25 February 2020

To the
Joint Select Committee ("JSC")
Director, Lok Sabha Secretariat,
Room No. 014 Ground Floor,
Parliament House Annexe, New Delhi- 110001

Subject: AIC Comments and Recommendations on India's Personal Data Protection Bill, 2019

The Asia Internet Coalition ("**AIC**") and its members express our sincere gratitude to the Government of India for the opportunity to submit comments on India's Personal Data Protection Bill, 2019 - **Bill No. 373 of 2019** ("**DP Bill**"). AIC is an industry association that represents leading global internet companies on matters of public policy. To further its mission of fostering innovation, promoting economic growth, and empowering people through the free and open internet, AIC would like to present our comments on the Personal Data Protection Bill, 2019 to the Joint Select Committee ("**JSC**").

In the backdrop of digitalization and growth of digital services across the world, the role of data has become more and more significant. This has given rise to concerns of informational privacy and the exercise of rights over personal data. Without a framework to govern these two subjects, no digital industry can be sustainable. In this context, the Personal Data Protection Bill, 2019 ("**DP Bill**") is a much-needed effort and parallels the global movement towards data protection legislations.

Although we appreciate the Indian government's efforts towards developing the DP Bill, we believe that there are concerns regarding its provisions, aspects of which contradict the draft Personal Data Protection Bill, 2018 published by the expert committee headed by Justice Srikrishna ("**2018 Bill**"), the *Puttaswamy* judgment of the Supreme Court of India as well as other international frameworks such as the EU GDPR.

We strongly recommend that the DP Bill should have more parity with the EU GDPR, on the grounds that standardization of national data protection regime will help improve compliance and improve business environment for SMEs and startups. Parity with GDPR on issues like the definition of personal data, data portability, the right to be forgotten, and the extraterritorial application of the new law, should be strongly considered by the Government of India.

In this regard, we are grateful to be able to present our concerns on the same, and would also like to re-state our continuous support and assistance to the Indian government in its efforts to bring about this transformational change in the privacy landscape in India.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

THE SUBMISSION IS DIVIDED INTO THE FOLLOWING PARTS

Table of Contents

A. Key Concerns – Deviation from the 2018 Bill

1. Timelines for implementation and enforcement

Clear timelines help create political will and industry preparedness to implement a data protection regime. In a significant departure from the Committee's draft Bill, the Bill does not specify timelines for the implementation of its provisions and leaves it to the Government to notify the dates on which different provisions may come into effect. This would create a great deal of uncertainty regarding the manner in which the Bill, if enacted, would come into effect and would severely impact businesses ability to transition to a compliant ecosystem. It is relevant to note that for similar onerous obligations upon data fiduciaries and data processors, other international data protection regimes (like GDPR & CCPA) indicated intimated the effective date to relevant stakeholders for better preparedness (e.g., GDPR set compliance deadline after a buffer of 2 years for GDPR preparedness).

Recommendations
Therefore, we recommend that the Bill should specify a minimum date/timeline for implementation and enforcement of the provisions. In the minimum the timelines provided under Chapter XIV (Transitional Provisions) of the draft Bill should be reinstated, with scope to extend it further after consultations with other stakeholders. This would also enable businesses and startups to better prepare for compliance with the Bill, including many necessary technical, operational and managerial requirements.

2. Definition of personal data and data portability

The definition of personal data has been expanded to include inferences drawn from personal data for the purpose of profiling. The inclusion of inferred data within the scope of personal data will expand the scope of data that is covered under the ambit of the law. Given that de-identified data already qualifies as personal data (unless it has been irreversibly anonymized), the expanded scope of personal data will ensure that de-identified inferred data will be part of the protections extending to personal data under the DP Bill. It is very likely that a great quantity of proprietary data may fall within the ambit of the law.

Similarly, the right to data portability provides data principals the right to port:

- data generated by the data fiduciary in the course of provision of services, and
- data inferred by the data fiduciary to form part of the profile of the data principal.

The data inferred by any data fiduciary is likely to form part of the business model of any entity and the data generated through an entity's proprietary software and algorithms is likely to be protected under copyright laws.

Recommendations

Given the drawbacks of the expanded definition of "personal data", we recommend the retention of "personal data" as contained in the 2018 Bill. With respect to the right to data portability, we recommend that:

- Users should be given the right to access their data (given/collected) and delete all their data (given/collected/inferred) rather than porting it because of the compliance burden.
- Data Portability should first be discussed as a concept. Data fiduciaries instead of mandating data portability in time can come up with voluntary standards. . Data portability as a concept is borne from market demand, and as consumers seek to port their data, entities will develop standards to meet this demand. With the introduction of consent managers in the DP Bill, data fiduciaries will need to coordinate and agree on industry practices over many aspects of consent collection and storage of personal data.

3. Right to be forgotten

The right to be forgotten under the DP Bill includes the right against "continuing disclosure". The inclusion of this term creates ambiguity surrounding this right, as it is unclear whether it applies only for those services that engage in user-initiated disclosure of personal data or if it is for data generated over the course of processing. Once the DP Bill comes into effect, an individual whose personal data appears on internet searches will be able to apply to an Adjudicating Officer for an order calling on 1 (one) or more search engines to remove such personal data from the public domain provided the conditions stipulated under section 27 are complied with, i.e., it can be shown that continuing disclosure of such personal data is no longer necessary or has served the purpose for which it was made.

Further, the balance of interest between such removal and the right to freedom of speech and expression and the right to information of any other citizen, must be weighed in favour of such individuals whose personal data is being removed. However, such individuals will not be entitled to seek erasure of such personal data and such personal data may remain etched on servers and other storage spaces. Personal data held in myriad other ways can also be restricted from further disclosure under the aforementioned section 27. Thus, the right to forget can be used to compel an employer to not disclose information pertaining to an ex-employee if it can be shown that such information, say a past act of indiscipline, is no longer relevant or pertinent.

There is a mixed kind of opinion over deletion of personal data under 'Right to be Forgotten'. Justice Sanjay Kishan Kaul in the case of *Justice K.S. Puttaswamy (Retd.) & Anr. v/s Union of India & Ors.*, which is also known as 'Right to Privacy Judgment' said that if India is to recognize 'Right to be Forgotten' on the verge of GDPR, it cannot be an absolute right. Such right cannot be exercised if the personal data is needed for the purpose of public interest, compliance with any legal obligation, national security, scientific and historical research etc. These conditions are exceptions to the right to privacy, including data privacy. Even the Data Protection Committee Report states that removing the information available to the public at large would infringe the individual's right to know as well as freedom of press. Granting such absolute right may affect the public realm of information if the information is totally removed. Such right may also involve the deletion of information from private storage which might create a hurdle in publishing the information later on.

Recommendations
Therefore, there must be a distinction between the deletion of information and restriction over disclosure of information and only the later one is possible to grant to an individual. We recommend that corporate obligation be limited to restricting continuing disclosure within its control. However, such obligation should not be expanded the way it did in Europe with the right to be forgotten to cover any instance on the internet. We therefore recommend that the nature and scope of the right to be forgotten, including the enforcement measures, be discussed and subsequently specified in the DP Bill.

4. Provisions relating to the sharing of non-personal and anonymized data

The Bill states that the government may, in consultation with the DPA, direct any data fiduciary or data processor to provide any personal data that is anonymised as per the standards prescribed by the DPA, or any other non-personal data (NPD) for certain purposes.

However, the Bill itself states that it shall not apply to the processing of anonymised data. Since the Bill covers only personal data and specifically excludes anonymised data from its scope, the inclusion of any provisions relating to NPD would create internal inconsistencies in the Bill and result in confusion.

Moreover, the power of the government to compel data fiduciaries and data processors to provide data is unreasonable. The Bill practically empowers the government to direct a business to dedicate additional resources to create anonymised data sets, which may not have been in existence, solely for the use of the government. A directive of such nature will negatively impact ease of doing business in India. Additionally, the Bill does not clarify the standards of anonymisation to be employed by a data fiduciary or data processor when it provides such data. It also does not clarify other conditions like the payment terms, contractual obligations, technical safeguards, etc.

4.1. Loss of competitive advantage for Indian firms

The anonymised or NPD, which is subject to a forced data sharing provision in the Bill, could be proprietary, confidential and critical to business interests. It seems to ignore the fact that substantial effort is required to make data useful. Businesses use complex processes to make data useful, including careful selection, assembly, anonymisation and execution of large data sets. The intellectual property rights regime, both domestic and international, legally protects such works. The provision on mandatory data sharing in the Bill could significantly impact the ability of Indian firms to compete in global markets, especially since global data frameworks do not contain a similar mandate. This may also discourage foreign investment in India, and consequently limit the types of products and services available in the Indian market for consumers.

4.2. Regulation of non-personal data is premature

The Bill states that the DPA will specify the anonymisation standards at a later date, once the Bill is passed. However, until such anonymisation standards are prescribed, there is no clarity as to what would qualify as anonymised data for the purpose of this provision.

Further, the definition of 'non-personal data' in the Bill lacks clarity. It is currently defined as 'data other than personal data'. However, data has been very broadly defined as a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing. Clubbing multiple types of data into a single group, without any parameters for classification, could result in the regulation of diverse categories of data types as if it were homogenous. It also does not account for mixed datasets, i.e. data sets that are composed of both personal and non-personal data, which are often inseparable. Therefore, imposing any obligations around NPD would increase business uncertainty and risk, which would impact the growth of the digital economy.
Additionally, some information may appear to be non-personal when considered in the context of a single individual, but could reveal private or sensitive information about groups of people. For example, if a service provider were required to share traffic data, they might reveal information about travel patterns in certain neighborhoods that could create privacy issues for that population. Due to the novelty of this provision, the risks and corresponding mitigations of this type of data sharing requirement are not already identified in privacy law or research. Until those protocols are developed, any requirements to share non personal data should be voluntary and undertaken in good faith by both parties in order to minimize risks and ensure that the public sees a benefit to these sharing programs.

Further, a separate government-appointed Committee of Experts under Kris Gopalakrishnan is currently engaged in deliberations around the issue of NPD. Given these developments, any provisions in the Bill concerning anonymised data or NPD are premature.

Therefore, we recommend that any proposed framework for anonymised data or NPD should be considered only after:

i. the Bill has been passed;
ii. the DPA has issued appropriate standards, rules and regulations (eg. on anonymisation);
iii. the NPD Committee has concluded its deliberations and published its recommendations after inviting comments from all relevant stakeholders, including from the public.

4.3. The use-cases are not clear and lack safeguards

The Bill empowers the government to seek anonymised data or non-personal data from businesses to enable (1) better targeting of delivery of services; or (2) for the formulation of evidence-based policies by the Central Government.

Firstly, the expert committee which prepared the Draft Bill did not recommend any provision of this nature. It is unclear how either use-case serves the objectives of the Bill, i.e. to protect the privacy of individuals relating to their personal data. The Bill neither defines these two use cases, nor does it provide any examples of permissible uses.

Moreover, the Bill lacks any safeguards to ensure that any data collected by the government under this provision is necessary and proportionate to the specified purpose. In the absence of any clear guidelines or safeguards on the implementation of this provision, there is ample scope for misuse of this provision, which could impact firms' proprietary rights and also introduce significant privacy risks defeating the core objectives of the Bill.

4.4. Cloud services and BPOs would be impacted

The requirement to share anonymised and NPD extends to data processors, which would include cloud service providers (CSPs), online storage services, outsourcing entities, etc. However, by their very

definition, and the contractual terms that govern their activities, data processors do not have any control or ownership over the data being requested. Therefore, it would be impractical and legally untenable for data processors to share such data with third-parties, especially in the absence of any clear guidelines and safeguards around its subsequent use. If the Bill retains this provision, it may discourage foreign businesses from outsourcing their business processing activities to India, which would be a severe setback to the Indian BPO industry and associated sectors, severely impacting the growth of India's digital economy.

4.5. Organisations already voluntarily make data and tools freely available:
Over the years, private enterprises have voluntarily made large data sets available, which helps empower other organisations to innovate and develop programs that produce socio-economic value. For example, firms make data sets available to local governments and other partners to inform sustainable mobility projects[1] and to help in urban planning[2]. Businesses have also made open data sets[3] and tools[4] available to third parties, free of charge, so they can leverage the power of emerging technologies like AI/ML and cloud technologies[5]. These tools help produce valuable insights around differential privacy[6], image processing[7], video annotations[8], natural language processing[9] and search trends[10]. Importantly, these tools and datasets have been made available to third parties after a careful review of the sensitivity of the data involved, privacy concerns, liability risks, and to ensure conformity with intellectual property laws, which would be difficult under a forced data sharing regime.

4.6. Market incentives should be aligned to promote data sharing:
Private firms share data with third parties after evaluating various factors and often in limited circumstances, including restrictions based on the use cases and an analysis of risks and liabilities involved. These restrictions are in place so that the sharing of such data with third parties like start-ups does not increase privacy and security risks[11] for individuals whose data is included. For example, bad actors could re-identify data of individuals. The inclusion of multiple providers in assembling such data sets can make it difficult to impose liability. Therefore, firms that voluntarily share data should be provided legal immunity from any liability that may arise as a consequence of sharing such data esp. given that re-identification is a criminal offence under the Bill. Moreover, firms should be provided financial and other incentives to share data, including for example through tax concessions and reputational credit. Suitable governance frameworks (institutional and technical) should also be developed to increase the availability of data in the open market. On the other hand, the lack of intellectual property protection and market incentives will hurt investments into India and consumer choice.

4.7. Conflict with Indian intellectual property laws
The proposal for forced disclosure of anonymised data and non-personal data would be in conflict with the provisions of the Indian Copyright Act, 1957. As per Indian copyright law, the arrangement and selection of certain anonymised data sets would be protected, and exclusive proprietary rights therein would vest with its owner. Further, such anonymised data sets are strictly confidential and proprietary, protectable as trade secrets. However, the Bill imposes an unreasonable requirement to forcibly share

[1] https://www.waze.com/ccp
[2] https://movement.uber.com/?lang=en-US
[3] https://www.tensorflow.org/datasets/catalog/overview
[4] https://www.tensorflow.org/
[5] https://aws.amazon.com/opendata/
[6] https://developers.googleblog.com/2019/09/enabling-developers-and-organizations.html
[7] https://ai.googleblog.com/2016/09/introducing-open-images-dataset.html
[8] https://research.google.com/youtube-bb/
[9] https://ai.googleblog.com/2019/09/announcing-two-new-natural-language.html
[10] https://trends.google.com/trends/?geo=US
[11] https://startupnation.com/manage-your-business/startups-cybersecurity-attacks/

data upon receipt of a direction from the government. As such, the person who holds rights over such data will be deprived of his/her exclusive rights under the Copyright Act, including common law and statutory principles dealing with trade secrets and confidentiality. Such inconsistencies would create business uncertainty and impact ease of doing business.

4.8. Anonymization is difficult when multiple data sets are shared with the same entity

While a single organisation can ensure the integrity of anonymized data, it is harder to protect against re-identifiability when data sets are shared with an external entity that has access to parallel data and an incentive to re-identify individuals.

For example, if the government has access to an anonymized set of data about ride-shares and a similarly anonymized set of data about hospital visits, it may be possible to re-identify an individual's movements in the event of an outbreak.

Rather than reserving a blanket permission to demand anonymised data, the government should (though a separate process) work with providers to promote voluntary data sharing, to access information, which simultaneously prevent risks of abuse.

Recommendations

- The provision in the Bill relating to forced sharing of anonymised data and non-personal data should be removed in their entirety, since they are outside the scope of the Bill.
- Any proposed framework for non-personal data or anonymised data should be deferred until the Bill is passed appropriate standards, rules and regulations have been issued (eg. on anonymisation) and the NPD committee's report has clarified key details, including the scope of the term, the rationale for data sharing and potential use cases, modalities of sharing, etc.
- The government should promote voluntary data sharing mechanisms separately (e.g. via data marketplaces and data exchanges), with adequate intellectual property protections, privacy protections, fiscal incentives and legal immunity in case of liability emanating from such sharing. Such mechanisms should only be introduced after the NPD committee's report has been published and comprehensive consultations have taken place.

5. Social media intermediary

5.1. Social media norms are outside the scope of the Bill

The Bill's primary objective is to protect the privacy of individuals relating to their personal data. However, in a significant revision from the Draft Bill, it now includes a provision "laying down norms for social media intermediaries". According to the Bill, social media intermediaries (SMIs) are intermediaries who primarily or solely enable online interaction between users and allow them to create, share and distribute content. Intermediaries that enable purely B2B transactions, or pure-play ISPs, search-engines, e-mail services, online encyclopedias and online storage services are excluded from the scope of SMIs.

However, the reasons for introducing the concept of SMI in the Bill are unclear and it is a case of legislative overreach. The scope of regulation of social media intermediaries is outside the scope of the Bill and also does not fit in the Statement of Objects and Reasons of the Bill; . This provision was neither recommended by the expert committee that prepared the Draft Bill, nor was it a part of the consultations around the Bill. It is also unclear what connection exists between social media norms and the protection of privacy, Further, there is no explanation for why the Bill is the appropriate legislation lay down social media norms, rather than any other statute, like the Information Technology Act, 2000 which already defines the term 'intermediary' and deals with social media issues more generally.

5.2. Lack of clarity on obligations and classification

The Bill states that the Government may notify certain SMIs as significant data fiduciaries (SDF), which would be subject to more stringent obligations under the Bill. Such SMIs will have to enable their Indian users to voluntarily verify their accounts in such manner as may be prescribed. Further, the Bill states that such verification mark should be demonstrable and visible to all users of the service, in such manner as may be prescribed.

The Bill does not provide any clarity on the identity verification mechanism to be enabled and leaves it open to be defined by regulations. However, if the prescribed mechanism requires collection and verification of personal data, or even official identity documents, which are considered as SPD under the Bill, it will pose a heavy compliance burden on SMIs, without any rational basis for their inclusion.

The basis for classification of an SMI, and subsequently as an SDF, is also unclear. The Bill states that SMIs may be classified as SDFs if (1) they have users above a specified threshold, and (2) its actions must have or must be likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India. However, it is unclear how the user threshold will be calculated (for eg. it is presumed to include only Indian users) or how the government intends to determine the potential 'impact on electoral democracy'. Given the broad definitions used in this provision, it is likely that the classification of SMIs as SDFs will result in additional obligations, unreasonable classification and discriminatory action. Additionally, the power of the Government to notify intermediaries as SMIs on the ground of 'having an impact on electoral democracy' should be removed. The effect of and impact on electoral process is the sole domain of the Election Commission of India, as an independent constitutional body.

Previously, a Committee of experts constituted by the Supreme Court in the *Prajwala* proceedings, considered a proposal requiring identification of user accounts of social networking sites by linking them to government IDs. The Committee rejected the proposal on the grounds that it was not in the interests of users.

Further, the Supreme Court as well as the Delhi High Court have dismissed two independent petitions seeking verification of users by intermediaries, specifically social media companies. In fact, the Madras High Court has also refused to entertain this issue, especially in view of the Supreme Court judgment in the landmark judgement striking down several provisions of the Aadhaar Act and precluding any mandatory use of Aadhaar by private entities.

5.3. Identity verification is antithetical to privacy:

Many social media platforms do not envision real-name identities for their user base at all - the idea of bringing in even a voluntary verification process runs contrary to the idea of anonymity that is crucial for continued engagement on these platforms. For example, users who wish to post information that is in the nature of parody, humour or critique may wish to remain anonymous or pseudonymous. While the Bill clarifies that identity verification is purely voluntary on the part of the user, any system which privileges verified users over others (for eg. by demonstrating their credentials publicly) through a voluntary identity verification process, will create invisible pressures on those who wish to remain anonymous. The fundamental feature on some platforms is that *no user has the option to verify themselves* -- this in itself is part of the attractiveness of these platforms, and in turn provides a platform for free speech and expression and guaranteed by the Constitution. A system which protects the anonymity of some users, also protects the privacy of all users -- which is the primary goal of the Bill. Therefore, to ensure that privacy, anonymity and free speech and expression are safeguarded, we recommend deleting this provision.

Recommendations

- The provisions dealing with classification of social media intermediaries (SMIs) and further classification of SMIs as Significant Data Fiduciaries (SDFs) should be deleted, since the regulatory objectives and basis of classification are unclear and the regulation of intermediaries is already covered under the Information Technology Act and its regulations.
- The provisions dealing with voluntary identity verification by social media intermediaries should be deleted in its entirety. Once the regulatory objective sought to be achieved has been clearly defined, the government should conduct stakeholder consultations to determine the appropriate legislation or regulation through which such a provision may be introduced.

6. Compliance Burden and Discretionary Powers of Data Protection Authority ("DPA")

6.1. Heavy compliance burden compared to global data frameworks:

The Bill vests many discretionary powers with the DPA and imposes several additional obligations, especially on Significant Data Fiduciaries (SDFs), which are not part of other prominent data protection regimes like the EU GDPR. For example, the Bill provides for:

- Mandatory registration
- External audits and publication of 'trust scores'
- DPA's approval for data transfers, new technologies, codes of practice, etc.
- DPA to specify what would constitute a 'reasonable purpose' exception
- Certifying the "Privacy by Design policy" to participate in the sandbox and otherwise
- Methods of anonymisation, de-identification, data erasure etc.

Such high-handed regulation will severely impact emerging digital sectors like fintech, healthcare, etc., where firms process large volumes of data. Moreover, there are concerns about the capacity of the DPA to establish the necessary infrastructure and expertise to approve, monitor and enforce these provisions.

The exercise of the DPA's discretionary powers will have a significant impact on the processing activities undertaken by businesses (for example, additional requirements for notice and obtaining consent, 'reasonable purposes', data portability, etc.). Frequent changes will require businesses to overhaul their technical and organisational practices. All this unpredictability would impede the ability of businesses to plan their operations ahead of time to off-set costs. For small businesses and start-ups especially, this would be a huge set back.

Instead, the Bill should promote co-regulation and self-regulation models, by leveraging domain expertise across stakeholders in areas like anonymisation, encryption, etc. Several of the Bill's provisions should be made voluntary, along with capacity building programs to promote best practices.

6.2. Need for a consultative approach to rule-making

The Bill establishes the DPA as an independent regulator to oversee the monitoring, enforcement of the Bill. In order to administer its functions, the DPA is empowered to make regulations, issues codes of practices and to give directions. These regulations, codes and directives will have far-reaching consequences for India's economy. Accordingly, the DPA should be required to engage in a thorough consultation process before exercising these powers. Besides this, it must conduct adequate *ex-ante* and *ex-post* assessments of regulatory impact. Such provisions for consultations and regulatory impact

assessments are already contained in laws governing regulators such as the Telecom Regulatory Authority of India (TRAI) and the Airports Economic Regulatory Authority (AERA).

Though the Bill provides for mandatory consultations between the DPA and other stakeholders before issuing codes of practice, it is important that this requirement be extended to the various other rule-making powers of the DPA, to ensure that the expertise within the private sector is appropriately leveraged, including for example on:

- Methods of anonymisation, de-identification, data erasure etc.
- Security safeguards to be mentationed, including encryption technologies

Further, according to the Bill, the government need not consult the DPA on key aspects of rule-making, including:

- Data classification (i.e. notifying categories of critical personal data and additional categories of sensitive personal data)
- Grievance redressal (manner of making complaints, etc.)
- Exempting certain data processors (eg. for the purpose of outsourcing activities) and government agency from the applicability of the law.

Ensuring that the DPA consults other stakeholders, and is consulted by the government on key delegated rule-making powers under the Bill, will help promote business predictability.

6.3. Lack of regulatory capacity and expertise within the DPA

The DPA is entrusted with various supervision and enforcement functions, including:

- notifying SDFs
- monitoring cross-border transfers
- approving privacy by design policies
- review of Data Protection Impact Assessments reports
- data audits and specifying the criteria for assigning a trust score

The developments in technology are so dynamic that attempting to monitor for compliance will likely place an overwhelming burden on any government agency or regulator entrusted with such monitoring obligations. It is also unclear whether the DPA will have the necessary regulatory capacity to make determinations regarding classification of SDFs and social media intermediaries. Instead of nurturing the technology ecosystem as intended, this regulatory load will ultimately harm consumers, businesses and the government as well.

For example in the case of data trust scores - the Bill says that the DPA may specify the criteria for assigning data trust scores. It is practically impossible to capture the entirety of any organization's data protection practices through a quantitative metric like a trust score. Further, unless the DPA consults with industry stakeholders to develop appropriate criteria, which is relevant to a particular sector or industry, the score assigned to a data fiduciary would be subjective, arbitrary and could jeopardise the ability of consumers to access useful services.

Therefore, as previously recommended the Bill should promote co-regulation and self-regulation models, by leveraging the expertise of the private sector. Several of the Bill's provisions, including those relating to trust scores should be made voluntary, along with capacity building programs to promote best practices.

6.4. Data breaches cannot be directly reported to users

According to the Bill, a data fiduciary must inform the DPA about any breach of any personal data, where such breach is likely to cause harm to any data principal. However, only the DPA can determine if the breach should be reported to the data principal by the data fiduciary. The Bill specifies two factors that the DPA will consider: (1) the severity of the harm that may be caused; (2) whether any mitigating action is required.

However, such a provision prevents the data fiduciary from unilaterally informing the data principal about any breach. While the Bill specifies certain factors for consideration, it does not contemplate situations involving government negligence or other such situation (for eg. state-sponsored attacks). Unless the independence of the DPA is ensured in the Bill (currently the DPA's selection committee consists entirely of government officers, none from the judiciary), it is possible that data principals may not be informed about certain data breaches.

Given that the Bill uses the term 'data fiduciary', which implies a relationship of trust with the user, it is important that data fiduciaries are allowed to inform data principals about breaches directly, without having to obtain the permission of the DPA for this purpose.

6.5. Grounds for classification as a significant data fiduciary (SDFs)

The factors to be taken into account for the classification of significant data fiduciaries (SDFs) are quite subjective, for example the volume or sensitivity of personal data being processed. This creates significant discretion with the DPA in the classification of SDFs. Parameters for classifying a data fiduciary should be more specific under the Bill basis which the DPA can classify data fiduciaries as SDFs.

Further, some of the factors for classification as an SDF are unreasonable. For eg: turnover of a data fiduciary and usage of new technologies for processing is not a reasonable classification for an entity to be classified as an SDF, especially given the use of such technologies in cutting-edge domains such as healthcare, fintech, etc.

6.6. Financial dependence of the DPA on the Indian government

The DP Bill continues to retain the financial dependence of the DPA on the Indian government for its functioning. Lack of financial autonomy creates a significant question mark over the independence of the DPA, and the degree of its non-partisan and apolitical nature. We urge that the DPA should be separated from the 'government' as a prerequisite for their ability to 'act objectively and impartially', because the 'government' might 'itself be an interested party' and neglect the data protection law 'in order to fulfil certain of its' other 'functions, in particular for taxation or law enforcement purposes'. Financial independence is essential for the effective functioning of the DPA. This incorporates DPA having a) a separate and independent annual budget – so as to ensure that influence is not exerted on the DPA by the government through the budgetary process, and b) adequate financial resources to carry out their mandate. There exist established cases to support the above argument.

For example, the Court of Justice of the European Union (CJEU) clarified the concept of "complete independence" of data protection authorities in two landmark judgements delineating the precise requirements regarding independence in relation to influence and supervision. In the 2010 judgment *European Commission v. Germany*, the CJEU interpreted Article 28 of the Data Protection Directive as a norm setting up DPAs, which "must enjoy an independence allowing them to perform their duties free from external influence". The CJEU reached this conclusion by interpreting the Directive homogeneously with the requirements in Article 44 of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. In the 2012 judgment

European Commission v. Austria, the CJEU reiterated that the independence required under EU law "precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect" which may affect the DPA's decisions.

6.7. Composition of the Selection Committee

The DP Bill contains an amendment over the 2018 Bill in the provision relating to the composition of the Selection Committee, which will be constituted to appoint the members of the DPA. Under the DP Bill, the Selection Committee will constitute only civil servants and no judicial members. Although the Selection Committee's role is limited to making suggestions about appointments to the DPA, the lack of any judicial member (specifically that of a former judge) will raise concerns about the independence of the Selection Committee. An independent Selection Committee is paramount to ensure that the composition of the DPA in turn remains independent and technically competent.

6.8. Submission of privacy by design policy to the DPA

The DP Bill states that subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy to the DPA for certification within such period and in such manner as may be specified by regulations. The DP Bill is unclear if it is mandatory to obtain certification for a "privacy by design policy" and we oppose such a requirement, which is assessed on the basis of satisfaction of the DPA, or an authorised officer. We therefore, urge removing the requirement of submitting a privacy design policy for certifications purposes on the following grounds:

- How will the DPA be in a position to judge whether or not the policy meets a certain standard?
- If it is mandatory for companies to submit a privacy by design policy to the DPA, it is absolutely crucial that the DPA not only has independence but also a strong knowledge and skills on data privacy. Without significant independence and relevant skills DPA is likely to become a bureaucratic blocker to companies.

Recommendations

- The DPA's prescriptive powers must be narrowed down to minimise business unpredictability and compliance burden, by promoting co-regulation and self-regulation models, specifically:
    - Mandatory registration requirements for significant data fiduciaries (SDFs) should be removed, since the DPA will be notifying authority for SDFs and can review or publish the list of SDFs if required.
    - The parameters for classification of SDFs should be more specific and reasonable. Unreasonable grounds such as turnover of a data fiduciary should be removed.
    - The concept of 'trust scores' should be encouraged as an industry best practice.
    - Submission of a Data Protection Impact Assessment should not be made mandatory for the use of new technologies or involving sensitive personal data categories.
    - Audits should be performed by the Data Protection Officer of the data fiduciary (and not external auditors) to encourage corporate accountability through self-regulation, prevent duplication of efforts and an increase in compliance costs for startups.
- To promote consultative rule-making, industry bodies, companies and startups should be consulted before any standards are prescribed around security, anonymisation, portability etc. and the government should consult with the DPA on key issues like data classification.
- The Bill should include measures for ensuring transparency and independence in the functioning of the DPA. For example, the selection committee for appointment of DPA members should be diversified and necessarily include members from the judiciary (eg. Chief Justice of India)

B. Overarching Concerns Carried on from the 2018 Bill

1. Data localisation and restrictions on cross border transfers

We are committed to protecting the privacy and security of users around the world. However, the proposed data localisation provisions in the Bill could increase privacy and security threats, restrict digital trade and harm consumers by limiting choice, reducing universal access to information and increasing overall costs of consumption.

On the other hand, data flows contribute significantly to economic growth and digital trade. A Mckinsey[12] report states that global data flows contributes $2.8 trillion to annual trade, which is a larger share of the increase in global GDP compared to the global trade in physical goods. Another report[13] by AIMA estimates that greater penetration of digital technologies in India and greater openness to data flows could result in a fourteen-fold increase in value to India's domestic sectors, reaching $512 billion by 2030. A recent report[14] by ICRIER-IAMAI estimates cross border data flows increase India's total volume of good trade by ~$43 billion annually.

The DP Bill has eased the norms for cross-border flow of personal data, however, it continues to impose localization requirements for sensitive personal data ("**SPD**") and critical personal data ("**CPD**"). SPD and CPD are subject to the following compliances:

- SPD and CPD can only be stored in India, subject to very limited exceptions;
- SPD can only be transferred abroad upon obtaining explicit consent as prescribed in the DP Bill, and must meet additional requirements such as a contract or intra-group scheme approved by the Data Protection Authority ("**DPA**"), an adequacy test, or specific approval by the DPA;
- CPD can only be transferred outside India for emergency processing or subject to an adequacy decision.

There remain a number of concerns with the above approach:

First, any conditions or restrictions imposed on the free cross-border transfer of data has a counterproductive impact on the global economy, which relies extensively on the exchange of data with entities across the world. Since India is a key player in the outsourcing sector, the promotion of cross-border flow of data is critical. If any data is mandatorily required to be stored and processed in a particular location, it may prevent foreign companies from looking at India as a facilitative environment for business.
Second, an adequacy decision allows cross-border transfer of data to foreign countries based on whether such country has adequate privacy safeguards to protect data received from India. Since adequacy decisions are time consuming and prone to political constraints, it has not been proven to be an effective measure for regulating cross-border data flows. Further, an adequacy decision requires robust and specialized technical and legal knowledge that should be based on verifiable criteria and global standards. Since such a decision should be taken by an independent regulator, the DPA would be better equipped than the Central Government to make informed decisions in this regard.

Third, under the DP Bill, companies are required to submit requests for approval for specific cases of cross-border data transfers, that is not only burdensome for companies, but also for the DPA, which is already

[12] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows
[13] https://aima.in/media-centre/news-items/benifits-from-digital-trade-may-grow.html
[14] http://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf

required to fulfil a plethora of functions. We strongly recommend removing this requirement, which if implemented will become a significant blocker to ease of doing business in India. The DPA should approve model contractual clauses that companies can adopt instead of approving individual requests. Such a mechanism has been adopted by the EU, where model clauses have simplified the process of cross-border data flows for businesses across the spectrum.

Fourth, any restrictions on cross-border data flows to other countries may in turn result in protectionist measures from those countries. Such measures may affect the competition in the digital sector and may also include adverse steps by other countries such as restrictions imposed on Indians in relation to travel and employment, barriers on Indian companies to enter foreign markets, and sale of Indian goods abroad.

1.1. Data residency can be disruptive to the local economy and does not enhance privacy

We recognize the concerns that governments have regarding digital privacy and security and are fully committed to improving privacy and security safeguards for users. However, restrictive data localization doesn't solve these problems. Effective security and privacy don't depend on the location of data or the territory where data is processed, but rather in the security and privacy controls applied to such data, irrespective of where the systems are physically located.

In fact, data localisation could exacerbate security threats, for example by limiting pattern analysis helpful in detecting fraud. Storing data in one location could make it a more attractive target. Rather, globally distributed networks better protect against loss of data or interruption of service as a result of a technical failure or natural disaster.

Forced data localization also harms consumers as it limits their choice of service providers, and the increase in compliance costs for businesses may be passed down to consumers.

1.2. Data Localisation of 'sensitive personal data' is unnecessary and creates privacy risks

The Bill states that 'sensitive personal data' (SPD) must continue to be stored in India, though it may be transferred outside. In addition to this local storage requirement, the Bill imposes strict conditions under which SPD can be transferred outside India (after obtaining explicit consent, along with other conditions; for eg. SPD can only be transferred to certain 'permissible' countries).

Since the transfer of SPD is otherwise strictly regulated through these conditions, the government can meet its sovereign objectives (for eg. consumer protection) without having to mandate any local storage requirements.

Additionally, most providers will not already have systems in place that isolate sensitive personal data from other, general account data. Requiring specialised types of processing for different types of data categories often stored in the same account could actually create privacy risks by requiring companies to sort and identify the data that fall into this category in order to meet these additional requirements.

1.3. The unclear scope of 'critical personal data' is disruptive to businesses

The Bill allows the Government to notify certain categories of personal data as 'critical personal data' (CPD). CPD must be processed *only* in India. At present the Bill lacks clarity in the scope 'critical personal data' in the following respects:

- it does not provide any definition of CPD;
- it does not specify any parameters or criteria for classification of CPD;
- the government can notify categories of CPD, without consulting either the DPA, or industry, who will be significantly impacted.

Without prejudice to the above, our initial assessment is that it creates a heavy compliance burden and imposes restrictions on how companies can develop their products and services. This could result in companies delaying or even stopping the launch of certain consumer offerings in India, or launching a version with limited features.

In the absence of any such guidance, data fiduciaries will not be able to anticipate the infrastructural changes required to comply with this rule, which creates business uncertainty and heavy compliance costs should the timeline for compliance be insufficient. (Note that the timeline to meet any requirements that require local infrastructure investments is often measured in years due to challenges acquiring needed resources while meeting technical redundancy standards.)

Such uncertainty could impact FDI flows into India and lower India's ranking in the 'Ease of Doing Business' index prepared by the World Bank.This could also result in companies defensively or preemptively delaying or even stopping launches of certain consumer offerings in India, or launching a version with more limited features.

1.4. Need for clarity on sectoral regulations

At present, it is unclear how the cross border transfer conditions in the Bill will be interpreted in light of sectoral regulations. For example, under RBI's directive,[15] payments data must be stored *only* in India, but can be processed on foreign servers, provided the data is deleted within 24 hours. The Bill should clarify that SPD can be stored outside India as long as necessary for processing that is legally permissible.

Although the Bill provides for consultations between regulators, the lack of clarity before passage of the Bill creates business uncertainty and risk, and would inhibit the ability of companies to innovate using such data. This could impact growth in key sectors of the digital economy such as fintech and healthcare. The additional obligations would also make it difficult for start-ups to compete in global markets. For example, the lack of clarity would make it difficult for Indian fintech companies to gain access to innovative technologies like data analytics, AI/ML tools, etc. which depend on data flows. They may also lose access to cost-efficient cloud services in the global market. Therefore, we recommend that sectoral regulators work with the DPA to ensure that regulatory uncertainty and conflicts are eliminated to promote business predictability.

1.5. Data transfer conditions should be flexible to align with international norms

The Bill vests many obligations and discretionary powers with the DPA and the government in relation to data transfers, which impose a heavier compliance burden. For example, the Bill stipulates that cross-border transfer of SPD must be based on the explicit consent of the data principal among other additional conditions. We submit that the Bill should allow businesses to transfer data outside India, so long as explicit consent has been obtained.

Additionally, it seems that the data fiduciaries will have to obtain approval from the DPA's for contracts or intra-group schemes involving cross-border data transfers, even after having obtained explicit consent of data principals for the transfer of SPD. It is likely that the DPA will not have the capacity and resources to approve each and every contract/scheme in a timely way. This will cause serious operational delays, in particular to the outsourcing industry.

[15] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

Instead, the Bill should allow for cross-border transfers on the basis of standard contractual clauses and binding corporate rules that are approved once off and not on a case by case basis. These mechanisms provide users assurances that a DPA approved level of privacy and security standards are being upheld, while creating a reasonable path for businesses to transfer data overseas as necessary to provide products and services.

Rather, the Bill should enable bilateral and multilateral/regional mutual recognition frameworks and certification regimes, (e.g. modelling a light-touch US-India data transfer agreement after the EU-Japan mutual recognition of adequacy). This would help promote the secure and free flow of data and support cross-border privacy protections that are compatible with the borderless nature of trade and digital flows.

1.6. The Bill should be harmonised with global data governance frameworks

Data flows contribute significantly to economic growth and digital trade. For example, the amount of data flowing from one country to another is 45 times larger than a decade ago, and data flows now account for $2.8 trillion in annual trade (McKinsey, 2016). A recent report estimates that greater penetration of digital technologies in India and greater openness to data flows and digital trade could result in an fourteen-fold increase in value to India's domestic sectors, reaching $512 billion by 2030 (All India Management Association, 2019). if India promotes cross-border data flows, it will increase the total volume of good trade by ~$43 billion annually (ICRIER-IAMAI).

However, the restrictions on data flows provided for in the Bill may impact India's digitally driven growth and its leadership position at global trade forums. As the European Commission recently stated: "Data localization requirements appear both unnecessary and potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments. This kind of provision would also likely hinder data transfers and complicate the facilitation of commercial exchanges, including in the context of EU-India bilateral negotiations on a possible free trade agreement" (European Commission Submission on Draft Personal Data Protection Bill).

Recent global and regional digital trade agreements (including the G20 'Osaka Declaration', CPTPP, USMCA, etc.) have prohibitions against data localisation. India's trade partners in the APAC region, including Japan, Australia, and Singapore, already endorse data flows. Therefore, the Bill should be amended keeping in mind India's current obligations and potential arrangements under new and existing international agreements.

Recommendations

- India should avoid data localisation requirements, which are ill-suited to protecting privacy and security, and which are inconsistent with trade commitments and modern data protection standards. Privacy and security protections are not based on the location of data.
- Instead, the Bill should focus on establishing baseline standards for personal data that are consistent with global norms. This can include acknowledging tools and policy instruments designed to enable transfer between legal jurisdictions.
- The requirement to continuously store sensitive personal data (SPD) in India should be removed. Further, data fiduciaries should not be required to obtain the DPA's approval before each instance of transferring data outside India. Instead, we recommend the DPA to consider alternative mechanisms that are privacy protective and yet do not disproportionately restrict business flexibility. For example, developing sample data transfer clauses, or setting out

minimum protections (eg. Singapore PDPC's guidance[16]) which should be in the scope of every contract governing overseas data transfer. Alternatively, the DPA can consider publishing one or more sets of approved standard contractual clauses which can be used by companies 'off the shelf', as the European Commission has done.

- If the data localisation requirement is retained, then: (i) data transferred to a data processor on a B2B basis (for example cloud service providers) should be exempted from any data localisation requirements (ii) for other transfers, it should be clarified that SPD can be stored outside India as long as necessary for processing that is legally permissible.
- The Bill should expand the conditions for cross border transfer of data, by allowing for transfer of SPD outside India if explicit consent has been obtained. Exceptions should be provided for certain categories of data, contracts or schemes based on the DPA's one-time assessment.
- To ensure that the restrictions with respect to overseas processing are harmonised with the Bill, all relevant sectoral regulations should be reviewed based on industry consultations.
- The Bill should clearly specify the categories of 'critical personal data' and/or specify a principled based criteria for classification, e.g. based on the risk of harm to the data subject. The DPA, industry bodies and other stakeholders should be consulted before categories of CPD are notified by the government.
- India should explore bilateral and multilateral frameworks and certification systems and make suitable changes to the Bill to promote the growth of the digital economy, trade and consumer choice.

2. Children's definition, age verification and parental consent

We support the Bill's objective to ensure that children are kept safe online through certain safeguards. We remain committed to working with government, regulators, parents and other stakeholders to help ensure that this objective is met.

However, we recommend that some provisions in the Bill should be revised to ensure that teenagers continue to have access to useful, informative and accurate information and have a positive experience online. Many teenagers rely on online services to learn and self-educate and this Bill should not inadvertently restrict their access to information.

To ensure harmony with other global data protection frameworks and promote access to information, we recommend that the definition of a 'child' in the Bill should be reduced from 18 years to any person who is under 16 years of age. The requirement to verify the age of a child should be removed, since it creates additional privacy risks -- it would invariably result in data fiduciaries collecting more information including sensitive data about all individuals (including children of all ages) in order to comply. Further, we recommend that the provisions relating to children's consent should be made applicable only to those services which are directed to children.

Lastly, the parental consent mechanisms should not be prescriptive, as it creates practical challenges and could result in a 'chilling effect'. Rather, the implementation guidelines should focus on empowering young users and their parents with transparency and privacy tools, while allowing service providers to consider a broader range of technical solutions to ensure this.

[16] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-19-9-Oct-2019.pdf

The Bill's objective to keep children safe online is laudable and we remain committed to working with government, regulators, parents and other stakeholders to ensure this objective is met. However, the Bill's provisions with respect to children's data significantly departs from global data protection frameworks and lacks clarity in implementation, which could have unintended negative consequences for children's access to information and their personal development.

The Bill's text should be revised to help ensure that it is as effective as possible, while still allowing children and adults alike to have a positive experience of online services, and allowing service providers to consider a broader range of technical solutions to ensure this. The recommendations below, if implemented, would increase legal certainty, in particular to avoid overlap or contradiction with other legal instruments. Further, the implementation of these provisions should focus on empowering young users and their parents with transparency and privacy tools to experience the internet in a safe manner that takes into account the individuality and rights of each child, including recognising a broader variety of age verification mechanisms as effective.

2.1. The 18 years of age threshold is inconsistent with global frameworks:

The Bill defines a 'child' as anyone below the age of 18 years. This is inconsistent with similar provisions in other global data protection laws. For example, in the United States, the Children's Online Privacy Protection Act (COPPA) pegs the threshold at 13 years, while it is 16 years under the EU GDPR, and many EU Member States have made use of their right to lower the age to 13 (eg. Belgium), 14 (Austria) and 15 (France).

For a country like India, where more than two-thirds[17] of internet users are in the age group of 12-29 years, it appears that the Bill does not reflect the realities of how internet services are consumed by the youth in India, especially services targeted at children that deal with educational, communication, vocational and recreational content.

Unfortunately, the threshold of 18 years may result in a very large number of users being cut off from access to these services, which could impact their overall well-being, as well as their intellectual and emotional development.

2.2. Age verification requirements will have unintended privacy-reducing outcomes

The Bill's proposed age verification mechanism for children would invariably result in data fiduciaries having to collect more information about all individuals, including data which is potentially sensitive personal data.

Practically, the service providers may need to verify the age of all users to comply with the requirement, which could create more privacy risks for users, including children. This seems to reduce and not increase privacy protections. Very importantly, such age verification could also undermine the privacy of these users and affect anonymity on the internet, essentially taking away certain privacy choices from individuals.

2.3. Applicability to child-directed services

Under certain international data protection law regimes, specific requirements in relation to the processing of children's data focus on services directed to children. For example, COPPA applies to operators of commercial websites and online services directed to children under 13, or that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children under 13. It also applies to operators of general audience websites or online services but only

[17] https://startupnation.com/manage-your-business/startups-cybersecurity-attacks/

when they have actual knowledge that they are processing personal information from children under 13. Similarly, GDPR requires parental consent for the processing of children's personal data when the online service is offered directly to a child. Therefore, we recommend that Chapter IV of the Bill should be made applicable only to those services which are directed to children.

2.4. Restrictions on Guardian Fiduciaries

Guardian fiduciaries, despite their very nature (i.e. of providing services to children) are precluded from targeting services to them. This is an unfair treatment of a guardian fiduciary under the Bill as it is being placed in a more restrictive position compared to any other data fiduciary (which is not the case under equivalent laws such as GDPR).

Further, the Bill restricts actions such as tracking or behavioural monitoring by data fiduciaries when such actions may be required to improve technology on the platform and address social issues (for eg, promoting child safety). If this concept is implemented, the Bill should be modified to clarify the specific and reasonable scenarios where tracking, profiling, etc is restricted, for instance only where such activities may cause significant harm to the child.

2.5. Lack of clarity on implementation

The Bill requires a data fiduciary to verify the child's age and obtain the consent of their parent or guardian. However, the Bill states that age verification and parental consent mechanisms will be specified by regulations later. In the absence of any clear guidelines on age verification and parental consent mechanisms, there may be a "chilling effect" on companies providing services to children, causing preemptive or defensive ceasing of services. Further, it would pose significant logistical challenges for providers, impacting business predictability and ease of doing business.

Given all the challenges outlined above, the unintended outcome of this requirement may be that data fiduciaries would instead choose to preemptively or defensively not provide services to children to avoid the compliance burden. It could also mean that companies can only offer services when users are "signed-in" and reducing options for individuals to stay anonymous.

Therefore, we recommend that the parental consent mechanisms should not be prescriptive, as it creates practical challenges and could result in a 'chilling effect'. Rather, the implementation guidelines should focus on empowering young users and their parents with transparency and privacy tools, while allowing service providers to consider a broader range of technical solutions to ensure this.

2.6. These rules create unnecessary restrictions on access to information.

Setting the age of consent to data processing at 18 will create additional friction in teenagers' online experience that will stand in the way of their access to knowledge and prevent them from getting the full benefits of online services. Many of these teenagers rely on online services to learn and self-educate.

Age-gating requirements will also be applied unevenly, creating disparity and disrupting the equalizing power of the Internet. For the children of less educated, less digitally literate families, the additional requirements of parental consent might be enough to impede their access to online services altogether.

Recommendations:

- The definition of a 'child' should be reduced from 18 years to 16 years based on global norms like the GDPR.
- The requirement to verify the age of children should be removed to avoid creating new privacy risks through the collection of potentially sensitive information of children and all users.
- We recommend that Chapter IV of the Bill should be made applicable only to those services which are directed to children.

- Any change requiring parental consent to process data for users under the age of consent (with or without age verification) should be applied on a going-forward basis. In other words, if a user has legally consented to the data processing typical for an account before enactment of this legislation, that individual should be able to use that account as agreed without additional parental consent.
- To impose reasonable restrictions on guardian fiduciaries, S.16(5) should be modified as follows: "The guardian data fiduciary shall be barred from profiling, tracking or behavioural monitoring or targeted advertising that can cause significant harm to the child or undertaking any other processing of personal data that can cause significant harm to the child."

3. Grounds of processing

3.1. Consent as a ground for processing personal data

The current grounds for processing based on consent do not cater to routine/repetitive processing of personal data and SPD nor do they account for contractual necessity. Fulfillment of a contract must be a lawful ground to process data without consent, as is the case in international data protection laws including GDPR. Otherwise, every contract would need to be accompanied by separate consent forms. It would also fundamentally take away the autonomy of citizens to enter into digital contracts after full disclosure from both parties. Therefore, we recommend that routine transactions and contractual necessity should be allowed as a non-consensual grounds of processing.

The DP Bill mentions that the consent of the data principal in respect of the processing of any sensitive personal data shall be explicitly obtained. However, in cases where an entity manifestly makes data public, e.g. customer providing healthcare data to the customer service to justify a cancellation for that service, it is likely that an explicit consent may not be obtained. This could lead to instances wherein data is processed, despite no request for data by a data fiduciary. The possibilities to process sensitive personal data should therefore be slightly broader, including e.g. that the data may need to be processed due to a legal obligation, to defend a legal claim or in cases when the information is consciously made public/shared by an individual. Further, in the employment context allowing the processing of sensitive data without consent only for the recruitment or termination of employment could be limited too. It would be more effective to refer to "necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law".

The DP Bill mentions that 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. In this regard we would like to seek further clarity if the exemption only applies when a regulation was enacted. We also recommend adding 'product development' in the list of "reasonable purposes".

3.2. Expanding the grounds for processing to promote business predictability

There is growing recognition among regulators, researchers and organisations that asking individuals to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important user choices. For example, some data processing is necessary to make products work and to ensure that they are secure and reliable. Users can generally accept and even expect and consider it reasonable that some personal information needs to be processed by a company providing a product or service. In this scenario, asking users to provide consent presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

Rather, we suggest allowing businesses to expand the grounds to include processing on the basis of "legitimate interests". In fact, something like 'legitimate interest' is an independent basis under many data protection statutes, including the EU, Australia, Hong Kong and Singapore. In many cases, legitimate interests can provide a more privacy protective standard, since it requires data controllers to balance the rights and freedoms of the individual against the interests of the organisation processing the data and justify the processing based on that test.

While the Bill currently recognises "reasonable purposes" as a legal ground for processing personal data, it is actually a lot more restrictive than "legitimate interest" because of the fact that the purposes have to be specified by regulations before they can be relied on. A one-size fit all set of purposes developed by the government does not seem compatible with the increasingly digitised world we live in, where technology facilitates and accommodates a wide range of business offerings and business models. Businesses are best placed to know what purposes of processing personal data are necessary to support their operations, subject of course, to the privacy protecting balancing act mentioned above.

We emphasize that contractual necessity is a form of legitimate interest, which helps in determining how data is processed in a way that fits with legitimate interests and yet is proportionate in relation to any privacy issues. Legitimate interest allows data processing for certain legitimate business purposes, giving best service/products under a most secure environment. In Singapore, since the advent of the Personal Data Protection Act ("PDPA") in 2012, there have been a number of significant developments as well as announcements made as to its future amendments. One such change that has been announced is the proposed introduction of a legitimate interests basis for processing personal data that does away with the need for individual consent. In fact, such a basis already exists under the European Union's General Data Protection Regulation ("GDPR"), which came into effect on 25 May 2018.

The legitimate interests basis is flexible, and facilitates the day-to-day running of business, including protecting businesses from onerous obligations. Without this legal basis, businesses could be faced with the onerous task of having to obtain consent from a data subject who already reasonably expects that such processing will occur. Allowing businesses to circumvent this obligation means they are able to save both time and money. Further, the legitimate interests basis allows businesses to exercise more long-term control over their processing activities, without fear of individuals withdrawing consent at any time, which could be disruptive to the business.

For example, in some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work before employment starts. In such a case, the organisation has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Where the organisation seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment. The organisation will not use data for any purpose other than the recruitment exercise for which you have applied.

Given the context above, contractual necessity is still not recognised as an alternative ground for processing data without consent. This omission can have a major effect on contractual relationships and commerce, with multiple layers of consent leading to user fatigue and making the data processing more cumbersome and time consuming. To align with existing international data protection frameworks, we suggest that contractual necessity be made one of the grounds for data processing.
Similarly, the grounds for processing should take into account factors beyond the consent of the data principal including processing necessary for emerging technologies (which keep evolving), such as

Artificial Intelligence and machine learning. This is especially important in the context of the 'reasonable purpose' clause, which remains ambiguous and can only be determined by the DPA. We recommend that data fiduciaries be permitted to determine reasonable purposes, in alignment with the ground of 'legitimate purposes' recognised under the GDPR.

Recommendations

- Expand the legal bases for processing, particularly by replacing "reasonable purpose" with the more useful concept of legitimate interest.
- Include explicit reference to processing in performance of a contract or for legal reasons.
- Expand the list of reasonable purposes contemplated in the Bill to include purposes that are common and very reasonable business activities across different industries, e.g., to monitor and improve existing products and services, to develop new products / services and services, for debugging purposes, first party marketing and promotional activities

C. Deviations from *Puttaswamy* judgment

1. Exemptions to state

The vast exemption provisions under the DP Bill act as a restriction on the right to privacy, but do not meet the requirements laid down in the *Puttaswamy* judgment (that are, legality, legitimacy and proportionality). Restrictions on privacy that do not meet these three conditions are not constitutionally valid and are liable to be read down in a court of law.

Further, these provisions also permit wide powers to state agencies to conduct surveillance, which leads to significantly weakened personal data protection, where there is even a peripheral involvement of state interest.

In accordance with the *Puttaswamy* judgement, we request that the width of the exemption provisions are reconsidered and due process safeguards are instituted to prevent abuses of state power.

2. Identity verification by social media intermediaries

The DP Bill creates a requirement on data fiduciaries that have been designated as social media intermediaries ("**SMIs**") to provide users with the option to voluntarily verify their accounts, and provide a distinguishable mark for such verified users. Identity verification of users does not appear to have any benefits to protect or enhance privacy. On the other hand, it is posited that such a measure could compromise privacy: first, by allowing social media companies to store sensitive personal data for verification purposes, the user is exposed to a greater risk of a privacy breach and second, if the verification requirement is made a precondition to accessing goods and services at some point, it would in effect become mandatory and take away from the right to remain anonymous, which is an inalienable part of the right to free speech and expression.

Not only will this provision increase the risk of data breach of the individuals but also tends to ignore the right to anonymity of the users of the internet. Such verification will no longer be 'voluntary' but will be 'manufactured' because of social pressure and the mere introduction of the public record which 'marks' verified accounts. This is absolutely unfair as though there is a choice given to the users, the choice is controlled by a number of social and legal factors which ultimately harm the users as they will be doomed

whether or not they choose to verify their accounts. For example, survivors of sexual abuse will not have a platform for anonymous sexual harassment allegations if the social media accounts have to be verified. There is a chilling effect on the freedom of speech and expression if the complainants have to reveal their identities.

No other country has the provision for a voluntary verification mechanism of this nature. It is unclear how this requirement achieves the objective of safeguarding the privacy of individuals. Further, the Bill does not provide any clarity on the identity verification mechanism to be enabled, while the basis of classification of SMIs is arbitrary. Overall, the reasons for introducing the concept of SMI in the Bill are unclear and it is a case of legislative overreach.

Moreover, it is important to note that the Supreme Court as well as the Delhi High Court have dismissed two independent petitions seeking verification of users by intermediaries. An expert Committee constituted by the Supreme Court in the *Prajwala Proceedings*, also rejected a proposal requiring identification of user accounts of social networking sites by linking them to government IDs on the ground that it was not in the interests of users.

Even if the proposal for identify verification is voluntary on users, it may create invisible pressures on those who wish to remain anonymous on the platform. We submit that it is important to safeguard the privacy of *all users* on the platform. A system which protects the anonymity of some users, also protects the privacy of all users -- which is the primary goal of the Bill.

Therefore, to ensure that privacy, anonymity and free expression are protected, we recommend that the provisions relating to SMIs should be deleted from the Bill.

D. Other Issues

1. Applicability

The DP Bill continues to be unclear regarding its extra-territorial application, and does not specifically exclude the application of the legislation where data fiduciaries and data principals have existing agreements subject to the law of the jurisdiction in which the data fiduciary is present.

We recommend that it be clarified that the DP Bill shall not apply to processing of personal data that a data principal and data fiduciary have contractually agreed to subject to the laws of another jurisdiction.

India is an important player in the global internet policy space. Indian government leadership is eager to position India as a global leader on democratic data regulation and has largely succeeded. India has high levels of global internet policy participation—that is, activity in the UN General Assembly and elsewhere on internet issues—and analysts have rated the nation high on its ability to influence international policy. However, the text of the DP Bill largely appears to be a crude amalgamation of provisions in the GDPR with authoritarian leanings. In the DP Bill, these include the enabling framework for government surveillance in the bill, which undoubtedly entrenches government power to undermine citizen privacy. Further, the blurring of the distinctions between non-personal data and personal data remain is concerning. The DP Bill ultimately dilutes protections on individual data rights by enabling the government to access data. These leanings ultimately undermine India's potential to guide emerging market economies and smaller democratic states. Though some privacy-protecting measures in the DP Bill mimic several provisions of the GDPR, the legislation needs significant revisions - particularly on the cross border data transfers, extra-territorial application and social media verification -- if India wants to be a leader in forging a democratic, privacy-

protecting approach to the internet, enable its technology sector and establishment of global companies in the India market.

2. Lack of Surveillance Reforms

The Bill empowers the Government to exempt (without even consulting the DPA) any government agency from any or all provisions of the Bill. Such broad exemptions would reduce India's prospects of entering into bilateral arrangements for data transfers or law enforcement access. For instance, India may not be able to satisfy the requirements to enter into an executive agreement with the United States government under the CLOUD Act. It would also impact India's ability to obtain an adequacy qualification from the European Union under the GDPR. Therefore, the Bill should be revised to account for these considerations and suitable revisions should be introduced to increase India's prospects in this regard.

3. Criminal Penalty for Re-Identification

The Bill seeks to penalise any person who knowingly or intentionally re-identifies any de-identified personal data, without consent. The Bill provides for imprisonment of up to 3 years or a fine, which may extend to INR 2,00,000, or both. Under the current definition of the Bill, it is not necessary to show that harm was caused. Accordingly, we recommend that the Bill be revised to remove the criminal penalties. Further, all criminal breaches under this Bill should be subject to the threshold of *'intentional' and 'wilful'* acts by the breaching party.

4. Scope of sensitive personal data

The Bill should allow for exceptions to the definition of certain categories of sensitive personal data (eg. biometric data) to promote processing for certain purposes, particularly when that data is not used for identification purposes.

5. Definition of 'personal data'

The inclusion of the phrase 'any inference drawn from such data for the purpose of profiling' in the definition of 'personal data' is very wide and subjective, resulting in business uncertainty and additional compliance obligations (for eg. relating to data portability). The Bill already contains adequate provisions prescribing safeguards against excessive or large scale profiling. Hence, this addition in the Bill should be removed.

6. Employment Data

The Bill should allow data fiduciaries to process 'sensitive personal data' for purposes related to employment, as had been provided for in the draft Bill.

E. Section-wise Detailed List of Issues and Recommendations on each of the provisions in the bill.

A. HIGH PRIORITY ISSUES

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
1.	The Bill does not have any transitional provision.	(2) The Act shall come into force no less than 24 months from the date of its publication in the Official Gazette or such later date as may be prescribed by the Central Government	The removal of the transitional provision has significant implications for all the stakeholders, as there is no indication regarding the timeline for the implementation of the Bill. This will create uncertainty for all stakeholders, in understanding the amount of time they will have to comply with the various requirements under the Bill. In contrast, the global legislation like GDPR provides for a transitional period of 2 years for processing that was already underway to comply with its provisions. Hence, we recommend that section 2 of the Bill should be amended to provide for a transitional provision.
2.	**Section 14: Processing of personal data for other reasonable purposes**	(*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 reasonable purposes, after taking into consideration- (*a*) the interest of the DF in processing for that purpose; (*b*) whether the DF can reasonably be expected to obtain the consent of the data principal;	(a) Section 14 of the Bill does not specify the grounds for which PD may be processed without consent but merely acts as an enabling provision under which the DPA may specify what may amount to such exempted 'reasonable purposes' under the Bill. This is not a forward-looking stance, as it relies too heavily on the future determinations of the DPA, while the need of the hour is to provide clear and specific understanding of 'reasonable purposes' to allow for businesses to structure their operations while taking this into consideration.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(*c*) any public interest in processing for that purpose; (*d*) the effect of the processing activity on the rights of the data principal; and (*e*) the reasonable expectations of the data principal having regard to the context of the processing. (*2*) For the purpose of sub-section (*1*), the expression "reasonable purposes" shall include, without limitation- (*a*) prevention and detection of any unlawful activity including fraud; (*b*) whistle blowing; (*c*) mergers and acquisitions; (*d*) network and information security; (*e*) credit scoring; (*f*) recovery of debt; (*g*) processing of publicly available personal data; (*h*) the operation of search engines; (i) where processing is necessary to protect the vital interests of the data principal or of another natural person; (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; (k) processing is necessary for the purposes of the legitimate interests pursued by the data fiduciary or by a third party, except where such	(b) The GDPR has taken a forward-looking view on this and has allowed for the processing without consent in cases such as (i) where it is necessary for the performance of a contract which has been entered into by the data controller or to take steps at the request of the data subject prior to entering into a contract; (ii) for protecting vital interests of the data subject or another natural person; or (iii) where the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. (c) Processing for contractual necessity and legitimate interests are essential concepts which ensure that businesses do not rely on consent to process data. Given that consent has reduced significance in the digital age, it is very important to have similar standards under the Indian law. The consent standards under the GDPR is more flexible and the Bill also should accommodate these standards. (d) Accordingly, Section 14(2) should also specify two more grounds as 'reasonable purposes'- (a) performance of a contract, and (b) 'legitimate interests'. Additionally, the list of purposes given in section 14(2) should be mandatorily included under 'reasonable purposes', and not only as an indicative list.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		interests are overridden by the interests or fundamental rights and freedoms of the data principal which require protection of personal data.; (l) internally, in a lawful manner that is compatible with the context in which the personal data was collected; and (m) any other reasonable purpose specified by the Authority (*3*) Where the Authority specifies a reasonable purpose under sub-section (*1*), it shall - (*a*) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and (*b*) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.	(e) It is important to include both these grounds because a number of common data processing activities are covered under these two heads. DFs will have to incur high business costs for carrying out such common processing activities if they have to solely rely on the ground of consent of the data principal, even in these two situations i.e. performance of a contract, and pursuing any legitimate interest. It will be practically unfeasible and prohibitively expensive for DFs with a large number of users to obtain consent at all points of data collection and processing in these two situations. (f) For instance, DFs often use personal data for targeted marketing, so as to show potential customers such advertisements which will be relevant for them. This is a highly common model of digital marketing. However, it is practically impossible for DFs to take the consent of every potential customer before advertisements can be displayed to them. Thus, such a situation can be covered in the ground of 'legitimate interests', as marketing/ advertising and should qualify as a legitimate interest for any business.
3.	**Section 33: Prohibition on processing of SPD and critical personal data outside India**	We recommend that section 33 be deleted in its entirety.	(a) The language of section 33 is ambiguous and creates uncertainty. It states that SPD may be transferred outside India, but it must be stored in India. However, it does not mention if a copy of SPD can be stored outside India, or if SPD has to be stored exclusively in India. It is also unclear about whether such data can be processed outside India or not.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			(b) Additionally, the provision that certain categories of personal data, being "critical personal data", can only be transferred offshore in very limited cases, is troubling because of the ambiguity in the definition of the term and because the Central Government has broad discretion to include an expansive scope of personal data within this requirement without seeking inputs from relevant stakeholders. (c) Cross-border data flows are crucial to the growth of India's digital economy, and data localization will only act as an impediment in such growth. Very few countries have adopted such data localisation requirements, and for good reason: data localisation requirements does not improve data protection and often undermines efforts to do so. Instead, they severely disrupt operations of both data fiduciaries and data processors and result in a range of negative economic consequences. While governments may perceive a sense of increased security when imposing data residency requirements for data processed and stored in local IT facilities because they offer physical proximity and control, restricting IT services to the local jurisdiction does not provide better overall data security. (d) Many privacy regimes around the world do not place restrictions on the cross-border transfer of personal data as long as the data controller remains responsible for the protection of the personal data. The GDPR, for instance, expressly recognizes that flows of personal data to and from countries are necessary for the expansion of international trade and international cooperation. In the

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			Philippines, personal data can be transferred offshore but the data controller remains accountable for its protection. In Australia, organizations are responsible for taking reasonable steps to ensure that the overseas recipient of personal data does not breach the Australian Privacy Principles and the transferring organization remains accountable for the overseas recipient's acts. Such an approach would ensure that the DF retains responsibility for the data, without attracting the negative effects of localization.
4.	**Section 34: Conditions for transfer of SPD and critical personal data.**	(*1*) The sensitive personal data may only be transferred outside India for the purpose of processing, where- (a) Where the data principal has consented; or (b) where 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 Bill; or (c) binding corporate rules; or (d) transfer is necessary for the performance of a contract or the implementation of pre-contractual measures; or (e) transfer is necessary for the conclusion nor performance of a contract concluded in the interests of the data principal between the data principal and the data fiduciary or another person; or (f) the transfer is necessary for important reasons of public interest; or	(a) The Bill sets out only very limited legal bases on which SPD can be transferred outside of India. These bases are far narrower than comparable privacy regimes around the world such as the GDPR. (b) This can affect routine operations of entities, especially given that the list of SPD is expansive and can be further added by the central government. (c) The grounds for transferring SPD offshore should be expanded, including circumstances where additional consent for the transfer is not required, in order to allow for easier cross border data flows the benefits of which as explained above. (d) If the DPA is required to provide approval for contracts or intra-group schemes for transfer of SPD, until the DPA is set up, transfer of SPD may be freely made without adhering to the safeguards proposed under the Bill. Further, a prior approval for each contract will

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(g) the transfer is necessary for the establishment, exercise or defence of legal claims; or (h) the transfer is necessary to protect the vital interests of the data subject where consent cannot be obtained; or (i) the transfer is subject to appropriate safeguards such as legally binding instruments, or a relevant law.	disrupt business and it may significantly delay transfers and affect ease of doing business in India. This would defeat the intent of the Bill. Therefore, as long as DF provides for measures to ensure the protection required under the Bill, the transfers should be permitted without requiring additional approval of the contract or scheme from the DPA. This will also take care of capacity issues as DPA approving all contracts will result in significant delays in both on-going and new data transfers.
5.	**Section 24: Security Safeguards**	24. (1) Every data fiduciary 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 appropriate technical and organization measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act. These measures may include: (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data. (2) Every data fiduciary shall undertake a review of its security safeguards periodically.	(a) Applicability to DPs - The Bill directly imposes an obligation on DPs to implement security safeguards including methods such as de-identification and encryption, apart from DFs. Further, under section 64, the data processor may be held liable to compensate data principals for not incorporating adequate safeguards under section 24. This is at odds with the role of a DP, which is to process PD based on the instructions of a DF and on behalf of a DF. It is the DF which is responsible for determining the purpose and means of processing and DPs ordinarily do not have any control over the data. DPs may not have visibility over the nature, scope and purpose of processing or likelihood of harm to make an assessment of security standards necessary for such processing and therefore, may not be in a position to determine the necessary safeguards. Therefore, the responsibility for determining and implementing security safeguards should be vested with DFs and should not be extended

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			to DPs. Hence, the references to DPs should be removed from Section 24 and Section 64 must be revised accordingly (*see discussion on section 64*). (b) Nature of Safeguards- The Bill provides that DFs and DPs must implement necessary security safeguards. It does not clarify the nature of such safeguards. Therefore, the provision must be amended to specify that only technical and organizational safeguards need to be implemented. (c) Necessary Safeguards - The standard under the GDPR provision is appropriateness, whereas the Bill requires implementation of necessary safeguards. The GDPR further stipulates that appropriateness must be determined by taking into consideration, the state of the art, costs of implementation, nature, scope, context and purposes of processing, and the risk for rights and freedoms of natural persons. The Bill does not provide any such indicators and it is unclear how DFs and processors must determine what safeguards would qualify as necessary. Further, the under the Bill, the DPA has the authority to specify security standards (section 50(6)(l)) through codes of practice. Thus, the DPA may change the applicable safeguards from time to time and this would impede the ability of businesses to plan their operations ahead of time. Therefore, the standard under the provision must be revised to appropriate safeguards and the DPA's power to determine the standards must be removed and left to the discretion of DFs.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
6.	**Section 50: Codes of Practice**	**50.** (*1*) The Authority may, by regulations, specify non-binding codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act. (*2*) Notwithstanding anything contained in sub-section (*1*), the Authority may approve any code of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory Authority, or any departments or ministries of the Central or State Government. (*3*) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any code of practice under this section. (*4*) A code of practice under sub-section (*1*) or sub-section (*2*), shall not be issued unless the Authority has made consultation with the sectoral regulators, industry bodies, association of any class of data fiduciaries or processors and other stakeholders including the public and has followed such procedure as may be prescribed. (*5*) A code of practice issued under this section shall not derogate from the provisions of this Act or any other law for the time being in force.	(a) Under the Bill, codes of practice will be issued as regulations, which suggests that they will be treated as law and non-compliance with regulations can be equated with non-compliance with the law itself. This is different from the Draft Bill, where non-compliance with the code was only a factor to be considered by the DPA/ tribunal in determining whether there is a violation of the law. Treating codes of practice as 'law' runs against the understanding of codes. Codes of practice are intended as guidelines to help organisations comply with the law, rather than the law itself. Equating them with the law creates an overly restrictive environment for business operations. The codes of practice therefore should not be binding in nature. (b) Further, the Bill does not allow DFs/DPs to show compliance with a different standard (higher or equivalent to that envisaged in the DPA's code). (c) The competence of the DPA to issue such comprehensive codes of practice is also questionable given that more often than not these may require industry-specific knowledge and expertise. The GDPR approach in this regard is more practical since it allows industry bodies and associations to draft suitable codes of conduct which are then approved by the authority. While the Bill does provide for mandatory consultation with sectoral regulators and

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(*6*) The code of practice under this Act may include the following matters, namely:— (*a*) requirements for notice under section 7 including any model forms or guidance relating to notice; (*b*) measures for ensuring quality of personal data processed under section 8; (*c*) measures pertaining to the retention of personal data under section 9; (d) manner for obtaining valid consent under section 11; (e) processing of personal data under section 12; (f) activities where processing of personal data may be undertaken under section 14; (g) processing of sensitive personal data under Chapter III; (h) processing of personal data under any other ground for processing, including processing of personal data of children and age-verification under this Act; (i) exercise of any right by data principals under Chapter V; (*j*) the standards and means by which a data principal may avail the right to data portability under section 19; (*k*) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VI;	other stakeholders, we recommend that the Bill specifies that the stakeholders shall include associations representing class of DFs and DPs and industry bodies. (d) Onus of Reporting - Under the GDPR, processors are also required to report PD breaches without undue delay. However, the Bill places responsibility for reporting breach only on DFs and therefore DPs are not required to report breaches to the DPA under the Bill. However, section 50(6)(o) of the Bill provides that the DPA may specify codes of practice for the appropriate action to be taken by DF or DP in response to a PD breach. It is unclear why this provision refers to DPs when the responsibility under section 25 lies only with DFs. This should be removed to clarify that the responsibility must lie with DF and not DP as DPs may not have necessary control over networks and data to make such determination or to report such breaches. The relationship between DF and DP is contractual and DPs will not have the right to make determination with respect to a breach and report it. Section 50(6) (o) must be amended accordingly to omit reference to DPs.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 24; (*m*) methods of de-identification and anonymisation; (*n*) methods of destruction, deletion, or erasure of personal data where required under this Act; (*o*) appropriate action to be taken by the data fiduciary in response to a personal data breach under section 25; (*p*) manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 27; (*q*) transfer of personal data outside India pursuant to section 34; (*r*) processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 38; and (*s*) any other matter which, in the view of the Authority, may be necessary to be provided in the code of practice. (*7*) The Authority may review, modify or revoke a code of practice issued under this section in such manner as may be prescribed.	
7.	**Section 64: Compensation**	(1) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made	(a) <u>Negligence by the data processor</u> - The scope of a data principal's right to seek compensation from DPs should be very narrow and should not include

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		thereunder, by a DF or a DP, shall have the right to receive compensation from the DF or the DP, as the case may be. Explanation.—For the removal of doubts, it is hereby clarified that a DP shall be liable to pay compensation under this Section 64 only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section 31, or where the data processor has not incorporated adequate security safeguards under section 24, or where it has violated any provisions of this Act expressly applicable to it. (2) Provided that no compensation shall be awarded by the Adjudicating Officer under this Section except pursuant to a complaint made by the Authority. (3) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same 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 the data principal. (4) Where a data fiduciary or a data processor has, in accordance with sub-section (3), paid the entire amount of compensation for the harm	negligence. It is the DF that determines when to collect personal data and the reasons for collection, and controls all decisions on how it uses and discloses that personal data. DPs typically process data on the instruction of the DF. DPs, including cloud service providers such as AWS, have no insight into decisions for collecting or processing personal data and often have no control over the personal data that is stored or processed using their systems. Therefore, it is unreasonable to hold DPs liable for negligence given their limited insight into the nature of data that they process and their role and control over the decisions regarding the processing of that data. (b) Private action: Privacylaws should be enforced by the DPA, and there should not be a separate private right of action, particularly one that can be brought on others' behalf, with the right to recover attorneys' fees. A private right of action would lead to pervasive uncertainty, with the potential for different interpretations of the law to be pushed by different data principals and leaving it in the adjudicating officer's (**AO**) hands to resolve. Because privacy legislation is such a complex area of law, it is preferable to see the DPA create a coherent, consistent enforcement program with clear interpretation of the law so that responsible actors know what is actually required by it. The DPA can be trusted with putting the public interest at the forefront when making decisions when it comes to privacy. If data principals are given a right to seek compensation for any violation individually, in

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		suffered by the data principal, such 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. (5) Any data fiduciary or data processor aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.	cases where a number of data principals have been affected by the same incident (for example, a data breach), each affected data principal can individually seek compensation from the DF or DP. This will lead to AOs being subject to a heavier caseload than is necessary and having to spend additional time and effort hearing each matter separately, and can result in disparity in adjudication. Given this, we recommend that the private right of action should be removed from the Bill and only the DPA should be empowered to initiate an action against DFs/DPs. (c) Seeking of compensation by the data principal: Section 64 of the Bill allows for a mechanism by which the data principal may seek compensation for any harm suffered by them due to violation of the provisions of the Bill. While this is a beneficial step for data principals, the mechanism by which it is implemented is unjust and fails to address the complexities associated with such a compensation structure. Under the proposed mechanism, any data fiduciary or data processor can be ordered to pay the entire compensation amount and later claim from each of the other data fiduciaries or data processors the amounts corresponding to their responsibility for the harm caused. As per this mechanism, even though a data fiduciary has a majority of the responsibility for a specific harm caused, it is possible that a data processor which was merely acting according to its contractual obligations on behalf of the data fiduciary be required to pay the full compensation amount to the

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			aggrieved data principal, even if the extent of harm caused by it is far less. Even after such payment, there is uncertainty as the Bill does not specify any clear mechanism by which the paying entity may claim against the other data fiduciaries or data processors, nor a timeline within which this must take place. As a result, it is not incentivizing entities which comply with the Bill and instead may cause difficulties to them on an arbitrary basis, particularly in case of data processors. In the process of addressing the harms caused to data principals, Section 64 is thus causing other harms to such entities. Section 64 must be amended to clarify that DPs will only be liable to make payments if the following conditions are satisfied (a) where it has acted outside or contrary to the instructions of the DF, or (b) the DP has violated any provisions of this Act expressly applicable to it.
8.	**Section 91 – Act to promote framing of policies for digital economy**	We recommend deleting section 91, 2 (B) and 93 (2) (x).	(a) There has been no discussion on regulating non-personal data either in the report of the committee on 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians' under Justice B.N. Sri Krishna, or in any subsequent consultations regarding the Bill. This is because the policy objective of regulating non-personal data is fundamentally different from that of personal data protection. The former is premised upon data sharing in the interest of transparency and openness, while the latter is concerned with protecting the privacy of individuals. The very objective of the Bill as witnessed from the title and the preamble of the Bill, is the regulation of PD, to protect individual

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			privacy. This is at odds with the apparent intent behind the proposed Section 91(2) - mandating the sharing of anonymized PD and non-personal data. As a policy to regulate non-personal data would require distinct considerations and deliberations, this therefore cannot form a part of the scope of this Bill. In order for companies to develop products and provide effective products for the public, it will be important for the bill to recognise some allowance for using data for the benefit of society. Therefore, there needs to be an allowance for use by companies of anonymized or obfuscated data for research purposes etc. (b) The current wording of the provision is vague and ambiguous as it is not clear whether the Government can direct sharing of such data to third parties. Further, the provision appears to empower the Government to direct the anonymization of any PD even when the data fiduciary has not otherwise anonymized the same. This may undermine the very privacy that the Bill seeks to afford to individuals especially since anonymization is a moving standard in reality and a very low standard of irreversibility could result in expose of personal data and potential harm to data principals. The Bill does not specify a liability mechanism for breaches or exposures of data subject to a direction under this provision. This could have unintended consequences and result in the dilution of protection afforded to such data.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			(c) The concept of 'non personal data' is also very broad and cannot be narrowed down to any specific subsets of data. If such data is to be mandatorily shared with third parties, it may have widespread consequences on various stakeholders and businesses, as such information may relate to proprietary information, trade secrets or intellectual property and contractually enforced confidentiality sections and may be reverse engineered to cause harm to businesses, thus disrupting their functioning and impacting their competitive advantage. (d) Non-personal data may also relate to information which may not be otherwise shared as per extant laws, for instance privileged communications with medical and legal professionals. It may also result in misappropriation of data in the absence of safeguards specified in the Bill. Further, such information may be sensitive to groups and communities, if not to specific individuals and sharing of such data may result in harms such as redlining, targeted advertising, curated fake news etc. Release of such data may have immense potential for misuse and may pose a risk to national security. (e) At present, India does not have a law governing the processing of non-personal data by private entities or the Government and prescribing adequate safeguards for such processing. In the absence of such a law mandating the release of such data, be it to the

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			Government or third parties, may be extremely detrimental. (f) Further, there are currently no corresponding global regulations which mandate the sharing of such data and therefore a detailed study needs to be undertaken to examine the advantages and disadvantages of requiring mandatory sharing of such data. This section may also fail to meet India's obligations under various international agreements. For instance, the creation of barriers through the introduction of mandatory sharing requirements can lead to violation of India's obligation under the General Agreement on Trade in Services to avoid creating "disguised restrictions" on trade in services. Moreover, India has entered into several bilateral treaties that severely restrict how the Indian state may expropriate the property of foreign entities in India. Non personal data generated in India by such entities will be considered to be their property, and to that effect the Government of India is not in a position to restrict or mandate sharing of this property without breaching its obligations under the respective bilateral treaties with parent countries of such foreign entities, which can invite severe financial and reputational harm for Indian before international fora. Such a requirement can therefore have negative implications on India's foreign trade and relations and must be avoided.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
9.	**Section 93 – Power to make rules**	(1) The Central Government may, by notification, make rules to carry out the provisions of this Act; Provided that such rules shall not be issued unless the Central Government has made consultation with the sectoral regulators, industry bodies, association of any class of data fiduciaries or processors and other stakeholders including the public and has followed such procedure as may be prescribed. (2) The Central Government shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any regulations under this section. (3) A regulation issued under this section shall not derogate from the provisions of this Act or any other law for the time being in force.	(a) The Bill has significantly expanded the powers of the central government to notify rules (for instance, the power to notify further categories of SPD). Considering that the government has already appointed a DPA under the Bill, we believe that the state will have excessive rule-making powers, which will neither be subjected to the scrutiny of any non-government body or Parliament. Thus, such rule-making power should at least be subject to the process of stakeholder consultations. (b) The digital economy in India is nascent and growing, and it is important that the government takes into account the rapidly developing and changing practices of this field while issuing rules which will impact the same. Not carrying out such a consultation process will therefore significantly impact this sector and lead to difficulty in operation of such companies in India, which in some cases may lead to the exit of such companies from operating in India, impacting the economy and limiting availability of quality services as well as employment generation in the country. Further, while the Bill does provide for mandatory consultation with sectoral regulators and other stakeholders, we recommend that the Bill specifies that the stakeholders shall include associations representing class of DFs and DPs and industry bodies. (c) Carrying out a consultation process will ensure that the central government takes into consideration the

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			comments of various stakeholders before notifying the rules, thereby allowing them to formulate subordinate legislation which is practical and in consonance with the prevalent global practices.
10.	**Section 94 (1):**	(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. Provided that such rules shall not be issued unless the Authority has made consultation with the sectoral regulators, industry bodies, association of any class of data fiduciaries or processors and other stakeholders including the public and has followed such procedure as may be prescribed. (2) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any regulations under this section. (3) A regulation issued under this section shall not derogate from the provisions of this Act or any other law for the time being in force.	As provided above, it is vital in such a nascent and growing field that the DPA is required to carry out a consultation and take into account the views of stakeholders prior to notifying any regulations under this Section.

[B] MEDIUM PRIORITY ISSUES

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
1	**Section 2 (28): Definition of personal data**	(*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 physical, physiological, genetic, mental, economic, cultural or social identity of such natural person, whether online or offline.	(a) The definition of 'personal data' under the Bill is extremely wide due to the inclusion of the phrase "or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling". This expanded definition does not correspond to the definition stated under global standard such as GDPR. (b) Article 4(1) of the GDPR provides that 'Personal data' means *any information relating to an identified or* identifiable *natural person ('data subject'); in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.* The definition of PD under the GDPR is more specific. The GDPR specifies the identifiers that may refer PD and ties the definition to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. The definition under the Bill may relate to any characteristic, trait, attribute or other feature of

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			identity. Further, the definition under the Bill includes inferences drawn from such data for the purpose of profiling. (c) Thus, the ambit of data that would get regulated under the Bill as PD is much wider. There is no clear rationale for extending the scope of PD beyond physical, physiological, genetic, mental, economic, cultural or social identifiers and therefore, the definition under the Bill must be narrowed down.
2	**Section 2 (29): Definition of personal data breach**	(29) "Personal data breach" means any breach of security leading to unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, or integrity of personal data.	The Bill defines "Personal data breach" breach in a slightly wider manner by treating compromise of availability of personal data to a data principal as a breach of personal data. However, this is a cybersecurity concern and not a privacy concern and therefore, should not be included as a breach of PD. Hence, we recommend that the definition of 'personal data breach' under the Bill must be revised accordingly.
3	**Section 5 (a) - Limitation on collection of personal data.**	Every person processing personal data of a data principal shall process such personal data— (*a*) in a fair and reasonable manner that ensures the security of the personal data in accordance with the Act;	In sub-section (a), "ensuring" the privacy of data principals is too high a bar—this connotes that a DF has the responsibility for providing for the data principal's privacy. Privacy is a nebulous concept and it is too strict an obligation to ask an entity to ensure privacy of the data principal as opposed to ensuring the security of the information itself, which is more objective and practicable. Unlike the Bill, Article 5 of the GDPR does not place an obligation on the DF to ensure the maintenance of privacy of the data principal but instead requires 'lawful' processing and ensuring appropriate security

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			measures. Further, the requirement to ensure privacy combined with the definition of DF, would result in a contractual relationship being converted into a trust-based relationship. Since it leads to ambiguity on the exact role of the DF, we recommend softening and limiting the extent of the obligation to aspects within the realm of their control, by removing the privacy requirement and replacing it with a more objective standard of ensuring security in accordance with the provisions of the Bill.
4	**Section 8: quality pf personal data processed**	(*1*) The data fiduciary shall take reasonable steps to ensure that the personal data processed is complete, accurate, not misleading and updated, where necessary having regard to the purpose for which it is processed. (*2*) While taking any steps under sub-section (*1*), the data fiduciary shall have regard to whether the personal data— (*a*) is likely to be used to make a decision about the data principal; (*b*) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or (*c*) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.	(a) Necessary Steps - Section 8 places an undue onus on the DF to maintain PD of accurate and complete nature. The GDPR only requires DF to take reasonable steps to ensure that inaccurate PD is erased or rectified. The requirement under the Bill seems to be more absolute in nature. Further, the obligation to take 'necessary' steps is vague and is a high bar, as it does not take into account the capabilities of the DF and instead imposes the obligation on them to do all that is required to ensure the quality of the data. The obligation should be limited to taking reasonable steps. (b) Notifying Recipients - The Bill further places an obligation on DFs to notify third party recipients of data if the PD is not of required quality. This is a difficult and commercially unreasonable obligation for DFs to implement, since it will require them to assess each type of PD provided to them and reach out to any entities having access to such data in case

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			they determine that the data is not adequate. The obligation should be on the data principal to ensure that the data that they provide to other DFs is accurate. The provision under the Bill should be revised to remove this obligation.
5.	**Concept of Consent Managers** **Section 21 (1), 23 (3), 23 (4), 23 (5) and 94 (2) (b)**	Section 21 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 directly 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. Section 94 94. (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. (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:— ...	(a) The concept of "consent managers" is dealt with in Sections 21(1), 23 and 94(2)(h) of the Bill. The Bill defines consent manager as a data fiduciary which enables a data principal to gain, withdraw, review and manage consent through an accessible, transparent and interoperable platform. The Bill requires them to register with the Data Protection Authority (DPA) and comply with technical, operational, financial and other conditions specified by the DPA by regulations. (b) There is a lack of clarity regarding the minimum standards that will be adhered to by consent managers. The concept of "consent manager" is new to the Bill and there is no precedent in any other jurisdiction that we can look to for guidance. Moreover, there is no industry practice that can serve as a standard for consent managers in India. (c) The only equivalent is the Data Empowerment and Protection Architecture (DEPA) which is a standardized technology architecture for financial information services. However, DEPA participants are regulated financial institutions which are subject

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			to strict compliances. There is no guarantee that consent managers will adhere to the same standards and lowered data security standards could expose all fiduciaries who are compelled to interact with consent managers pursuant to the Bill. (d) Further, it is unclear whether the Bill expects data fiduciaries to conduct due diligence on consent managers to ensure whether they are registered and compliant with the Bill. Such an obligation would significantly increase their compliance burden. Additionally, delegation of decision-making obligations of data principals to any third party, opens up the potential for consent manipulation and increases the risk of harm that can accrue to the data principals concerned. (e) Accordingly, we have recommended that the language regarding consent managers is removed from the sections of the Bill that reference the same. Hence, we recommend Section 21 (1), 23 and 94(2) (h) to be revised in the manner set out herein.
6	**Section 25: Reporting of personal data breach**	(1) Every data fiduciary, after becoming aware of a personal data breach, 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. (*2*) The notice referred to in sub-section (*1*) shall include the following particulars,	(a) Trigger for Reporting - As per the GDPR, the obligation of the data controller to notify the breach kicks in only once the data controller has knowledge of the breach. This knowledge qualification is not present in the Bill. The knowledge qualification is necessary since DFs may not be in a position to notify breaches that are outside their knowledge. Therefore, section 25 must be amended accordingly.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		namely:— (*a*) nature of personal data which is the subject-matter of the breach; (*b*) number of data principals affected by the breach; (*c*) possible consequences of the breach; and (*d*) action being taken by the data fiduciary to remedy the breach. (3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority without undue delay after becoming aware of a personal data 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. (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. (6) The Authority shall not require the data fiduciary to report the personal data breach to the data principal under sub-section (5) if the data fiduciary has taken subsequent measures which ensure that the risk to the	(b) Timelines for Reporting - The GDPR specifies that the breach must be notified without undue delay and where feasible, not later than 72 hours after becoming aware of the breach. On the other hand, the Bill provides that the DF must report the breach to the DPA as soon as possible and within such period as may be specified by regulations following the breach. Therefore, at present, it is unclear what the reporting time period would be and this could cause hardships to DFs. Therefore, the Bill should specify that the reporting should be without undue delay and not 'as soon as possible'. (c) Informing Data Principals- The Bill requires DPA to determine whether the DF should report the breach to data principal. One way to interpret this provision is that the Bill requires DFs to inform data principals of breach only if the DPA requires it to. This would impact the DFs ability to inform data principals on their own. More importantly, there may be situations where the DF may have already taken measures to mitigate the risks arising from breach to data principals or it would involve significant costs to inform each data principal. The GDPR has taken this into account and requires the data controller to inform data subjects of breach only if it is likely to result in a high risk to the rights and freedoms of natural persons. Further, the controller need not report breach if it has implemented appropriate technical and organisational protection measures,

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		rights and freedoms of data subjects referred to in sub-section (1) is no longer likely to materialize, or it would involve disproportionate effort, in which case it shall require the data fiduciary to provide a public communication of the personal data breach. (7) The Authority may, in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (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. (8) The Authority may, in addition, also post the details of the personal data breach on its website.	which were applied to the breached PD, the controller has taken subsequent measures to alleviate such risk or it would involve disproportionate costs. Further, the supervisory authority may require the controller to inform the data subject only if the controller has not communicated the breach where it was mandated. These nuances are absent in the Bill.
7	**Section 26 – classification of data fiduciaries as significant data fiduciaries**	26. (1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:— (a) volume of personal data processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm by processing by the data fiduciary; (e) use of new technologies for processing; and (f) any other factor causing harm from such processing. (2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations.	If a DF is notified as SDF, it will be subject to higher compliances under the Bill which may include conducting DPIA, data audit, and appointment of DPO etc. Further, any new category of DF may be classified as SDF if the DPA is of the opinion that any processing carries significant harm to any data principal. A DF that falls under a notified category of SDF or fails to undertake DPIA or conduct a data audit or to appoint DPO would face penalty which may extend up to the higher of, INR 50 Million or 2% of its total world-wide turnover of the preceding financial year (section 57(1)). Despite the heavy penalties proposed to be imposed, there is no clarity in the Bill regarding which categories of DFs would be subject to SDF-related obligations. The Bill leaves it to the central government to make regulations to provide for the manner of registration

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(3) Notwithstanding anything contained in this section, any social media intermediary,— (i) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and (ii) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary: Provided that different thresholds may be notified for different classes of social media intermediaries. Explanation.—For the purposes of this sub-section, a "social media intermediary" is an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily,— (a) enable commercial or business-oriented transactions; (b) provide access to the Internet; (c) in the nature of search-engines, on-line encyclopedias, e-mail services or online storage services.	of SDFs (section 94(2)(i)). This is a crucial aspect on which further clarity would be welcome.
8	**Section 29 - Audit of policies and conduct of processing etc.**	**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.	(a) Applicability of Audit - Any DF notified as an SDF will be required to undertake annual audit of its data protection policies and operations. Other DFs may also be required to undertake data audit if the DPA is

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		(*2*) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including— (*a*) clarity and effectiveness of notices under section 7; (*b*) effectiveness of measures adopted under section 22; (*c*) transparency in relation to processing activities under section 23; (*d*) security safeguards adopted pursuant to section 24; (*e*) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25; (*f*) timely implementation of processes and effective adherence to obligations under sub-section (*3*) of section 28; and (*g*) any other matter as may be specified by regulations. (3) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section. (4) The data fiduciary shall engage independent persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as data auditors under this Act.	of the opinion that their processing is likely to cause harm. The Bill throws no further light on circumstances where a DF who is not notified as an SDF may be required to conduct such audit. This regulatory uncertainty must be addressed in the Bill. (b) Auditor - The Bill provides that the audit must be conducted by independent auditors registered with the DPA. It is unclear why the Bill is imposing further conditions on the auditor in this manner. The SDF should be able to engage any qualified auditor for this purpose. The Bill should be revised to remove such onerous conditions. (c) Trust Score - The Bill contemplates that the data auditor may assign trust score to DFs pursuant to the data audit. The DPA is responsible for specifying the criteria for such trust score under the Bill. The Bill does not provide any clarity on the basis in which the score will be assigned and therefore this an arbitrary measure and must be removed from the Bill.
10.	**Section 94 – Power to make regulations**	**94.** (*1*) The Authority may, by notification, make regulations consistent with this Act	(a) The powers given to the DPA under the Bill to make regulations are wide. The rule making power of the DPA in relation to manner of deletion of PD,

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		and the rules made thereunder to carry out the provisions of this Act. (*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:— (*a*) information required to be provided by the data fiduciary to the data principal in its notice under section (*n*) of sub-section (*1*) of section 7; (b) the safeguards for protecting the rights of data principals under sub-section (*3*) of section 14; (c) the additional safeguards or restrictions under sub-section (*2*) of section 15; (d) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (*1*), the fee to be charged under sub-section (*2*), the period within which request is to be complied with under sub-section (*3*), and the manner and the period within which a data principal may file a complaint under sub-section (*4*) of section 21; (e) 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; (f) the form and manner for maintaining the records, and any other aspect of	obtaining parental/guardian consent, verification of age, submission of privacy by design policy for certification, registration of SDFs, DPIA, data audits etc. are particular concerning for DFs and must be removed from the Bill. (b) There is also a residuary provision under section 94(s) which needs to be limited, since there is no mention of what circumstances would require a DPA to make regulations. (c) It must be noted that the DPA has powers under Section 50 of the Bill to specify codes of practice in relation to various processing aspects and together, these sections make for a body with extremely wide prescriptive powers. The extensive nature of these powers is likely to cause regulatory uncertainty and disrupt the functioning of businesses.

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		processing for which records shall be maintained under sub-section (*1*) of section 28; (g) the qualification and experience of a data protection officer under sub-section (*1*) of section 30; (h) the period within which transfer of personal data shall be notified to the Authority under sub-section (*3*) of section 34; (i) the provisions of the Act and the class of research, archival or statistical purposes which may be exempted under section 38; (j) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (*2*) of section 48; (k) the code of practice under sub-section (*1*) of section 50; (l) the form and manner for providing information to the Authority by the data fiduciary under sub-section (*3*) of section 52;	

[C] DIGITAL ECOSYSTEM ISSUES

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
1.	**Section 17: Right to confirmation and access**	17. (1) The data principal shall have the right to obtain from the data fiduciary— (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; (b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof; (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing. (2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person. (3) The data principal shall have the right to access in one place the categories of data fiduciaries or data processors with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.	Identities of DFs - The Bill increases the scope of access to PD by data principals. DFs will have to share the identities of other DFs with whom they have shared a data principal's PD and the categories of PD shared with them, all in one place and in the manner prescribed by regulations. As part of the notice under Section 7, DFs are required to inform data principals of the individuals or entities with whom PD may be shared, if applicable. Therefore, this requirement is excessive and a duplication of obligation that would only increase compliance costs for the DF and should be removed. We recommend revising the provision such that DF is only required to share the categories of DFs and DPs with whom PD has been shared.
2.	**Section 18: Right to correction and erasure**	(1) The data principal shall where necessary, having regard to the purposes for which personal data is being	(a) Scope of the Rights - The right of rectification under the GDPR is comparable to the Bill. But the scope of

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		processed, have the right to— (a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; and (d) the erasure of personal data which is no longer necessary for the purpose for which it was processed. (2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application. (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal. (4) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (1), such data fiduciary may take commercially reasonable steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them,	right to erasure under the Bill is more limited than the GDPR and is available only if the PD is no longer necessary for processing. (b) Rejection of Requests- Section 18 allows the DF to reject such a request with adequate justifications. In case the data principal is not satisfied with the justification, the data principal can require the DF to take reasonable steps to indicate that such data is disputed by the data principal, alongside the relevant data. However, under Article 18 of the GDPR, in case of any dispute regarding the accuracy of data, the data subject has the right to restrict processing. Except for storage, such data can be processed only with the data subject's consent (and in certain other specific exceptional situations). In this regard, the rights of data principals are diluted under the Bill as compared to the GDPR. (c) Exceptions- The GDPR recognises types of processing where right of erasure will not be available to the data subject. The Bill does not recognise any similar exceptions. Given that the right of erasure under the Bill is already narrow in scope, further exceptions are unnecessary. (d) Notifying other DFs - Article 19 of the GDPR imposes an obligation on the DFs to notify relevant persons of the rectification to the PD. However, this obligation is required to be fulfilled only if such notification is not impossible or does not involve

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		unless this proves impossible or involves disproportionate effort.	disproportionate effort. Section 18(4) of the Bill also imposes a similar obligation. However, the Bill makes it mandatory for DFs to notify relevant persons about the rectifications and does not provide any exceptions or qualifications. In this regard, the Bill increases compliance requirements for DFs. Since DFs are obligated to comply with the Bill for all processing by and on its behalf, the standards should be lowered to "commercially reasonable steps" or similar exceptions as provided in the GDPR should be included in the Bill. Section 18(4) should be revised accordingly. (e) Manner of Rectification - Further, the Bill provides that the manner of such rectifications will be prescribed by regulations. Depending on the DPA's exercise of these powers from time to time, businesses may have to change their organisational practices. This unpredictability would impede the ability of businesses to plan their operations ahead of time to off-set costs.Therefore, the manner of exercise of these provisions should be left to the DFs and Section 18 should be amended accordingly.
3	**Section 27 – Data protection impact assessment**	**27.** (*1*) Where the significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data in large scale, or any other large scale processing which carries a risk of significant harm to data principals, such processing shall	(a) Trigger - Recital 91 of the GDPR clarifies that a DPIA is required to be conducted prior to large scale use of new technology or processing of special categories of data However, under section 27, a DPIA must be conducted prior to every processing involving new technologies or using SPD, without

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section. (*2*) The Authority shall, by regulations specify, such circumstances, or class of data fiduciary, or processing operation where such data protection impact assessment shall be mandatory. (*3*) A data protection impact assessment shall, *inter alia*, contain— (*a*) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed; (*b*) assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and (*c*) measures for managing, minimising, mitigating or removing such risk of harm. (*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. (*5*) On receipt of the assessment and its review, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.	regard to the scale of the processing operations. The Bill must be revised to qualify that use of new technologies or SPD would require DPIA, only if it is in large-scale. Further, the Bill provides that the DPA *may*specify the circumstances or classes of DFs or processing operations where DPIA shall be mandatory. Given the potential costs that may be incurred by DFs in conducting DPIA, it is important to ensure that the exercise is conducted only where absolutely necessary. The GDPR requires supervisory authority to publish the list of operations requiring DPIA. In the same vein, the DPA shall also publish a list of processing operations that would require DPIA. (b) Content of DPIA - The GDPR requires the DPIA to contain an assessment of the necessity and proportionality of the processing operations in relation to the purposes. This requirement has not specifically been provided under the Bill. (c) Auditors - The Bill provides that the DPA may specify instances where DF must engage a data auditor to undertake DPIA. The DPA has been given the authority to register persons with expertise in certain areas such as information technology, computer systems, data science, data protection or privacy and other qualifications (as specified in the regulations) as data auditors. (*see discussion on Section 29 regarding the appointment of data auditors*) Unlike the Bill, the GDPR does not require

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
			DFs to engage data auditors. It is advisable to leave the decision to appoint data auditors to DFs to provide flexibility to businesses. The Bill is to be revised accordingly (*see discussion on Section 94*) (d) Manner of DPIA - Under Section 50(6), the DPA may also specify codes of practice regarding the manner in which DPIA may be carried out by a DF. It is unclear whether the DPA would have the capacity to make determinations regarding the manner of undertaking DPIA. While the GDPR requires supervisory authorities to specify the operations that would require DPIA, it does not require them to lay down the manner of conducting such DPIA. Therefore, the provision under the Bill is excessive and must be toned down. (*see discussion on Section 50*)
4	**Section 83: Offences to be cognizable and non-bailable**	(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be non-cognizable and bailable. (2) No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority. *It is also recommended* *that Section 94 of the Draft Bill be reinstated as below:* Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer	(a) Cognizable offences do not require a warrant from the Magistrate to make an arrest, as compared to non-cognizable offences. The Law Commission of India, in its 177th report states that the basis for classification of an offence as being cognizable is based on the need to arrest a person for various factors such as the need to prevent the commission of further offences, reassurances to the public, the need of investigation and so on. Similarly, a non-bailable offence is one that is classified on the basis of the gravity of the offence and the need to keep the perpetrator incarcerated during the pendency of the investigation. The offences under the Bill do not pose

NO.	PROVISION FROM THE 2019 BILL	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		not below the rank of Inspector shall investigate any offence under this Act.	a high enough level of risk to the public or invite consequences that require the suspension of an individual's liberties. Any investigative hurdles or risks that the offence may be committed again is not without remedy considering that the Authority is empowered with broad powers of search and seizure. (b) Unlike the Bill, the IT Act classifies only certain offenses as cognizable and non-bailable. Such offences are offences punishable with imprisonment of three years and above. Further, matters in relation to the Bill are technical in nature and require expertise during investigation. The IT Act recognises this and prescribes that only police officers of certain rank (inspectors and above) must investigate offences under the IT Act. A similar provision (which was previously under the Draft Bill) should be reinstated in the Bill.