processing is necessary for the purposes of the legitimate interests pursued by the data fiduciary or by a third party, except where such* |

| | | | |
|---|---|---|---|
| | | | *interests are overridden by the interests or fundamental rights and freedoms of the data principal which require protection of personal data.;*<br><br>*(l) internally, in a lawful manner that is compatible with the context in which the personal data was collected.* |
| 7 | **No indicative timelines for compliance:** | The Bill does not indicate any timelines for complying with the Bill, which can cause uncertainty for businesses. | ***Bearing in mind the onerous compliance obligations under the Bill, we recommend that organizations should be allowed sufficient time for compliance.*** |
| 8 | **No requirement for notice to an organization when initiating an inquiry into its practices** | Under the draft bill recommended by the Justice Srikrishna Committee in July 2018 ("**2018 Bill**"), investigative officers could only undertake an inquiry after providing a written notice to the persons subject to the inquiry stating the reasons for the inquiry and the relationship between the DF and the scope of the inquiry. This requirement appears to have been deleted from the 2019 Bill. The removal of this requirement means that if an organization is subject to an inquiry by an investigating officer under the Bill, it will not receive a notice before the commencement of such inquiry. Thus, an entity may not have visibility over any inquiry into its activities undertaken by the DPA until such time as the DPA demands certain information or documents in furtherance of the inquiry. | ***We recommend that investigating officers should only undertake an inquiry after providing a written notice to the persons subject to the enquiry.*** |
| 9 | **Restrictive data retention provisions** | Under Section 9 of the Bill, a DF is not permitted to retain personal data beyond the period necessary to satisfy the purpose of processing and shall delete the personal data at the end of the processing. This is stricter than the 2018 Bill, which allowed DFs to retain personal data only till it is 'reasonably necessary' to fulfil the purpose of processing. A blanket restriction on retention may not be feasible to | **We recommend that the Bill revert to the provisions in the 2018 Bill in this regard.** |

| | | | |
|---|---|---|---|
| | | implement. The threshold of 'reasonably necessary' in the 2018 Bill may have addressed that concern. A strict restriction on retention, as is the case in the Bill, may result in a technical violation of the law. | |
| **MEMBER 11** | | | |
| 1 | Section 13 | N/A | 13(1) Notwithstanding anything contained in section 11 and subject to sub-section (2), any personal data including ~~not being any~~ sensitive personal data such as biometrics and financial data, may be processed, if such processing is necessary for—<br><br>(a) recruitment or termination of employment of a data principal by the data fiduciary;<br><br>(b) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary;<br><br>(c) verifying the attendance of the data principal who is an employee of the data fiduciary;<br><br>or (d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.<br><br>(2) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under the said sub-section. |
| 2 | **N/A** | N/A | Privacy by design policy should be left to the wisdom of the data fiduciary based the framework provided by the Authority subject to filing of a declaration by the Data Fiduciary. Suggested additions and deletions this section are as under in blue font: |

| | | | |
|---|---|---|---|
| | | | 22. (1) Every data fiduciary shall prepare **a privacy by design policy,** containing—<br><br>(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;<br><br>(b) the obligations of data fiduciaries;<br><br>(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;<br><br>(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;<br><br>(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;<br><br>(f) the processing of personal data in a transparent manner; and<br><br>(g) the interest of the data principal is accounted for at every stage of processing of personal data.<br><br>(2) Subject to the regulations made by the Authority, the data fiduciary may submit a declaration that its privacy by design policy prepared under sub-section (1) to the Authority is compliant with the requirements as ~~for certification within such period and in such manner as may be~~ specified by regulations.<br><br>~~(3) The Authority, or an officer authorized by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).~~<br><br>(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary ~~and the Authority~~. |

| | | | |
|---|---|---|---|
| 3 | Section 23 | N/A | Consent Manager specified in Section 23 requires more clarity whether it is the data fiduciary, who is processing the data or an independent third party data fiduciary. The registration provisions for the data fiduciary who is processing personal data as Consent Manager would be onerous.<br><br>It is suggested that Section 23(5) shall be deleted as compliance under the other provisions of this section is necessary for a consent manager. Changes are given below in red font:<br><br>23(5) ~~The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.~~ |
| 4 | Section 25 | N/A | 25. (1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.<br><br>(2) The notice referred to in sub-section (1) shall include the following particulars, namely:—<br><br>(a) nature of personal data which is the subject-matter of the breach;<br><br>(b) number of data principals affected by the breach;<br><br>(c) possible consequences of the breach; and<br><br>(d) action being taken by the data fiduciary to remedy the breach subject to technical feasibility.<br><br>(3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within reasonable ~~such~~ period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. |

| | | | |
|---|---|---|---|
| | | | (4) Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.<br><br>(5) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.<br><br>(6) The Authority may, in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section<br><br>(5), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.<br><br>(7) The Authority may, in addition, also post the details of the personal data breach on its website. |
| 5 | Section 57 | | Penalties under Section 57 are punitive and requires to be rationalized generally. Penalty for the first time non-compliance related to a data security breaches, which are inflicted by third parties ( such as introduction of a virus in the system or hacking). |
| 6 | Section 33(1) | | 92. No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law including this Act. |

| | | | |
|---|---|---|---|
| **MEMBER 12** | | | |
| 1 | **General Observations** | N/A | 1. The Draft Bill defines 'financial information' as 'sensitive personal data' and lays down requirements of storing one set of the data locally in India. Further, the government has the authority to define 'critical data' at a later date and which data cannot be transferred to any data system outside India. These restriction would critically impact the operations of MNCs and impose huge costs of compliance.<br>2. The Draft Bill also proposes criminal penalties including imprisonment for non-compliance. Even under the GDPR regime, no criminal penalties are imposed.<br>3. The Draft Bill also does not lay down the legal regime completely and the same remains to be evolved by the Data Protection Authority of India ("**DPA**") creating ambiguity and uncertainty.<br>4. The data localization requirement could be a huge burden, and is the provision of most concern.<br>5. The lack of a legitimate interest purpose could be make it difficult to justify processing in some cases, unless reasonable purpose is interpreted similarly<br>6. The Fiduciary standard could also be a burden if it sets a significantly higher bar for controllers. |
| **MEMBER 13** | | | |
| 1 | **General Observations** | | 1. The definitions of Sensitive personal data, health data and critical personal data should be detailed to avoid any ambiguity.<br>2. Data retention guidance should be shared or aligned with other applicable laws<br>3. If a contract between two parties exist which talks about consent and purpose for data processing, additional consent may not be required<br>4. The necessary rules or clarifications are required for format of consent, other documents like model contracts, clauses etc. Uniformity needs to be ensured to avoid confusion. |

| | | | |
|---|---|---|---|
| | | | 5. Companies need to have more visibility on whether they will fall within the definition of significant data fiduciary as this draws further obligations and costs (having an in country DPO/ compulsory registration/ mandatory DPIA)<br>6. Government rights to access personal data are vast and they should be curtailed with detailed procedures enforced by law<br>7. Transition to new law should be thought through and done in phased manner. Adequate time and resources (in terms of clarifications and standardization) shall be provided to industry to comply<br>8. Penalties prescribed must be graded /compounding provisions should exist |
| **MEMBER 14** | | | |
| 1 | Clause 2; 37 | | It would discourage the use of India-based service providers because the provisions would cover Personal Data that are originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable privacy laws, and sent to India for processing.<br><br>It could clash with other privacy legislations. Unless the exact verbiage of the exemption (under section 37) is clear – it will not be possible to assess the impact.<br><br>**Clarity must be sought.** |
| 2 | CHAPTER II, 4, 5, 11,<br><br>Chapter III 12, 13, 14 | | Grounds for Processing Personal Data (without consent) do not include the **performance of a contract** nor **legitimate interest** (other than "reasonable purposes"), which may constitute a significant burden to Data Fiduciaries -<br><br>We recommend including *performance of a contract* and *legitimate interest* as a ground for processing personal data.<br><br>Additionally, it could be considered if the 'reasonable purposes' ground could be reconfigured to allow a data fiduciary to balance the considerations in Section 14 |

| | | | |
|---|---|---|---|
| | | | with the proposed processing to determine if there is a 'reasonable purpose' rather than requiring regulations. |
| 3 | **N/A** | N/A | Many provisions are with the government or the DPA e.g. to determine which entities are “significant data fiduciaries”; notify certain categories of personal data as “critical personal data” that can only be processed in India or “sensitive personal data”; make adequacy determinations about cross border transfers; and exempt any agency of the Government from the provisions of the Bill.<br><br>Heavy reliance has been put on delegated legislations and future rules. **Clarity must be sought**. |
| 4 | Clause 91 | N/A | This provision potentially gives the government the right to access business intelligence and intellectual property of companies for its own "planning" and "development" purposes.<br><br>The possibility of allowing government access to non-personal data needs more granularity and guidance - will this become a burden to organisations if it'll mean anonymizing all data? Or even increase the complexity of organization's data management systems? Will this also entail a subsequent need for more security measures with regards to non-personal data?<br><br>Under section 91 the government can direct the data fiduciary or a data processor to provide any personal data anonymized or other non-personal data. This could potentially expose the client data which is being processed by an Indian service provider as a ‘data processor’.<br><br>**Clarity must be sought** about the extent of this provision. |

| | | | |
|---|---|---|---|
| 5 | Clause 33 – 36 | N/A | What will happen in the case of an international company when using an Indian data processor for the processing of personal data of non-Indian citizens - is it necessary to keep a local copy?<br><br>**Clarity must be sought** since this could potentially breach other data privacy laws (for examples, principles of data minimization). |
| 6 | Clause 22 | N/A | Privacy by Design Policies may be submitted to DPA for certification. The Bill notes this is **voluntary**. The benefit of certification is that the Fiduciary will have a policy that is 'signed-off' as compliant by the DPA. If certified, the policy will be published on the DPA's website (as well as the Fiduciaries' website) > **still unclear how this will operate in practice, clarity must be sought.** |
| 7 | CHAPTER X | N/A | Criminal liability and imprisonment are excessive consequences, which should not be addressed in a privacy law, but rather regulated in criminal codes and for intended violations of the law such as cybercrime or fraud. Like other matured geographies with respect to data privacy legislations – PDP should also confine to civil penalties. |
| **MEMBER 15** | | | |
| 1 | Section 3(28) & Section 19 | Broad scope of definition of personal data and the issue of data portability | The definition of personal data in the 2019 Bill is a more expansive one than the 2018 Bill and includes "any inference drawn from such data for the purpose of profiling." This inclusion appears to widen the definition of personal data to include data about or relating to a natural person who is not directly or indirectly identifiable through it. This would have implications for the processing activities of data fiduciaries in relation to inferred data (in terms of needing valid consent/ explicit consent from the data principals before processing such inferred data as well). Other regulatory frameworks such as the GDPR and the California Consumer Privacy Act (CCPA) do not include derived and inferred data and limit the requirements of their respective data protection legislations to provided and observed data. Further, the definition of what constitutes personal data also impacts what data can be portable. Since inferred and derived data could involve considerable proprietary resources, making this type of data portable would also raise issues of intellectual property rights infringement. Therefore, we would urge the JSC to issue a clarification that personal data extends only to user- |

| | | | |
|---|---|---|---|
| | | | provided and observed data and also limit the scope of portability to encourage industry set interoperability standards. |
| 2 | Section 3(8) | Age of child under 18 years to be reconsidered and reduced | Designating under 18 as the age at which an individual will be considered a child is much higher than international norms and will inevitably create barriers to individuals accessing services in their own capacity as they mature. International jurisprudence sets varying ages for a child, for instance the GDPR sets the age as 16 with a capacity for countries to set a lower age depending on their domestic experiences; Belgium and Denmark set a child's age at 13 years; Bulgaria 14 years. The UK's Information Commissioner's Office recognises children of 13 years and above as capable of giving a valid consent for lawfully processing a child's personal data. 1 |
| 3 | Section 91 | Sharing of non-personal data | Under the 2019 Bill, the Central Government has been given unfettered powers to direct a company to share with it anonymised or non-personal data if so required, to better target policies and services made available by the State. This is problematic for many reasons: first, under the 2019 Bill, non-personal data also refers to anonymised data. To anonymise data, companies would need to invest significant resources in terms of data analytics tools, etc., making this anonymised data their private property. By empowering the government to use this data is tantamount to letting the government appropriate private property, which has continued to be a controversial subject, especially since it is an absolute power, without any safeguards built in. Further, businesses have a legitimate copyright interest in processed datasets comprising of non personal data. Such processed datasets are likely to pass the test of 'originality' and be copyright-protected as 'literary works'. Thus, any direction that mandates sharing such protected datasets with the Government is likely to violate copyright protections as well as proprietary economic rights vested in businesses. We would suggest that such a vast power should not be available to the State without adequate checks and balances and merits re-examined. Ideally, it should be taken out of the scope of a legislation dealing with personal data protection and form part of a separate policy. |

| | | | |
|---|---|---|---|
| 4 | Section 3(36) and Section 15 | Caution to be exercised on further categorisation of Sensitive Personal Data | While the designation of categories of personal data requiring more rigorous protections is welcome, however there may be some practical challenges in the context of financial data and official identifiers that are considered sensitive personal data requiring explicit consent. Financial data will require consent from the user each time the user is providing financial information to complete a transaction and potentially cause them not to appropriately consider consent, leading to consent fatigue. Additionally, in the case of official identifiers which may be provided in a range of situations such as employment, collection of explicit consent may not be appropriate. Furthermore, the ability under Section 15 to designate further categories of sensitive personal data creates considerable uncertainty for data fiduciaries who would have to amend processes for collection personal information depending on such designations. |
| 5 | Section 7 | Long notice requirement for processing personal data | The requirement of notice for collection or processing of personal data enlists a number of items(14) that will result in lengthy Privacy Notices with legalese and will increase the complexity for a data principal. Moreover, if a consumer is provided with too much information at the same time, he may be unable to comprehend the complete implications of the data collection process. It needs to be taken into account that users spend limited time on screens, thus information needs to be as clear and concise as possible and in a form that they will digest. For instance, graphical representations or short videos may be one examples of facile means to conveying information. |
| 6 | Section 8(3) | Burden on data fiduciary to check quality of personal data processed by third party | The requirement to notify individuals/entities if a third party to whom the personal data is (validly) disclosed does not comply with the data quality requirements, imposes an untenable burden on data fiduciaries to monitor the compliance levels of third parties. Further, repeated notifications are likely to lead to notice fatigue in individuals, who may not be concerned with relatively minor diversions. |

## About American Chamber of Commerce in India

The American Chamber of Commerce in India (AMCHAM – India) is an association of American business organizations operating in India. AMCHAM – India is a member to the Chamber of Commerce of USA, Washington DC, U.S.A. (COCUSA) and the AmChams of Asia Pacific. Established in 1992, AMCHAM has over 400 U.S. companies as members. The incumbent U.S. Ambassador to India is the Honorary President of AMCHAM. AMCHAM enjoys a very close relationship with the U.S. Embassy and complete support in fulfilling its objectives.

AMCHAM's principal objectives are:

a) Promote activities that would encourage and stimulate investment by U.S. companies in India

b) Support ongoing business operations of its members

c) Encourage bilateral trade between the U.S. and India

AMCHAM fulfils these objectives in a variety of ways, such as:

Providing a forum on an organized basis in which American business organizations in India can discuss and identify common issues and interests regarding their economic and commercial interests in India and/or the United States.

Providing opportunities to members to represent and express their views and opinions, especially regarding trade, commerce, finance, services, industry, agriculture and related issues and to seek to understand and give effect to such opinions to the extent considered desirable and possible.

Maintaining Sectoral Committees to implement the primary objectives of these committees.

Undertake advocacy on policies and procedures affecting AMCHAM members' operations in specific sectors as well as affecting the growth of foreign direct investment in India.

**Secretariat:**

**Mrs Ranjana Khanna**
DG and CEO
Email: ranjana.khanna@amchamindia.com
**Ms. Ishita Sengupta**
Program Director
Email: ishita.sengupta@amchamindia.com