

NASSCOM[®]



A **NASSCOM[®]** Initiative

**NASSCOM-DSCI FEEDBACK ON
THE PERSONAL DATA
PROTECTION BILL, 2019**

25 February, 2020

NASSCOM-DSCI Feedback on the Personal Data Protection Bill, 2019

NASSCOM and DSCI are pleased to submit before the Joint Parliamentary Committee (JPC), their submissions on the Personal Data Protection Bill, 2019 (PDP Bill 2019). We appreciate the consultation and review undertaken by the Ministry of Electronics and Information Technology (MeitY) on the Personal Data Protection Bill, 2018 (PDP Bill 2018). Public consultation undertaken by the JPC on the PDP Bill 2019 is a welcome step in continuing the discussion on creation of a robust framework for data protection in India. Upon the introduction of the PDB Bill 2019 in the Lok Sabha on 11 December 2019, NASSCOM and DSCI conducted both face-to-face and virtual industry consultations. This has informed our assessment of the PDB Bill 2019 and its likely impact on the industry, while keeping the focus on the key subject, i.e. the citizen and her privacy.

Overall, we support the PDB Bill 2019's adoption of a rights-based approach to privacy, and the creation of principal-agent relationship between data principals and data fiduciaries. Likewise, the importance placed upon the requirement of free, informed, specific and clear consent, is commendable. We welcome the direction reflected in the PDB Bill 2019 (vis a vis PDB Bill 2018) to ease cross-border flows of personal data.

However, certain issues subsist within the framework of the PDB Bill 2019, that we think can be resolved with this round of consultation, particularly regarding:

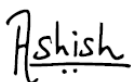
1. Categorisation of Sensitive Personal Data and its consequential impact
2. Restrictive grounds for Processing Personal Data and Sensitive Personal Data
3. Restrictions and conditions for Cross-Border Transfer of Sensitive Personal Data and Critical Personal Data
4. Lack of appropriate framework to build trust for processing of global data in India:
Power to Exempt certain Data Processors
5. Provisions Dealing with Non-Personal Data
6. Strengthening of framework for an effective and accountable Data Protection Authority
7. Lack of appropriate grading of Criminal Offences

Our submission is organised in four sections as follows:

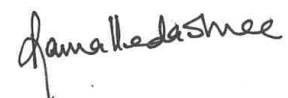
Sn.	Particulars	Page no.
I.	Recommended Principles for an effective Personal Data Protection Framework	3
II.	Key Concerns in the PDP Bill 2019 and suggestions to address them	7
III.	Key areas where the provisions of the PDP Bill 2019 need clarification in order to minimise uncertainty.	26
IV.	A clause by clause analysis of the PDP Bill 2019	32

We have provided rationale for each of our suggestion and wherever possible we have provided examples and use cases to highlight our point. We hope that our submissions can help operationalise an effective framework for individual privacy in India, while projecting India as a trusted, efficient and competitive player in global digital value chains.

We would like to be given an opportunity to appear before the Committee to explain our recommendations and discuss the same.



Ashish Aggarwal
Sr Director and Head-Public Policy
NASSCOM



Rama Vedashree
CEO
DSCI

Part 1

Recommended Principles for an Effective Personal Data Protection Framework

These **three foundational principles** must form the basis of the data protection and privacy legislation, i.e.

1. Operationalise privacy as a fundamental right;
2. Enhanced trust in the ecosystem governed by the legislation and a framework that is suitable for Data Driven Innovation (**DDI**);
3. Transparency and accountability requirements for all players in the ecosystem, including the State and regulators.

Each of these foundational principles, comes with a set of imperatives, which have been elaborated through the course of the present submission.

(1) Operationalising Privacy as a Fundamental Right

The Supreme Court of India's re-statement of the fundamental right to privacy in *K.S. Puttaswamy v. Union of India* was a pathbreaking moment for privacy in India. We believe any law that is created to protect the privacy in India, should work with the primary objective of operationalising privacy as a fundamental right by creating an equitable framework for execution of data principal rights, and guarding against potential excesses by enterprises and state alike.

Meeting the following **imperatives** would be necessary in achieving this end:

- a) Access to Speedy Redressal – Provide users with accessible and effective methods for exercising their rights and voicing their grievances about the practices of data fiduciaries.

It is imperative that the system so created provides speedy execution of user rights that flow from the constitutional status of privacy as a fundamental right, and user's grievances around data fiduciaries' practices vis-à-vis the data principals rights.

- b) Respect for User Choice and Control – The framework should focus on enabling a user to exercise her choice, on the purpose of processing of her personal data, especially with respect to disclosure and third-party sharing of such data. Other specifics, including technological specifications or the location of personal data, should not be user driven, and should not be the primary consideration from a regulatory perspective.
- c) Foster Adoption through Privacy Literacy – Enable the creation of a data ecosystem where all the stakeholders understand their roles and responsibilities vis-à-vis the user's privacy. The Data Protection Authority in collaboration with data fiduciaries should champion the goals of creating greater privacy awareness amongst users, as well as greater awareness amongst enterprises and the Government, on issues of data privacy.

(2) Encouraging Innovation and Increasing Trust:

It is imperative to create an environment that fosters DDI in India. One of the essential features of innovation is to explore unknown applications of technology. DDI isn't just about collecting more data. One innovates to modernise, and modernity means harnessing all the

knowledge one can, from the data one processes. To achieve long-term success, a company charts out a comprehensive digital transformation journey and prioritises the infrastructure and resourcing needed to leverage and extract data to its full potential. Such innovation cannot take place in the absence of user trust; hence it is important to establish a symbiotic relationship between trust and innovation.

Meeting the following **imperatives** would be necessary in achieving this end:

- a) **Fair use of Personal Data Processing** – While processing a user’s personal data with a view to innovate on products and processes, an organisations’ first and foremost focus must be on the fairness of the organisation’s decision making.

Users should be able to understand to an extent, what operations are being performed on their data. Without clearly explaining and communicating to the user the contours of their data usage, we cannot create digital trust in the innovation ecosystem.

- b) **Responsible Access to Data** – Enable responsible access to data so that organisations can carry out DDI, based on accountable data collection. Organisations should also be allowed to innovate freely with data that doesn’t fall within the sphere of privacy rights, i.e. anonymised data.
- c) **Readiness to deal with uncertainty** – For innovation to flourish and for the legal framework to be future ready, the proposed law must bind the discretion provided to the Data Protection Authority or the Central Government with due processes to ensure a high level of confidence in the regulatory actions, including regulation making. Flexibility in law should strengthen the ability to act swiftly and appropriately but should not result in hasty or opaque decision making. An inconsistent adherence to the objective of the legislation leads to disproportionate regulatory burden and has an unintended chilling effect on innovation.

Currently, in some areas, the Bill suffers from being overly prescriptive and in some situations, it saddles DPA and the industry with avoidable processes. Examples of this include, the requirement for the DPA to approve each cross-border transfer and the inclusion of an expansive definition of sensitive personal data (including official identifiers, financial data, etc.), despite the Bill having adequate regulatory principles to guard against harms.

Sanjeev Sanyal’s recent paper has highlighted the policy challenge aptly – “*It is very difficult to create regulations for every possible state-of-the- world. It is also very difficult to account for every non-compliant... It is then a slippery slope towards a regulatory framework that throttles the compliant with endless box- ticking and excessive requirements. It would be far better, therefore, to have a simpler regulatory framework supplemented by active and efficient supervision. The problem is that supervision demands active monitoring and accountability from the government department or regulatory body. This creates a perverse incentive to keep adding more top-down regulations regardless of their effectiveness.*”¹ The JPC should therefore review the proposed Bill for excessive requirements and remove them and focus on creating an active and efficient supervisory mechanism built on accountability and transparency. Further, our industry consultations pointed to many areas where there is a possibility of varied interpretation of the clauses. The JPC may consider

¹ Risk Vs Uncertainty: Supervision, Governance & Skin-in-the-Game, Discussion Paper No. 1/2020-DEA, see: <https://dea.gov.in/sites/default/files/Risk%20Vs%20Uncertainty%20Final.pdf>

simplifying the law to enable ease of interpretation and avoid unnecessary litigation over the interpretation of regulatory requirements under the Bill.

(3) Accountability and Transparency:

Accountability and transparency are the two most important elements for effective data privacy governance. Establishing a legal and reporting framework that nudges the ecosystem towards adopting organisational structures, strategies and procedures that imbibe and foster a culture of privacy should be the cornerstone of the legislation.

Meeting the following **imperatives** would be necessary in achieving this end:

- a) Actions to Demonstrate Compliance – The Bill must create a legal and reporting framework with finite and definable actions through which the fiduciary is able to communicate meaningful compliance with the law.
- b) Clear and Predictable Enforcement Guidelines – Recognising that this would be the first endeavour towards privacy compliance for several organisations and the State alike; the guidelines for enforcement should clearly communicate what is expected of data fiduciaries, towards complying with the law. These guidelines must be certain and allow for periodic consultative updation.
- c) Regulatory Governance – The authority established to implement the law must be independent in its operation, guided in its rulemaking by certain and well-established principles, be transparent and consultative in the discharge of its functions, and be accountable towards the execution of its duties and action.
- d) Co-Regulation and Self-Regulation – The development of code of practices/regulations to implement the law must be done in a manner that accommodates the needs of a range of stakeholders. This will require the codes to be dynamic, technology agnostic and flexible to adoption of different standards if they meet the desired intent of the legislation. The Bill must recognise the importance of industry codes and certifications as a mode of regulation.

In line with the foundational principles outlined above, NASSCOM and DSCI note that there are several **positives** in the PDB Bill 2019, as referred to the JPC, taking cognizance of the feedback received during previous rounds of Public Consultations, and we recommend that the JPC may strengthen these:

- 1) Easing of Restrictions on Cross-Border Transfer of Personal Data**
The PDB Bill 2018 required one copy of personal data to be stored within the territory of India, for transfers of ‘personal data’ to take place. Further, such transfers could only take place based on standard contractual clauses or intra-group transfer schemes. These restrictions have now been removed.
- 2) Removal of Passwords from the indicative list of Sensitive Personal Data**
Passwords have been removed from the indicative list of Sensitive Personal Data under Clause 2(36) of the PDB Bill 2018.
- 3) Removal of certain Criminal Offences**
The PDB Bill 2018 listed the obtaining, transferring or selling of personal and sensitive personal data in a manner contrary to the Act as an offence punishable with imprisonment up to three years. These provisions have now been removed.

4) Creation of sandbox to encourage innovation

The DPA shall create a sandbox for encouraging development of artificial intelligence, machine learning or any emerging technology in public interest.

5) Due Process Requirements for Investigating Offences

The power granted to police officers above the rank of Inspector to investigate offences under the PDB Bill 2018 have been removed. In PDB Bill 2019, an investigation must happen based on a complaint by the DPA, and subsequent to a court order issued based on such complaint.

Likewise, the inclusion of accountability and transparency requirements such as purpose limitations, collection limitations, and importance given to new age regulatory principles such as “privacy by design”, are big positives but each of these requirements could present compliance challenges that need to be recognised and addressed, through express guidance in the Bill itself.

Through our submission we’ll express these concerns under two buckets – the first focussing on elements of the Bill that raise major concerns for the industry; the second, focussing on those elements of the Bill that create uncertainty and manifests in ambiguity and risk.

The major concerns and the elements which contribute to ambiguity and risk have been supplemented with industry use cases to bring out the impact on the industry in case the Bill is adopted in its present form.

Part 2

Major Concerns

I. Categorisation of Sensitive Personal Data and its consequential impact [Clause 3 (36), 3(18), 3(21), 3(26) and Clause 15]

Under the Bill, sensitive personal data (SPD) includes ‘financial data’, ‘official identifiers’ and ‘health data’. In turn, the classification of these categories of data as SPD, has cascading ramifications on the grounds available for processing these categories of data, the ability of an enterprise to make cross-border transfers of such data, and other controls applicable to SPD.

Likewise, each of these categories of data, i.e. ‘financial data’, ‘official identifiers’ and ‘health data’, have been defined broadly enough to capture within their ambit significant amounts of data which are not sensitive, and consequently do not merit the significantly stringent safeguards associated with SPD.

Illustrative Use Cases

Illustration 1 – Financial Data (Wide scope): Person X applies for an insurance policy with Company A. Company A, in order to enable tracking of the status of the policy application, generates an application ID. Further, to check for the authenticity of the policy request requires the Person X to enter their mobile number as part of the initial sign up process.

The application ID and mobile number would qualify as sensitive personal data under the present definition as it represents the relationship between Person X and Company A (being a financial institution).

Company A would now require upgrading its security controls around Application IDs, Passwords associated with their users’ dashboards, mobile numbers, and other associated personal data – which by extension would have to be treated as SPD.

Company A would also be required to continue storing a copy of *all* the data within India and take explicit consent for collection of mobile numbers and other similar personal data as part of this process.

Illustration 2 – Financial Data (Applicability to Employers): Company A, for the purpose of payroll processing requires to process bank account details of its employees every month and if it is a global company, store this data in its global accounting/ HR system. Processing of financial data for the purpose of employment is essential and an employee does not really have an option to disallow such processing.

Consider another variation, Company A, for the purpose of reference check, processes data related to financial status or credit history of a potential recruit. It takes explicit consent. It recruits the candidate and the candidate is now an employee. Should explicit consent be necessary for processing (including storing) of the reference check related financial data in global accounting/ HR system of Company A?

Given that an employee has remedy in case of any harm as a result of such processing, requiring the employer to build/ offer and manage a consent architecture and related compliances due to financial data being an SPD appears to be excessive.

Illustration 3 – Financial Data (Applicability to entities other than financial institutions/ payment system providers or employers): Person A is admitted to a small Hospital X where she or her family member is required to share credit card details or insurance policy details to cover for expenses etc. Hospital X can legitimately process this information only for discharging service to the patient. Requiring hospitals to implement explicit consent-based architecture, especially small hospitals, appears to be excessive. Even

for a global hospital chain, requirements to comply with cross border restrictions in processing of financial data is excessive.

It is not clear how this would increase the safeguards to data privacy. How will the explicit consent requirement will work when the patient is not in a medical condition to share his insurance policy details (would this be financial data?) and the data is shared by someone else on behalf of the patient?

Illustration 5 – Health Data (Wide Scope): Person Y, while registering for a health check-up at Hospital A, is required to fill in her medical history information in the registration form. As part of the form she is also asked to fill in her name, mobile number, date of birth, place of residences, etc. which would traditionally fall under the category of personal data.

Hospital A is an international chain with its presence in India through joint-venture partners. As a part of the charter agreements, Hospital A is required to utilize the vendors of the global chain, for processing and maintaining patient records in a manner compliant to standards of protection accorded to healthcare data in the jurisdiction of incorporation of Hospital A.

However, since this data is collected in course of registration for a health service, it would have to be treated as sensitive personal data by Hospital A.

This would require Hospital A to seek explicit consent of Person Y, for both the processing and transfer of otherwise personal data (such as phone numbers, which are processed for varied purposes including transactional messages, and updates on appointments), as also localising the data – which might be at variance with its charter agreements.

Illustration 6 – Official Identifier (Relevance as an SPD – business requirement): Company C, in order to maintain access control, and maintain a record of persons entering and exiting its premises collects government issued identifiers.

Person X, not being an employee of Company C, has a meeting in the premises of Company C. The security guard asks for Person X to produce his Government ID and hold it before a camera so a picture of the ID can be taken and stored in the security system. Person X refuses to give his explicit consent for capturing of his Government ID.

Illustration 7 – Official Identifier (Relevance as an SPD - AML Requirements): Company A, which is based out of Singapore engages Vendor B, an MSME in India for IT services. Company A requires information which includes official identifiers and account information to execute wire transfers to the personal accounts of one of the representatives of Vendor B.

Company A, to be able to make such wire transfers, would be required to conduct due diligence in the form of processing and analyzing financial information offshore for anti-money laundering (AML) and combating financing of terrorism (CFT) purposes. However, Company A will be required to take the explicit consent of Vendor B (which by its definition, is capable of being withdrawn), and for each similarly placed end-user.

Illustration 8 – Visa Processing Services (Official Identifier - Relevance as an SPD): User X, wishing to travel to Japan, needs to apply for a travel visa. For this purpose, User X needs to provide details of his official travel document (an official identifier) and biometric details, to Vendor A, which processes Visa applications for Japan.

In this scenario, both explicit consent as well as a case-by-case approval by the DPA to enable the offshore processing of this data, is superfluous in view of the country's obligations under international law, and the travel requirements of User X.

However, under the Bill as it currently stands, owing to the classification of both official identifiers and biometric data as SPD, Vendor A and the Government of Japan would necessarily be expected to comply with all the associated compliance requirements under the Bill.

European experience (Health as an SPD)

In Europe health data is relatively narrowly defined and financial information is not an SPD. Even to comply with this narrower scope, hospitals and healthcare institutions across the European Union need to significantly adjust staff recruitment, staff training, business adjusting, and technical upgrades, etc. Only those institutions capable of affording the capital and human input in the effective protection for patients' personal health data will survive in the future.² As per PDP Bill 2019, health institutions in India would need to process both financial information and health data as SPD. The proposed scope needs to be reviewed so that the cost of health services is not unnecessarily increased, and digitalisation of health services is not discouraged.

Key Concerns:

1. The concept of SPD is primarily used for providing a higher level of protection to the data principal against instances of profiling, discrimination and infliction of harm that are identity driven. We are of the opinion that financial data, especially in the broad form it is currently defined, should not fall into this category.
2. In its present formulation, the Bill lays down an ambiguous definition for 'financial data' and 'health data'. Under the Bill, 'financial data' includes, *any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history*. As for 'health data' it includes, *data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services*.
3. As illustrated above, such a broad formulation would invariably raise data that would have been previously classified as 'personal data' to the category of SPD, hence defeating the purpose of having a special category of data that requires added protections and differential compliance requirements.
4. The twin effect of financial and health data being afforded such a broad definition, and being classified as SPD, may lead to potential difficulties in several day-to-day operations. This includes internal operations such as processing of employee data for payroll and health services, HR related processes for onboarding new employees, as well as handling of client and customer data.
5. Likewise, 'official identifiers' include *any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal*. Such numbers may be official ID cards such as Aadhar, PAN, Passport, etc.

² Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International journal of environmental research and public health*, 16(6), 1070. <https://doi.org/10.3390/ijerph16061070>

6. Due to several regulatory requirement the collection of such identifiers is mandatory in nature and has become the norm in terms of practices such as employee background verification and access control measures for infrastructure security. Keeping in mind their ubiquitous usage, and as illustrated above, such categorization for official identifiers would be problematic, especially keeping in mind the limited grounds for processing of sensitive personal data, i.e. solely based on explicit consent of the data principal.
7. All of the above concerns are compounded by the fact that personal, sensitive or critical personal data may be collected from the same source during a single transaction. Companies will be forced to adopt a stricter approach with all types of data, irrespective of their classification. This would defeat the intention of the legislation to prescribe differential requirements based on data classification.
8. Sectoral regulators have powers to provide for conditions of processing of personal data and at-least in the case of financial data, this is already being done. For example, Reserve Bank of India (**RBI**) could provide conditions, including condition of explicit consent for processing of financial information (personal data of users like account details, payment credentials, transaction data, credit history and financial status) as may be deemed appropriate to a wider set of entities where such a condition may be relevant.³ Therefore, treating 'financial information' as an SPD under the PDP Bill 2019 is excessive. It is likely to lead to undue hardship for processing of such information for purposes of employment, contractual obligation, legal compliances etc. It is likely to be excessive for supplier of services, especially small suppliers and unnecessary for large service providers who might be storing some of this data in their global servers.
9. Moreover, the power to classify further categories of SPD and critical data rests with the Central Government. While in the case of SPD, the Government is required to consult the DPA and the concerned sectoral regulator, there is no obligation upon the Government for a public consultation.

Recommendation

The classification of data into three separate categories of data, i.e. personal data, SPD and critical data, in its present formulation is likely to lead to disproportionate costs for enterprises without any meaningful bolstering of privacy rights of data principals. Accordingly, NASSCOM and DSCI recommend that:

- R 1.** The definition of SPD should be made explicit, and limited to such personal data, which could lead to profiling, discrimination and infliction of harm that are identity driven. Financial information is important as in, its breach is likely to result in harm. The remedy against harm is available even if it is not an SPD. This coupled with the ability of sectoral regulators to provide additional safeguards is the basis for us to recommend that 'financial data' should to be removed from the category of SPD. In case of 'official identifier' also, remedy against harm is available even if it is not an SPD. Accordingly, 'financial data' and 'official identifiers' should not be treated as SPD and the definition of 'health data' should be limited to data concerning the health of the person. The definition of SPD should ideally be exhaustive, not subject to regular updation. Should

³ RBI, Frequently Asked Questions, Storage of Payment System Data. This lists out the wide set of financial sector entities to which its payment data storage requirements apply. see: <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130>

the JPC be of a contrary opinion, alternate recommendations (i.e. **R 2** to **R 5**) may be considered.

- R 2.** *Financial data:* In case the JPC is of the contrary opinion, SPD could include an identified sub-set of financial data, which in the opinion of the DPA would suit the definition recommended in **R 1** above. For instance, the subset could be aligned to Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**), where *financial information is said to include bank account or credit card or debit card or other payment instrument details.*
- R 3.** *Health data:* The definition of ‘health data’ should be revised to mean *data concerning health of the person* in line with globally accepted definitions of ‘health data’. It should not cover personal data that may be processed as part of the processing of the health data.
- R 4.** *Official identifier:* In line with the earlier expressed concerns ‘official identifiers’ should be dropped from the SPD classification; alternately, there should be relaxation of the requirement for seeking explicit consent for the processing of ‘official identifiers.’
- R 5.** The power of further classification of SPD should be moved back to the DPA, and there should be a statutory mandate to provide reasons for classifying any ‘personal data’ as SPD, including an account of potential harms that could arise, and a mandate to conduct a thorough public consultation exercise before any personal data is notified as SPD.

II. Restrictive grounds for Processing Personal Data and Sensitive Personal Data (Clause 11 and Clause 12)

The legal grounds for processing personal data under the Bill include: (i) consent, (ii) functions of state, (iii) compliance with law or order of court/tribunal, (iv) for prompt action in case of individual medical emergencies or in case of public health emergency, (v) purposes related to employment, and (vi) reasonable purposes of the data fiduciary. [Chapter III of the Bill]

However, the legal ground for processing SPD under the Bill is restricted to explicit consent alone. [Clause 11 (3) of the Bill] This could be restrictive, and lead to disproportionate costs being imposed upon data fiduciaries even in day-to-day operations.

Illustrative Use Cases

Illustration 1 – Consent Fatigue (Non-Provision of Performance of Contract as ground for processing): Person X is purchasing a car and is looking to purchase associated accessories and services online.

First, Person X makes an online purchase for a smart-car hub. The e-commerce site needs to process the address of the individual in order to deliver the goods and must process Person X’s credit card information to provide him this service. Person X will have to provide his consent for the processing.

Next, Person X decides to do some research on car insurance premiums and requests a quotation from an online financial services company. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car, as well as certain personal data, and details of official identifiers such as whether the insured person has a valid driving license and will accordingly need to obtain the explicit consent of Person X.

Meanwhile, having received his dashboard phone-holder purchased online from Company A, Person X contacts the company because the colour of the product purchased is different from what was agreed upon. The processing of personal data of the customer for the purpose of rectifying this issue is necessary, and will accordingly require consent from Person X.

Following which, Person X provides their postal code to see if a car customisation service provider operates in his area. This processing is necessary to take steps at the request of the data principal prior to entering into a contract pursuant.

Upon receiving the smart-car hub the next day, Person X finds the item to be faulty, and approaches the e-retailer to replace the item as it falls in the warranty period. To initiate the warranty claim, the retailer needs to store certain data for a specified retention time after exchange of goods/services/payment.

Person X had to provide his consent/ explicit consent 5 times in the course of 48 hours.

Illustration 2 – AML Requirements (Need for alternate grounds to processing SPD): Company A, which is based out of Singapore engages Vendor B, an MSME in India for IT services. Company A requires information which includes official identifiers and account information to execute wire transfers to the personal accounts of one of the representatives of Vendor B. Company A, to be able to make such wire transfers, would be required to conduct due diligence in the form of processing and analyzing financial information offshore for AML and CFT purposes. However, Company A will be required to take the explicit consent of Vendor B (which by its definition, is capable of being withdrawn), and for each similarly placed end-user.

Company B, which is also a financial services company, but based out of India, and is accordingly subject to the regulatory requirements relating to KYC and AML as prescribed by the Reserve Bank of India. For this purpose, Company B is required to process SPD such as official identifiers, and other financial information. However, Customer X declines from providing his explicit consent for such processing.

Illustration 3 – Company Day to Day Operations (Need for alternate grounds to processing SPD in the context of employer-employee relationship, and security-based applications): Company B is a global organization, having a workforce in India as well.

Company B would require financial data of employees to be sent offshore for: (i) Managing employee benefits (e.g. financial data provided to payroll providers) (ii) Processing of employees' family members' health data for global benefit and insurance purposes (iii) Background checks – e.g. official identifiers.

Company B believes that the exemption to processing of personal data for employment purposes would enable him to process this data, since consent might not be appropriate given the nature of the employer–employee relationship, which dilutes the consent provided by the employee. However, financial data is SPD, and will be subject to explicit consent of the employee, accordingly, requiring Company B to seek explicit consent for each of the above internal operations.

Similarly, Company B is concerned regarding security and access control measures. In its warehouse, for security purposes it has placed a video surveillance system. Such video cameras capture facial images and gait of the individual entering and exiting the premises.

This type of data would qualify as biometric data and require explicit consent of the persons entering the warehouse. Person X, visiting the warehouse as an external contractor, refuses to give his explicit consent and wishes to pass through the warehouse undetected. Company

B will have to either engage a different external contractor or breach the provisions of the Bill.

Key Concerns:

1. The Bill's emphasis on consent being the nerve centre of the data protection framework is one of the most important aspects of the legislation. However, the reliance on consent for processing personal data in routine transactions where a requested service cannot be provided without processing personal data, would lead to consent fatigue and trivialize the importance of consent, as the user would become accustomed to providing consent for all data collection activities.
2. Given the possibility of consent fatigue, the absence of performance of a contract as a lawful ground to process personal data and SPD could limit the efficacy of the Bill. An alternate ground should be available to the data fiduciary when processing is necessary to deliver the fiduciary's side of the contract with the data principal. The data required to enter into a contract or perform a contract must be within the scope of the contract and services offered. Reading this with the larger transparency obligation on fiduciaries, would prevent any potential misuse and reduce burden on consent for every potential digital exchange between the consumer and the fiduciary. This ground is also recognised under the European General Data Protection Regulations (**GDPR**).
3. Further, the Bill lays down that processing of SPD can be undertaken only on the ground of explicit consent⁴, which is a highly restrictive and onerous threshold, as illustrated above, especially given the expansive definition of SPD that is currently provided under the Bill.
4. For instance, Clause 13 of the Bill does not allow processing of SPD for employment purposes. Processing such SPD would therefore require additional explicit consent. However, the same clause recognises instances where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal⁵ or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing and allows usage of purposes related to employment as a ground for such instances of processing.⁶
5. In real world applications, these instances of imbalance of power in the employee-employer relationship and disproportionate effort are not exclusive to processing of personal data. Processing of SPD such as **financial data** is critical to recruitment processes and payroll services; likewise, **biometric data** processing and usage of **official identifiers** are necessary for access control measures to maintain infrastructure security.

⁴ Clause 11 (3), Personal Data Protection Bill, 2019; The explicit removal of the Chapter relating to Grounds for Processing Sensitive Personal Data without consent, and the inclusion of "explicit consent" under Clause 11(3) of the Bill, renders the interpretation that SPD cannot be processed on any other ground except for explicit consent. Such an interpretation would lead to implementation and compliance issues, as well as defeat the intention of certain alternate grounds provided under Chapter III of the Bill, for example, processing of 'financial data' in the context of an employer-employee relationship.

⁵ Article 29 Working party, [Opinion 2/2017](#) on data processing at work, lays down, "Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer."

⁶ Clause 13 (2), Personal Data Protection Bill, 2019.

6. Requirements such as access control measures are sometimes mandatory requirements from client organisations outsourcing data processing operations. Failure to provide such safeguards could potentially lead to loss of business opportunities for companies as well. Providing an alternative measure to a centralised mechanism for processing of such employee data would lead to disproportionate effort on part of the data fiduciary.
7. Lastly, while the Bill provides for ‘reasonable purposes’ as an alternate ground for processing in the absence of consent, the list of ‘reasonable purposes’ for processing of data under section 14(2) is highly restrictive and requires the DPA to notify the purposes. This negates the prerogative of service providers to self-determine the purposes for which they will require data for the provision of their services and conduct a balancing exercise concerns the rights of the users and the business prerogatives of an organization.
8. The list of ‘reasonable purposes’ does not account for situations such as processing for machine learning or artificial intelligence, that rely on data sets. Processing of data for “legitimate purposes” (as in the case of the GDPR) should be permitted, so that data fiduciaries may self-determine the purposes for which they need to process data. This will help save users from consent fatigue and make compliance easier for the companies.

Recommendation

In order to ensure an effective privacy regime which – (a) avoids creating consent fatigue; (b) enables enterprises’ flexibility, while holding them accounting for all processing activities, the Bill should include additional grounds, apart from consent, (which accompanied with existing accountability and transparency measures), would ensure an effective personal data protection regime.

Accordingly, NASSCOM and DSCI recommend that:

- R 6.** Contractual necessity should be included as a ground for processing of personal and sensitive personal data, and no additional consent should be required for fulfillment of a contractual obligation.
- R 7.** As an individual’s unwillingness to provide explicit consent could lead to a statutory non-compliance for an organisation; compliance with law, or Order of Court/Tribunal, should be added as an alternate ground to explicit consent for the processing of SPD.
- R 8.** The ground for prompt action in case of individual medical emergencies or in case of public health emergency should extend to personal data, as well as SPD. Alternately, a specific carve-out should to be created for the usage of health data or genetic data under this ground, otherwise the intention of creating this ground would be defeated.
- R 9.** Considering the imbalance of power between the employer and the employee to execute valid explicit consent, processing for the purposes of employment, should be an alternate ground for the processing of SPD as well.
- R 10.** ‘Reasonable purposes’ as a ground for processing, should extend to both personal data and SPD. There should not be a blanket usage of this ground. The DPA should come out with a code of practice for how an organisation should carry out a self-determination exercise and document the same as evidentiary proof. Such self-determination should take into consideration the rights of the data principals and carry out a balancing test. A prescriptive list and pre-approved list of purposes would be detrimental for innovation

and would not be flexible enough to stand the pace of technological development and offering personalised services to consumers.

R 11. The grounds relating to ‘functions of the State’ should cover processing of personal data by the State for providing any service or benefit to the data principal from the State; or the issuance of any certification, license or permit for any action or activity of the data principal by the State.

For processing sensitive data, the state should be required to take explicit consent of citizens due to the heightened degree of harm that may be caused to an individual if such sensitive data is misused in any manner.

III. Restrictions and conditions for Cross-Border Transfer of Sensitive Personal Data and Critical Personal Data (Clause 33)

The Bill requires continued storage of sensitive personal data in India, and instances where cross-border transfer of sensitive personal data can happen. It is unclear as to what this requirement entails vis-à-vis manner of storage. In terms of personal data categorised as critical personal data, such data can only be processed in India. Although there are instances where such data can be transferred outside the country, the Bill does not elaborate the nature of such transfers, vis-à-vis the manner of storage of data in India, once such transfer is carried out.

Illustrative Use Cases

Illustration 1 – Fraud Detection (Issues with requiring explicit consent for cross-border transfer of SPD): Employee X conducts fraud across multiple countries which needs to be investigated. Employee X leaves the company and withdraws consent / does not provide consent for the transfer of information (e.g. the evidence of the transfer of monies into his personal bank accounts). Company is hindered in conducting a multi-country investigation which requires the transfer of information to internal or external investigators/auditors who may be in different countries.

Illustration 2 – Fraud Litigation Issues with requiring explicit consent for cross-border transfer of SPD): Person X defrauds Person Y in India. Person X transfers all assets to foreign country and absconds to the said foreign country. Prior to absconding, Person X withdraws consent from entities in India (e.g. banks, Person X’s law firm, auditors) from transferring of Person X’s sensitive personal data (e.g. financial data, official identifier), or does not provide explicit consent for the transfer. This has the effect of hindering Person Y from transferring sensitive personal data required to directly pursue debt recovery or litigation proceedings in the foreign country.

Illustration 3 – Data Centre Disaster Recovery (Issues with restrictions on transfer of critical data): Company X presently stores data in India and Singapore to maintain availability of the said data in multiple locations, so that in case of a disaster, the operations are not permanently affected. One data element that Company X presently stores is categorised as critical data under the Bill and must be stored only in India. Should an unforeseen event such as a natural disaster result in destruction of their Indian data centre, this would lead to permanent loss of such data element.

Illustration 4 – Employee Data Processing (Issues with explicit consent for transfer of employee data for global companies): Company Y is a global organisation with local workforces that travel within India and other countries. They use a global solution to process business travel expenses for workforces across countries. The solution is hosted in another Asian country and requires uploading of employee financial

information to the company's expense reporting systems so that expenses can be accurately accounted for. If a data element of such financial information is notified as critical, Company Y would have to employ a different process for India alone, segregated from its global system. This would be seen as business overhead and operational challenge, and impact competitiveness of India as a destination for global businesses.

Illustration 5 – Employee Data Processing (Issues with explicit consent for transfer of employee data for global companies): Company Z manages offices and employees at multiple locations around the world, employees and contractors are increasingly able to work remotely from any location and companies recruit from an increasingly global talent pool. To manage employees at multiple global offices, company 'y' wants to make use of employee management services based out of Singapore that are world renowned for their services. To make use of this service they must transfer employees' personal data and sensitive data across international boundaries. If a category of sensitive data is classified as critical then it would impact the centralised systems that organisations have created for processing of employee data that leverage global talent and services for providing optimum services to the employees.

Illustration 6 – Employee Data Processing (Issues with explicit consent for transfer of employee data for export-oriented companies): Company A is an India based employee management service provider and has started attracting global clients. To provide this end-to-end service they need access to employees' financial data, health data and their government issued ID cards. Clients from different countries transfer foreign national's data to India to make use of services offered by Company A. If the Central Government were to classify certain data elements associated with financial, health, or official identifier data as critical data, it would have to be stored exclusively in India. This would act as a deterrent for potential clients to pick an Indian service provider.

Key Concerns:

1. The Bill still does not provide any definition of what critical data is, nor does it provide any guidelines for the determination of what may be notified as critical data. This is an area that needs further clarity to create business predictability from an operational standpoint. If a broad class of personal data is classified as critical personal data, this could lead to stringent data localization norms, thereby disrupting businesses. It must also be noted that data cannot easily be disaggregated, with only certain subsets of it stored locally, while other subsets can be freely stored anywhere.
2. Transfer of Critical Personal Data is only permitted to locations that have been deemed "adequate", unless in case of emergencies. Globally, we have learnt that the process of recognising destinations to be adequate for data transfers is time consuming requiring several rounds of Government to Government discussions, that could last for several years. Therefore, until such time that destinations are recognised as adequate, transfer of critical personal data would be completely prohibited, posing challenges for businesses in India.
3. At present, and unlike the case with other jurisdictions, the existence of adequacy decisions or approved standard contractual clauses, are not valid grounds in and of themselves, but require the explicit consent of the data principal in order to validate a cross-border data transfer.

4. As mentioned earlier in **Page 10**, data that is collected by the Industry, is in many cases, a mix of both personal data and SPD. Therefore, the provisions on restrictions on data transfer, although simplified and eased from the previous draft, will offer limited relief, if explicit consent continues to be the primary basis for cross-border transfers.
5. Accordingly, it might be desirable to have standard contractual clauses (model clauses, which do not have to be approved by the DPA on every instance) and binding corporate rules (**BCRs**) as alternative grounds to the processing and transfer of SPD as well. Further, the DPA should give due consideration to existing industry transfer mechanism such as the APEC Cross Border Privacy Rules (**CBPR**) framework.

Recommendation

While acknowledging and addressing the risks associated with cross-border transfers of certain categories of data, the Bill must not over-restrict transfers in today’s global business environment.

Accordingly, NASSCOM and DSCI recommend that:

- R 12.** The classification of Critical Data should be closely linked to the requirements of National Security. This will limit the impact of stringent localisation and offer certainty to businesses in their data processing activities. Till such time countries / destinations are not recognised as adequate, critical personal data transfers may be approved basis standard contractual clauses, with additional safeguards.
- R 13.** The requirement to obtain an additional consent for cross border transfer should be removed, since it would be onerous for companies particularly where there is a huge volume of cross border transfer on a regular basis. Moreover, it would irrelevant to the Bill’s overall intent of effective data processing, since the processing (even in the absence of this additional consent) can only take place based on permitted grounds of processing.
- R 14.** Standard contractual clauses and BCRs based on frameworks such as the APEC Privacy framework and the CBPR should be considered as alternate grounds to processing SPD under the Bill.

IV. Lack of appropriate framework to build trust for processing of global data in India: Power to Exempt certain Data Processors (Clause 37)

Central Government has the power to exempt data processors, that process personal data of data principals outside the territory of India. While this was included in the earlier draft of the Bill as a miscellaneous provision, this has now been included under the Chapter on exemptions under the Bill. However, no material changes have been made to the text. The industry will need greater certainty on the scope and issuance of the exemption.

Illustrative Use Cases

Illustration 1 – Data Analytics Offshoring (Localisation of Foreign National Data): Company A is based out of Singapore and transfers its citizen’s data to India for data analytics purposes to company B. The data transferred to Company B includes the Singapore citizen’s financial transaction history. Company B would be required to continue to store this foreign national’s sensitive data in India.

Illustration 2 – Contractual Data Analytics (Localisation of Foreign National Data): Company X is processing non-personal data of a client organisation pursuant of a contractual relationship between the two. Company X is contractually bound by the data fiduciary and cannot share data (personal or non-personal) or any insights thereof, as they belong to the client of the data processor on whose behalf the data processing entity is conducting data processing activities as per instructions and contract.

Illustration 3 –Conflicting Data Protection Obligations: An EU based company, Company A, transfers EU resident’s data to Company B based out of India. Company B maintains compliance with EU GDPR to legally process such data. As part of compliance requirements, the data needs to be stored for ‘x’ amount of days.

However, under the Bill, Company B maybe asked to store the data for ‘y’ amount of days, which happens to be less than the ‘x’ days required under EU GDPR. Company B is now faced with a situation where the same body of data is subject to two contrary processing obligations.

Key Concerns:

1. There is a need for greater certainty around this provision, especially given the fact that in the absence of transition provisions, there is no guidance on when the obligations under the Bill will be applicable. In a situation where there is no exemption notified, and the remaining obligations under the Bill are notified, several Indian enterprises would be in breach of their obligations vis-à-vis foreign national data.
2. The provision for notified exemption for processors dealing with foreign national data is inadequate. In the absence of upfront exemptions, sensitive personal data and critical personal data being processed in India, will need to be stored in India with provisions for transfer notified as per category (Ref Clause 33, 34).
3. Government can access data from both data fiduciaries and data processors, that includes nonpersonal data/ anonymised data (Ref Clause 91). This will have a huge impact on business confidence of overseas clients and foreign nationals, as they would be apprehensive of Government of India’s access to Foreign national data, especially since the process of access is uncertain.
4. Notification on a case to case basis will disrupt ongoing and upcoming contract finalisation and will impact confidence of clients outsourcing data processing to India.

Recommendation

While acknowledging and addressing the risks associated with cross-border transfers of certain categories of data, the Bill must not over-restrict transfers in today’s global business environment.

Accordingly, NASSCOM and DSCI recommend that:

- R 15.** Upfront exemptions, for organisations’ processing foreign national’s data in India, from select provisions, should be considered. This could be important for India to achieve adequacy status from the EU and other geographies. This will suitably ring fence the applicability of the law, without any discretionary powers and process uncertainty. Accordingly, exemptions in relation of processing of foreign personal data should be explicitly provided in the PDP Bill 2019 for certain provisions, especially those referred below:

- a. Restriction on retention of personal data. (Clause 9, Chapter II)
- b. Restriction on Transfer of Sensitive Personal Data and Critical Personal Data Outside India (Chapter VII)
- c. Act to promote framing of policies for digital economy, etc. (Clause 91)
- d. Bar on processing certain forms of biometric data. (Clause 92)

R 16. In addition, the PDP Bill 2019 should provide that the Central Government may, by notification, exempt the processing of personal data of foreign Data Principals resident outside from the application of any provision of the Act, to the extent that the same is desirable to enable such processing to be in conformity with the requirements of the particular country where the:

- a. Data principals are located; or
- b. Organisation which alone, or in conjunction with others, determines the purpose of processing of personal data is located, or incorporated.

V. Provisions Dealing with Non-Personal Data (Clause 91)

The Bill empowers the Central Government to direct data fiduciaries or data processors to share anonymised personal data or non-personal data for the purpose of enabling better targeting for delivery of services or for the formulation of evidence-based policies by the Central Government.

Illustrative Use Cases

Illustration 1 – Contractual Restrictions (Issues with data-sharing directions issued to data processors): Service Provider ‘A’ is processing non-personal data of a client organisation ‘B1’ pursuant of a contractual relationship between the two. Service Provider A is contractually bound by the data fiduciary (i.e. Organisation B1). Service Provider ‘A’ has similar arrangements with client organisations ‘B2’ and ‘B3’ each of whom are market leaders in industry segment B.

The Government directs Service Provider A to share non-personal data processed by it to enable the formulation of evidence-based policies for industry segment B.

While Service Provider A will be required to comply with the direction of the Government, it will also be face consequential liability under contract, as Service Provider A, cannot share data (personal or non-personal) or any insights thereof, as they belong to the clients (i.e. B1,B2 and B3) on whose behalf the data processing entity is conducting data processing activities as per instructions and contract.

Illustration 2 – Non-Availability of Non-Personal Data (Need for safeguards): Organisation X is a start-up data fiduciary in the healthcare sector that collects and processes personal and sensitive personal data of its customers, in accordance with the provisions of the Bill. All personal and sensitive personal data so collected, including insights derived from such data is treated as personal data, and the Organisation’s data security practices tag and treat the data as such. All personal and sensitive personal data is retained to the extent of processing and deleted subsequently, in accordance with the Bill.

The Government directs Organisation X to share an anonymised personal data set for better targeting of service delivery. However, Organisation X being a start-up had allocated no resources to effective and irreversible anonymisation of personal data or maintained any anonymised personal data sets.

Therefore, Organisation X is not able to comply with the Government's mandate without re-allocating sparse resources towards anonymisation, or with the explicit consent from its customers to share non-anonymised sets.

Illustration 3 – IP Rights and Competition Issues (Need for safeguards for Intellectual Property Rights): Organisation A, which started offering a pre-paid instrument (online wallet) in 2014, integrated other e-Commerce features such as shopping, and micro-credit into its platform after a few years of commencing operation.

It processes significant volumes of data, and can generate insights into popular products, purchase and spend habits, product quality, etc. Organisation A claims intellectual property rights over the non-personal insights generated from the anonymised data sets by way of its proprietary algorithm.

The Government, by notification requires Organisation A to provide anonymised data sets and insights. Upon sharing, the data is subsequently provided to Start-Up A, a FinTech start-up operating in a regulator-led regulatory Sandbox. Start-Up A, trains its credit assessment algorithm using the data set, and compete directly with Organization A.

Organisation A loses its valuation, ahead of a plan to get publicly listed, on account of de-valuation of its assets.

Illustration 4 – Re-identification and De-Anonymisation Risk (Need for accountability and safeguards): Organisation ABX, collects significant amount of sensitive personal data in the healthcare services sector. Other organisations, including Organisation ACX and Organisation ADX, equally collect significant amount of data in the healthcare related financial services sector.

Each of the organisations are required to anonymise the sensitive personal data so collected and share the same with the Government.

While each of these sets is anonymised, Vendor A working with the Government to develop healthcare coverage policies of the Government, is able to develop insights, which on a cumulative assessment of data provided by Organisations ABX, ACX and ADX, leads to the unintended re-identification of the data.

Vendor A could potentially be subject to criminal prosecution on account of Clause 82 of the Bill.

Key Concerns:

1. Companies, large and small, established or start-ups generate non-personal data through their operations, and such data in several instances is proprietary in nature. Similarly, companies have developed tools and techniques to anonymise data, to be used for creation of new products and services. Such data continues to remain protected under intellectual property rights and/ or as trade secret. The concern therefore relates to likelihood of dilution of such protection available through other statutes or through contractual obligations.
2. While it is acknowledged that such non-personal data/ anonymised personal could be of tremendous benefit towards improving public sector delivery of services, and policy making, the commercial and market facing implications of such directions cannot be ignored.

3. There could be, for instance, implications relating to the ability of an enterprise to compete effectively, should such data be required to be shared. In this context, it might be noted that the proposed Draft Competition (Amendment) Bill, 2020, recognising this very interplay between intellectual property rights and competition, extends the exemption available to enterprises with regard to restraining any infringement of, or to impose reasonable conditions, as may be necessary for protecting any intellectual property rights, to both Section 3 (anti-competitive agreements) and Section 4 (abuse of dominant position). This proposed amendment, effectively recognises the commercial value of intellectual property rights, and how instrumental they are in ensuring that an enterprise can compete effectively, while having sufficient incentives to sustain innovation.
4. Moreover, given the statutory recognition of intellectual property rights over intangibles such as patents, designs, copyright, etc., and the recognition granted to contractual rights such as trade secrets, any mandatory sharing of the above-mentioned types of data can be viewed as expropriation. The compulsory acquisition of private property is subject to restrictions placed by the Supreme Court and may only be done under very narrow and limited circumstances.⁷
5. Should the Clause have over-riding effect over all other intellectual property rights related legislation, it may lead to concerns with India's trading partners over the efficacy of intellectual property laws in India and the protection available for trade secrets. Moreover, any apprehension surrounding compulsory licensing or acquisition of data could stifle innovation. As the clause stands, it applies even to offshoring of data processing activities into India and would be a negative consideration for the global industry while evaluating India for such activities.
6. This clause can effectively defeat the intent of the legislation, by bypassing the control of personal data with the data fiduciary and directing a data processor to share anonymised personal data, or non-personal data. Moreover, the obligations of data processors under their contracts with data fiduciaries, typically restrict data processors from sharing, disclosing, or processing data beyond the purposes for which the contracts are intended.
7. Further, the clause could effectively subject enterprises to additional costs by forcing them to acquire technology to irreversibly anonymise personal data, and to prepare and maintain datasets of anonymised personal data and non-personal data. This, notwithstanding the risks of re-identification of the anonymised personal data, for which additional costs will have to be provisioned for.
8. In any event, given that the intent of the legislation does not cover non-personal data under its ambit, and seeks to solely protect personal data, provisions dealing with non-personal data should ideally be left to be dealt with separate legislation.

Recommendation

The Government's powers to direct the sharing of anonymised personal data or non-personal data, should account for the concerns highlighted above.

⁷ *Gilubhai Nanbhai Khachar v. State of Gujarat*, AIR 1995 SC 142

In fact, concerns such as these, were the very reason the Justice Srikrishna Committee left non-personal data out of the ambit of its work and recommended the establishment of a separate committee to consider and make appropriate recommendations on the issue.

In fact, currently, the Kris Gopalakrishnan Committee, set up in 2019 under the aegis of the Ministry of Electronics and Information Technology, is seized with the task of recommending to the Government, an appropriate regulatory framework for non-personal data in India.

Accordingly, NASSCOM and DSCI recommend that:

- R 17.** The provision be removed from the Bill, and issues surrounding non-personal data be left to be dealt with by way of separate legislation.
- R 18.** If included in the Bill, the provision should have appropriate safeguards and governance frameworks built-in, in the form of –
- a. Enterprises that are directed to share such data, being required to establish that intellectual property rights exist, or that such data is otherwise confidential and business sensitive, and that disclosure could significantly harm the enterprises commercial interests and diminish the commercial value of such data.
 - b. The Government being required to ask for a reasonable and proportionate volume of data (such as a sample) and required to clearly specify the ground on which the data is being directed to be shared, including the exact policy towards which such data would be utilised;
 - c. The Government being required to prevent onward disclosure of such data beyond the purposes stated.
 - d. Accountability provisions for the government in this regard.
- R 19.** The Data Protection Authority should have a greater role in ensuring that the provision is exercised only in such instances where the risks of re-identification are minimal.
- R 20.** The State and all State and non-State entities with whom any data is shared must be accountable as to the use and disclosure of the data.
- R 21.** The provision must ensure that data sharing does not lead to dilution of the commercial value of the data, expropriation of intellectual property rights, or breach of contractual liabilities.
- R 22.** A thorough assessment of the costs, benefits, and impact on competition of each direction issued under the Clause, together with a reasoned statement on the intended use of the shared data, and the potential risks of reidentification must be reported clearly and transparently by the Government agency issuing a direction.

VI. Strengthening of framework for an effective and accountable Data Protection Authority

Key Concerns:

1. The DPA has been vested with significant powers and functions, including the power to prescribe rules, regulations and standards regarding the enforcement of the provisions of the Bill. Given this, it is imperative that the DPA be held accountable to explain the rationale of its rulemaking and be open and transparent in its functioning. In the absence, of established principles for rulemaking, there is the risk of erosion of regulatory certainty, *ad-hoc* interventions, and unintended chilling effects on economic activity.

2. Frequent changes based on rules and regulations issued by the DPA will require businesses to overhaul their technical and organisational practices, which could be expensive and cumbersome. Instead, the DPA should rely on self-regulatory efforts (e.g. internal audits, rather than external audits) and market driven efforts (e.g. voluntary mechanisms around trust scores).
3. Given that the Bill applies equally to State and Non-State entities, in ensuring that the DPA is an effective regulator, it is imperative that the DPA be independently funded and staffed, have inbuilt regulatory governance mechanisms.
4. As indicated in other places in the submission, NASSCOM and DSCI believe that principles relating to the functions of the DPA must be set out clearly and unambiguously in the Bill itself. For instance, the question of which data fiduciaries would qualify as a 'significant data fiduciary' or a 'guardian data fiduciary', are threshold questions, which determine the applicability of differential regulatory requirements upon businesses. While admittedly the Bill specifies certain grounds for the DPA to make these determinations, in the absence of clarity as to whether a cumulative assessment of these grounds will be conducted, or whether certain grounds would outweigh the other grounds, makes the applicability of significant portions of the Bill subject to the DPA's discretion. (Refer Part III at Page 26)
5. Moreover, the wide ambit of functions vested in the DPA, and given the significance of the task that would lie before the newly established DPA, it is important that resources be utilised to prioritise key regulatory functions – capacity building, education & awareness, and grievance redressal. Regulatory responsibilities such as approving and monitoring cross-border transfers, are second order regulatory issues, which do not relate directly to operationalising privacy for the data principal.

Recommendation

NASSCOM and DSCI recommend that:

- R 23.** In order to maintain its independence as a regulator, the DPA should be independently staffed and funded. The JPC may consider reviewing the composition of the selection committee for the DPA, the composition of the DPA, and provide for an independent funding mechanism.

The DPA should be advised by domain experts on data protection, privacy, technology and law, and have a hard-coded obligation to consult with industry and other relevant stakeholders including sectoral regulators, so that it can leverage domain expertise.

- R 24.** The Bill should provide for clear and unambiguous principles that should form the basis of the DPA's discharge of functions, including the issuance of rules and regulations; together with the obligation for the DPA to conduct its business in a transparent and consultative manner. While the Bill provides for DPA to undertake consultations, the process of undertaking consultation should be provided in the law. The recommendations of the Financial Sector Legislative Reform Commission (FSLRC) on regulatory governance as encoded in the draft Indian Financial Code

should be used as a reference and similar provisions should be drafted in the PDP Bill 2019. *A model consultative process is suggested.*⁸

VII. Lack of appropriate grading of Criminal Offences

Key Concerns:

1. While the Bill does drop certain offences (i.e. regarding obtaining, transferring or selling of personal and sensitive personal data), the remaining offence with regard to the re-identification of anonymised personal data is non-bailable, and the punishment does not appear to have been graded proportionately to the nature of the offence.
2. Conditions of cognizable and non-bailable punishment under the Bill are extremely harsh and will impact the sentiment of the Industry. There is apprehension of misuse, compounded by lack of understanding of technology and its working, as Data related offences are investigated. Instead, practical requirements combined with monetary compensation and conduct remedies are adequate to protect privacy interests of data principal
3. An expansive definition of ‘significant harm’ under the Bill, coupled with steep monetary penalties, should serve as sufficient deterrent against re-identification of anonymised personal data. Attaching additional criminal liabilities is therefore disproportionate to the objectives sought to be achieved by the Bill and may have an unintended chilling effect on innovation in the industry – in terms of reluctance to work with any manner of anonymised data altogether. The risk of imprisonment is likely to result in companies avoiding India as a potential market, which would harm the Indian economy and consumers.

⁸ 1. Before making any regulation or code, the DPA shall approve and publish a draft of such regulation, accompanied with a statement setting out,-

- (a) the objectives of such proposed regulation/ code;
- (b) the problem that such proposed regulation/ code seeks to address;
- (c) how solving this problem is consistent with the objectives of the DPA under this Act;
- (d) the manner in which such proposed regulation/ code will address this problem;
- (e) the manner in which such proposed regulation/ code complies with the provision of this Act under which such a regulation/ code is made;
- (f) an analysis of costs and an analysis of benefits of such proposed regulation/ code as far as possible; and
- (g) the process by which any person may make a representation in relation to such a proposed regulation/ code.

2. The DPA shall, –

- (a) give a time of not less than twenty-one days to enable any person to make a representation in relation to such a proposed regulation/ code; and
- (b) consider all representations made to it within such time as may be specified.

3. The DPA shall publish, –

- (a) all the representations received by it under sub-section (2) of this section; and
- (b) a general account of the response of the DPA to the representations.

4. If a regulation/ code made differs substantially from such a proposed regulation/ code, the DPA, in addition to the requirements of

sub-section (2) of this section, shall also publish, –

- (a) the details and reasons for such difference; and
- (b) an analysis of costs and an analysis of benefits, of the differing provisions.

5. The DPA shall review every regulation/ code of this Act within three years from the date on which such regulation/ code is notified.

Recommendation

NASSCOM and DSCI recommend that:

- R 25.** The Bill should remove criminal liability for contraventions of the provisions of the Bill and limit the circumstances for individual liability to situations in which it is proven that the relevant individual possesses an appropriate level of culpability for alleged violations. Given that some of the processing steps could involve new technology, and there may be good faith processing interventions that hinge on subjective opinions, an efficient enforcement mechanism with monetary relief would ensure that the rights of data principals and the interests of fiduciaries and processors are protected.

Part 3

Areas Requiring Clarification

I. Provisions relating to Significant Data Fiduciaries [Clauses 26, 27 and 30]

Key Areas Requiring Clarification:

1. **Discretion with the DPA to classify Significant Data Fiduciaries** – There is a need for further clarity on the way the DPA is required to classify “significant data fiduciaries”. Further clarity is required as to –
 - a. Whether the DPA will be required to do a cumulative assessment of the factors listed under Clause 26(1), or whether the existence of either of the factors would be enough in the DPA’s determination.
 - b. Whether in case the DPA is required to undertake a cumulative assessment of the factors listed under Clause 26(1) of the Bill, all factors will be given equal weightage, or will they be attributed differential weightages.
 - c. Whether the assessment of whether a data fiduciary is a ‘significant data fiduciary’ will be carried out at the level of a product line, an enterprise, or a group of enterprises.
 - d. Whether the DPA’s decision will be subsequent to a hearing afforded to a data fiduciary, and whether the DPA’s decision will be subject to any review, revision, or appeal.

Recommendation: It is recommended that the Bill provide abundant clarity regarding the grounds and processes for classifying ‘significant data fiduciaries.’ In particular, the JPC should consider clarifying that a **cumulative assessment** of the factors listed under Clause 26(1) be carried out, since the existence of any one single factor cannot be a standalone indicator of the likelihood of ‘significant harm.’

Further it should be clarified, that the classification of significant data fiduciaries, will be done based on the **nature and extent of an enterprise’s activities in India**, in order to minimise the risk of disproportionate regulation.

To illustrate, Company A (part of global group of companies Group ABC) operates in India as a data processor alone. However, as a large-scale data processor, it employs close to 3000 employees in India. Company A, vis-à-vis its employees, is a data fiduciary, however, that alone cannot be the grounds to designate a *data processor as a ‘significant data fiduciary.’* Neither can the fact that companies of Group ABC act as large data fiduciaries in other jurisdictions, justify the classification of a data processor as a ‘significant data fiduciary.’

Lastly, given the significant and differential regulatory obligations case upon ‘significant data fiduciaries’, it should be clarified that the decision of the DPA would be based upon **due notice to the concerned data fiduciary, the consideration of submissions from the data fiduciary, and procedures subject to the rules of natural justice**. The JPC may also consider the **inclusion of a right of appeal** against the decision of the DPA in this regard, before the Appellate Tribunal.

2. **Appointment of Data Protection Officer** – A significant data fiduciary is required to appoint a Data Protection Officer (**DPO**) in the territory of India. The DPO is supposed to act as the representative of the data fiduciary and monitor compliance with the law. Clarity is required, as to –
 - a. Whether the office of the DPO is independent, and adequately safeguarded to prevent any potential conflicts of interest, especially since the Bill mentions that the fiduciary can give the DPO additional duties – which could in certain circumstances confront the DPO with competing objectives.
 - b. Whether the DPO and Chief Information Security Officer (**CISO**)’s offices would be separate. This is imperative, given that some security controls may lead to invasion of an individual’s privacy and there could be conflict of interest in reviewing/deciding on such security controls from data privacy standpoint.
 - c. Whether the appointment of the DPO must be undertaken afresh, even in instances where a global DPO is appointed with the specific mandate of ensuring compliance with data protection laws in India, including the provisions of the Bill.
 - d. Whether the DPO function can be outsourced to an independent office outside the organisation (as is allowed under the GDPR), to avoid both conflicts of interest, and cost effective compliance steps.

Recommendation: It is recommended that the Bill be unambiguous in its statement that the office of the **DPO must be an independently functioning office**, that is ring-fenced from any potential conflicts of interest.

In doing so, the Bill should clarify that the Office of the DPO and that of the CISO should be separate, and that an existing DPO, or an external independent DPO office would suffice for the purposes of compliance, as long as the criteria for independence of the office, and the scope of their functions are aligned with what is prescribed under the Bill. In any event, organizations should be given some time to recruit and appoint a DPO.

3. **Data Audits** – A significant data fiduciary is required to have its policies and the conduct of its processing of personal data audited annually, by an independent data auditor.

Additionally, **any data fiduciary** (not being a significant data fiduciary) may also be subjected to a data audit in case the DPA deems it necessary to find if any processing of personal data has harmed or may cause harm to data principal.

In this regard, further clarity is required as to **whether there are any specific grounds basis which an audit may be directed, and whether an opportunity of being heard would be provided to the data fiduciary, before being directed to conduct an audit.**

Recommendation: It is recommended that the Bill expressly clarify the process of issuance of audit directions by the DPA.

In particular, the DPA should be required to specify the precise grounds based on which it may issue directions, and the data fiduciary must be given an opportunity to be heard before being directed to conduct an audit.

II. Change in the definition of Personal Data [Clause 2(28)]

Key Areas Requiring Clarification:

1. The definition of ‘personal data’, which continues to be wide, has been *inter alia* amended to include “inferences drawn from personal data for the purposes of profiling.” Given the significant compliance changes across industries that will flow from the Bill, the lack of certainty around what these inclusions mean, could lead to unintended consequences. In particular, it is not certain as to –
 - a. Whether the reference to inferred data relates to all insights inferred from the data being processed. The definition could have significant implications in terms of the business interests of enterprises regarding inferred and derivative data.
 - b. Whether the definition of ‘personal data’ would apply to natural persons (thereby including deceased natural persons) or only to living natural persons (as is the case with the GDPR)

Recommendation: In order to avoid any unintended consequences of subjective interpretation, it is recommended that the Bill replace the reference to “inferences drawn from personal data” and replace it with “**de-identified data used for the purpose of profiling.**” This would ensure clarity over the fact that inferences and insights based on anonymised personal data will not be included within the scope of the Bill. Additionally, the JPC may **consider specifying a few illustrative personal data elements** (e.g. identifiers, location data, etc.) in order to aid organisations in personal data identification. Lastly, the JPC should consider clarifying whether the Bill would apply to the personal data of “living natural persons” or to the personal data of “deceased natural persons” as well.

III. Preliminary Clauses [Transition Provisions and Territorial Applicability]

Key Areas Requiring Clarification:

1. **Territorial Applicability** – At present, the Bill states that its provisions apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is *in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India.*

The jurisdiction of the law should be clear and easy to interpret, especially with respect to extra-territorial application. The issues around applicability have been a source of debate and have emerged as one of the major challenges that NASSCOM and DSCI members have faced during the first year of enforcement of the EU GDPR. Vagueness in drafting would invariably create a multitude of issues for organisations operating in the international digital ecosystem. At the moment, an enterprise operating in EU can only rely on guidance issued by European authorities to ascertain as to how one can establish that goods or services are being specifically targeted towards data principals within the defined territory.

Recommendation: The JPC should consider clarifying the scope of extra-territorial applicability by including illustrations to display the scenarios of extra-territorial applicability of the Bill, and provide illustrative instances to establish if goods or services are being offered to data principals in India, in a systematic manner.

2. **Transitional Provisions** – The Bill excludes transitional provisions provided for in the earlier draft. Even in the earlier draft, the industry had made known the need for enough time to implement changes to their business models, in order to ensure effective compliance with the provisions of the Bill. Accordingly, there is a need for further clarity from the Central Government as to the way in which various provisions will be brought into force, so that the industry is able to achieve meaningful compliance. At the moment, it is not clear from the Bill as to whether:
 - a. Adequate time will be provided for the implementation of the provisions of the Bill. It must be noted that around 2 years’ time was provided for the implementation of the provisions of the GDPR, even though most companies were already in compliance with a wide-ranging European Privacy Directive.
 - b. The Bill accounts for the fact that the implementation of the privacy regime put forth by the Bill, will be a much-needed fresh start for regulators and for domestic industry, especially since this Bill has cross sectoral impact and will require variety of industries and institutions ranging from automotive, retail, oil & gas, PSUs, power companies, health services, State and Central government departments, and many others to learn and comply.

Recommendation: The JPC should consider specifying in the Bill, a **minimum compliance period of 24 months**, from the date of notification of any obligation, standard, code of practice or rule. This period should exclude the stakeholder consultation period that the Authority needs to undertake before notification of such section, standard, code of practice or rule. A phased introduction plan should **provide for timelines for formation of the DPA** given especially, the significant scope of responsibilities vested upon the DPA, in terms of giving shape to several substantive compliance requirements under the Bill. Lastly, for data processors dealing with foreign national data, there might be a need for additional timelines, as they would require international contract re-negotiations.

IV. Other Compliance Issues [Privacy by Design Policy, Data Principal’s Right to Correction]

Key Areas Requiring Clarification:

1. **Privacy by Design Policy** – The earlier draft of the Bill, intended for enterprises to embed “privacy by design” in their organisational and business practices. However, the Bill in its present form replaces these obligations (under Clause 22) with the approval and publication of a “privacy by design policy”. There is no clarity as to whether these certification and disclosure requirements would apply at the level of a product line or process, or at the level of the organisation as a whole.

In this regard, it is noted that companies have a variety of processes and corresponding systems for processing personal data, both as a fiduciary and processor. If a “Privacy by Design Policy” is required to be certified and published for each of such processes/system, then it would be challenging. Illustratively, some of the various

processes in a company are –Recruitment, Employment, Information Security, Visitor Management, Sales, Marketing, Information Technology, Project delivery etc.

This becomes particularly problematic, since there is no clarity as to whether such a policy should contain granular descriptions of business practices and technical systems of the data fiduciary.

As technology companies develop products, privacy and security by design are essential features of offerings that offer significant competitive advantage. Disclosures of technical systems that ensure privacy by design could in effect lead to disclosure of trade secrets and confidential business-sensitive information.

Recommendation: The JPC should consider adopting the approach to “privacy by design” as contained in the earlier draft of the Bill, i.e. the DPA should issue broad guidelines and specify the objectives and should permit data fiduciaries to formulate their own policies, as long as such objectives are met.

2. **Data Principal’s Right to Correction** – The right to correction has been expanded to include “erasure”. A new sub-clause (1)(d) has been included to provide that subject to the conditions and specified by the Authority, the data principal shall have the right to “the erasure of personal data which is no longer necessary for the purpose for which it was processed.”

In terms of technical data protection nomenclature, ‘erasure’, refers to a complete removal of all copies of the data principal’s personal data from the organisational ecosystem. This is also known as the “Right to Erasure” under the GDPR.

From the previous version of the Bill and the Report of the Data Protection Committee it is abundantly clear that a ‘right to erasure’ (akin to the GDPR) has been incorporated as the ‘right to be forgotten’ in the Bill.⁹ Accordingly, it would be useful to clarify that the right to correction refers to ‘deletion’ and not ‘erasure’ of such personal data.

Recommendation: The JPC should consider replacing the term ‘erasure’ with the term ‘deletion’ and provide a corresponding definition for ‘deletion’ in order to lend guidance as to the extent of deletion to be achieved. Further, the data fiduciary should be allowed to reject such requests if it’s in contravention with an existing law that requires data to be stored for a certain time period.

V. Other Issues Requiring Clarity [Processing of Biometric Data, Definition of Harm and Financial Institution]

Key Areas Requiring Clarification:

1. **Processing of Biometric Data** – The Bill prohibits the processing of such biometric data, as the Central Government may notify, unless such processing is expressly permitted by law. If Biometric data such as fingerprints, facial scans, retina scanning etc., are notified as prohibited for processing, then it may lead to concerns related to security related processes for organisational infrastructure protection, employee attendance, payment authentication, etc. This could also severely impact start-ups and other social sector enterprises aiming at providing services geared towards financial

⁹ Data Protection Committee Report, page 78 ([accessible here](#)) ; “The Committee is of the view that permanent deletion of personal data from storage should not be a part of this right.”

inclusion, and healthcare services. Lastly, it may cause significant uncertainty for enterprises currently relying upon biometric data for various products – including localised security protocols on devices.

Recommendation: The JPC should consider lending more clarity by specifying the biometric data that can be used in the Bill itself, keeping in mind the significant benefits of biometric data processing – particularly in security applications.

2. **Definition of Harm** – The Bill currently provides “loss of employment” as one of the instances of harm that can be caused to a data principal. However, this inclusion could lead to inconsistencies with existing labour legislation, as well as other specific legislation.

For the purpose of employment related services, benefits to employees, etc. organisations need to process SPD such as financial data and health data. Such processing, and decisions resulting from such processing, should not come under the definition of “harm”, especially since employers should retain the right to make an assessment based on processing of certain data (e.g. health data), as to whether a potential employee would be fit to discharge the employment effectively. Moreover, specific legislation already prohibit discrimination based on certain types of SPD, e.g. the Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995, the Industrial Employment Standing Orders Act, 1946, Maternity Benefits Act, 1961, etc.

Recommendation: The JPC should consider clarifying that “loss of employment” alone would not be sufficient to establish harm, but rather “loss of employment, based on processing that is *ex-facie* discriminatory and contrary to laws for the time being in force.”

3. **Definition of Financial Institution** – As discussed earlier, the Bill defines ‘financial data’ as *‘any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.’*

However, the Bill does not define the term ‘financial institution.’ While guidance can be sought from other legislation defining the term, the closest definition available under the Reserve Bank of India Act, 1934, is framed in the context of non-banking institutions. The lack of a clear definition of the term under the Bill, could therefore bear the risk of misinterpretation, and leave out other institutions such as banking institutions, and payment service providers, from the ambit of the definition.

Recommendation: In tune with our recommendations regarding the classification of ‘financial data’ it might be helpful for the JPC to provide an exhaustive definition of ‘financial institution’, and consider providing a limited definition of ‘financial data’ extending to an identified sub-set of financial data, aligned with the current classification under the SPDI Rules.

Part 4

Clause-by-Clause Remarks

S. No.	Provision	NASSCOM-DSCI Remarks
Preliminary and Definitions (Chapter I)		
1.	Clause 1 of the Bill removes references to transitory provisions (including ‘Chapter XIV’ of the earlier draft of the Bill); Further, references to the geographical scope of the Bill has been removed, presumably on account of extra-territorial applicability of the provisions of the Bill.	Refer to <i>Part 3: Areas Requiring Clarification, under III. Preliminary Clauses, at Page 28.</i>
2.	Clause 2(B) of the Bill adds a carveout for anonymised personal data, by introducing Clause 91 enabling the Central Government to direct the sharing of anonymised personal data or non-personal data for the purposes of better targeting of delivery of services or for evidence-based policymaking.	Refer to <i>Part 2: Major Concerns, under V. Provisions Dealing with Non-Personal Data, at Page 19.</i>
3.	Definition of “Anonymisation” updated to specify that Authority will specify “ <i>standards of irreversibility</i> ”	<p>Given the fact that the provisions of the Bill do not apply to anonymised personal data, and Clause 91 of the Bill envisages the sharing of anonymised personal data, significant risks could remain, in terms of re-identification of data (which is a criminal offence under the Bill at the moment). Therefore, the importance of high levels of anonymisation cannot be understated.</p> <p>We appreciate the Bill recognising the role to be played by the DPA in setting the baselines and standards for achieving effective anonymisation.</p> <p>Further, we reiterate the importance of codes of practices that will be developed in this regard, in consultation with the industry, in order to ensure that such standards are both technically feasible and effective in preventing re-identification, given existing technologies.</p>
4.	Under Clause 3(15) of the Bill, the definition of “data processor” has been updated over the previous draft, to drop the phrase “ <i>but does not include an employee of the data fiduciary.</i> ”	It is unclear whether the effect of this deletion is that employees of data fiduciaries will be included within the ambit of the definition and could be considered as data processors.

S. No.	Provision	NASSCOM-DSCI Remarks
		We recommend that the deleted phrase be retained in order to avoid interpretational ambiguities.
5.	Definition of “Explicit Consent” has been dropped and has instead been provided under Clause 11(3) detailing the grounds for processing SPD.	Refer to <i>Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11.</i>
6.	Clause 3(28) of the Bill, amends the definition of “personal data” over the previous draft to include data, “ <i>whether offline or online</i> ”, and “ <i>any inference drawn from such data for the purpose of profiling</i> ”	Refer to <i>Part 3: Areas Requiring Clarification, under II. Change in Definition of Personal Data, at Page 28.</i>
7.	<p>Definition of “sensitive personal data” under Clause 3(36) of the Bill, has been amended to:</p> <ul style="list-style-type: none"> a. Remove reference to “passwords”; b. Shifting the power to specify further categories of SPD from the DPA to the Central Government, by referencing Clause 15 of the PDP Bill. c. Include definitions for “intersex status” and “transgender status” in the Explanation (these were earlier separate definitions) 	<p>We welcome the rationalisation of the categories of SPD under the Bill.</p> <p>For detailed comments on data classification and its consequential impact, refer to <i>Part 2: Major Concerns, under I. Categories of Sensitive Personal Data and its Consequent Impact, at Page 7.</i></p>
Obligations of Data Fiduciary (Chapter II)		
8.	Clause 9 of the Bill relating to “data retention” has been amended over the previous draft of the Bill. While earlier the retention was for such periods “ <i>as may be reasonably necessary</i> ”, the provision (under sub-clause (1)) has been amended to make retention for the “ <i>period necessary</i> ” and adding “ <i>shall delete the personal data at the end of processing</i> ”. Further, longer data retention periods can now be maintained on (a) the basis of explicit consent of the data principal; or (b) on account of statutory obligations.	<p>We welcome the edits. The carve out for the longer retention period based on explicit consent or for complying with statutory obligations removes conflicts with statutory retention period under other applicable laws.</p> <p>We recommend that a similar process of harmonisation be undertaken for other obligations under the Bill, which may cause potential conflicts with compliance obligations under existing laws.</p>

S. No.	Provision	NASSCOM-DSCI Remarks
9.	Clause 10 of the Bill, relating to accountability of data fiduciary, has been amended over the previous draft of the Bill (earlier Clause 11) to delete sub-clause (2), which provided <i>“The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.”</i>	<p>It is not clear whether the deletion of the earlier sub-clause (2) removes the opportunity for data fiduciaries to establish compliance with Clause 10.</p> <p>It should be clarified that appropriate opportunity for hearings before the DPA on actionable provisions, would include an opportunity to demonstrate that processing activities undertaken are compliant with the provisions of the Bill.</p>
10.	Clause 11 of the Bill, includes a new sub-clause (3), added in lieu of the deletion of the earlier Chapter IV. The new sub-clause (3) provides that in the case of SPD, processing shall be based on explicit consent.	<p>The explicit removal of the Chapter relating to Grounds for Processing Sensitive Personal Data without consent, and the inclusion of “explicit consent” under Clause 11(3) of the Bill, renders the interpretation that SPD cannot be processed on any other ground except for explicit consent.</p> <p><i>As detailed in Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11; such an interpretation would lead to implementation and compliance issues, as well as defeat the intention of certain alternate grounds provided under Chapter III of the Bill, for example, processing of ‘financial data’ in the context of an employer-employee relationship.</i></p>
Grounds for Processing Personal Data without Consent (Chapter III)		
11.	Clause 13 of the Bill (Clause 16 of the earlier draft) relating to exemption on employment-related personal data, has been amended to clarify that it excludes SPD of employees.	<p>As mentioned at Point 10 above, the exclusion of SPD from the ambit of Clause 16 could cause implementation and compliance hurdles.</p> <p><i>Refer to Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11, for detailed submissions in this regard.</i></p>
12.	Clause 14 of the Bill (i.e. Clause 17 of the earlier draft concerning “reasonable purposes” has been amended to include the item <i>“operation of search engine”</i> as an indicative reasonable purpose under sub-clause (2).	<p>The introduction of “operation of search engine” is a positive addition to list of “reasonable purposes” for which personal data may be processed.</p> <p><i>Refer also to detailed submissions on grounds for processing at Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11.</i></p>

S. No.	Provision	NASSCOM-DSCI Remarks
13.	The remainder of the earlier Chapter IV (dealing with grounds of processing of SPD without consent) has been deleted.	Please refer to remarks at points 10 and 11 above; and <i>Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11.</i>
14.	<p>Clause 15 of the Bill (i.e. Clause 22 of the earlier draft) has been amended to:</p> <p>a. Shift the power to specify additional categories of SPD from the DPA to the Central Government, in consultation with the Authority and the sectoral regulator concerned.</p> <p>b. Additional safeguards and restrictions in the case of repeated, continuous or systematic collection, now does not apply to “personal data” but only “sensitive personal data for profiling”.</p>	<p>We welcome the edits restricting the applicability of additional conditions to only “collection of sensitive personal data for profiling”</p> <p>For detailed submissions on data classification, refer to <i>Part 2: Major Concerns, under II. Restrictive Grounds for Processing Personal Data and Sensitive Personal Data, at Page 11.</i></p> <p>While we appreciate inclusion of the obligation of consulting the DPA and the relevant sectoral regulator prior to classifying personal data as SPD, we however reiterate that frequent updation to the categories of SPD could have unintended consequences on the technology and innovation ecosystem in India, especially given the higher and differential compliance requirements applicable for SPD.</p>
Personal Data and Sensitive Personal Data of Children (Chapter IV)		
15.	<p>Clause 16 of the Bill deals with the processing of personal data and SPD by data fiduciaries, who by reason of processing such data, are designated as ‘guardian data fiduciaries’ under the Bill.</p> <p>The provisions apply to the personal data and SPD of data principals who have not attained majority (i.e. below 18 years of age, as prescribed under the Bill)</p>	<p>The specification of age of majority as 18, is not aligned with the contemporary landscape of digital awareness and capabilities of children, who are exposed to a digital ecosystem early in their lives through various educational and support-based applications.</p> <p>While it is up to the JPC to consider aligning this to global standards, i.e. 16 years of age, what is imperative is to clearly and unambiguously specify age-verification mechanisms.</p> <p>Given that there are significant and differential obligations applicable to ‘guardian data fiduciaries’ under the Bill, the DPA must develop effective and technologically feasible standards in consultation with the industry through codes of practice, in order to render certainty to enterprises that will be treated as ‘guardian data fiduciaries.’</p>

S. No.	Provision	NASSCOM-DSCI Remarks
		Please refer to <i>Part 2: Major Concerns, under VI. Data Protection Authority, at Page 22</i> on the role of the DPA in this regard.
Data Principal Rights (Chapter V)		
16.	Under Clause 17 of the Bill, dealing with the right to confirmation and access, a new sub-clause (3) provides that <i>“the data principal shall have the right to access in one place the identities of the data fiduciaries 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.”</i>	<p>The provision appears to point to the creation of a “consent-dashboard”. We understand that this in itself would translate into an obligation upon data fiduciaries to provide such facilities either on their own, or through a “consent manager” (Refer to Point 20 below), which allows companies to take a cost-based decision and affords flexibility.</p> <p>This is a novel concept, that puts the focus on operationalising the data principals’ choice and control over their personal data.</p> <p>However, additional clarity will be required regarding the modalities of the functioning between a consent manager and another data fiduciary, given especially, that in certain circumstances, a “consent manager” (which by definition is a data fiduciary) may be acting in the capacity of a data processor, while offering a consent-dashboard as a service to another data fiduciary.</p>
17.	The right to correction under Clause 18 of the Bill has been expanded to include a “right to erasure”. A new sub-clause (1)(d) has been included to provide that subject to the conditions and specified by the Authority, the data principal shall have the right to <i>“the erasure of personal data which is no longer necessary for the purpose for which it was processed.”</i>	Refer to <i>Part 3: Areas Requiring Clarification, under IV. Other Compliance Issues, at Page 29.</i>
18.	Clause 19 of the Bill provides for a data principal’s right to be provided her personal data in a machine readable and interoperable format. Further, in this Bill, the right has been qualified and has been limited to instances where <i>“the processing has been carried out through automated means”</i> thereby leaving manual processing of personal data outside the scope of the right to portability. Further, an	<p>The inclusion of the right to data portability, is in line with other jurisdictions, such as Europe. However, this has been widely acknowledged as one of the most difficult rights to implement meaningfully.</p> <p>Given that the right extends to data and linkages drawn by data fiduciaries to establish inferred relationships between two or more data principals, the exercise of the right by a data principal, may come in conflict with the rights of another data principal.</p>

S. No.	Provision	NASSCOM-DSCI Remarks
	<p>amendment has been made to sub-clause (1)(a) and the reference to “<i>personal data relatable to the data principal</i>” has been removed and has instead been referred to in sub-clause(1)(a)(i) which deals with “<i>personal data provided to the data fiduciary.</i>”</p>	<p>Accordingly, the JPC should consider limiting this right to the personal data actively and knowingly provided by the data principal, and data that is observed solely by virtue of the data principal’s use of the service or product (i.e. generated data).</p> <p>However, data which is inferred or derived, not by virtue of the data principal’s use of the service or product, but rather by the data fiduciary’s assessment of personal data provided by the data principal (i.e. inferred or derived data) should be left out of the scope.</p> <p>Lastly, regarding the inclusion of “inferred data” within the scope of ‘personal data’, refer to <i>Part 3: Areas Requiring Clarification, under II. Change in Definition of Personal Data, at Page 28.</i></p>
19.	<p>Clause 20 of the Bill includes a new sub-clause (5), which has been inserted to afford a right of appeal to any aggrieved person before the Appellate Tribunal against the order of the Adjudicating Officer regarding the right to be forgotten. This is in addition to the right to request a review of the Adjudicating Officer’s decision.</p>	<p>We welcome the inclusion of a right to appeal against the decision of the Adjudicating Officer.</p>
20.	<p>Under Clause 21 of the Bill, amendments have been made over the previous version, to the provisions on general conditions for the exercise of data principal’s rights –</p> <ol style="list-style-type: none"> a. Reference has been added to “consent manager” in sub-clause (1) for the exercise of rights barring the right to be forgotten. b. The remaining sub-clauses (2) to (5) have been broadly retained, with modalities left to be specified through regulations by the DPA. 	<p>This addition provides a new business model layer for entities that can provide for interoperable consent dashboards for other data fiduciaries.</p> <p>While this is welcome, there remains the need for further clarity around the modalities of the relationship between a data fiduciary and a third-party consent manager.</p> <p>(Also refer to Point 16 above, and Point 22 below)</p>

S. No.	Provision	NASSCOM-DSCI Remarks
Transparency and Accountability (Chapter VI)		
21.	The concept of “privacy by design” as contained in the earlier draft, i.e. that the Chapter II principles were to be embedded in the organisational and business practices of an organisation, has been changed. In its place, there is a requirement to prepare and get certified by the Authority, a “Privacy by Design Policy”, and publish the same upon certification.	Refer to <i>Part 3: Areas Requiring Clarification, under IV. Other Compliance Issues, at Page 29.</i>
22.	<p>Amendments have been made to the transparency obligations of a data fiduciary under the new draft. These include (Clause 23 of the PDP Bill):</p> <p>a. The phrase “reasonable steps” has been substituted with “necessary steps”</p> <p>b. New sub-clauses (3) to (5) have been included to introduce the concept of “consent managers”; the criteria for registration of “consent managers” will be specified by the Authority. The explanation, elaborates upon the definition of “consent managers” and provides that, “a “consent manager” is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.”</p>	<p>The PDP Bill introduces a concept of data fiduciaries getting registered as “consent managers”. This voluntary requirement is for those data fiduciaries who wish to provide for interoperable “consent dashboards” which enable the data principal to access, manage and withdraw the consent provided to multiple data fiduciaries.</p> <p>As mentioned at Point 16 above, given that this introduces a new layer of actors, who could act both as data fiduciaries and data processors, there is a need for greater clarity on the nature and modality of relationships between two or more fiduciaries, with one acting as a consent-manager.</p>
23.	Clause 28 of the Bill, i.e. the provision on record keeping obligations has been amended to include new provisions for “social media intermediaries”, obligating such intermediaries to provide for a voluntary self-verification procedure for their users in such manner as may be prescribed by Rules to be issued by the Central Government. Such users will have	<p>This inclusion is a limited obligation for social media intermediaries. While it is mandatory for social media intermediaries to provide a facility for voluntary self-verification by users, it is not mandatory for users to self-verify.</p> <p>We appreciate the inclusion, given the effectiveness this may have in tackling issues of misinformation and cyber bullying.</p> <p>However, it is important that this requirement be made a voluntary process, and not a</p>

S. No.	Provision	NASSCOM-DSCI Remarks
	to be demarcated on the platform as being verified users.	mandatory requirement for self-verification by all social media users, as it would require significant product alterations, and increase the risk of surveillance.
24.	Clause 29 of the Bill, i.e. the provision on data audits has been amended over the previous version of the Bill to make it explicitly applicable to “significant data fiduciaries”, and the scope of the audit has been extended to the obligations imposed upon “social media intermediaries” under Clause 28(3) i.e. enabling voluntary self-verification.	<p>We believe this clarification has been included to limit the obligation to conduct data audits to only such data fiduciaries that are designated as “significant data fiduciaries.”</p> <p>However, there remain concerns with the data audit process, which have been detailed at <i>Part 3: Areas Requiring Clarification, under I. Provisions relating to Significant Data Fiduciaries, at Page 26.</i></p>
<p>Restrictions on Cross-Border Transfer of Personal Data Outside India (Chapter VII)</p>		
25.	<p>Restrictions on the transfer of personal data have been removed under Clause 33 of the Bill.</p> <p>Further, the restriction on cross-border transfers has been limited to sensitive personal data only, subject to the same requirement as earlier, that such sensitive personal data must continue to be stored in India (similar to the earlier requirement of having one serving copy of such data in India).</p> <p>The provisions regarding critical personal data remain, and critical personal data must continue to be processed within India. However, the grounds for notifying critical personal data, i.e. necessity or strategic interests of state have been removed.</p>	<p>We welcome the removal of restrictions on cross-border transfers of personal data under the Bill.</p> <p>Please refer to <i>Part 2: Major Concerns, under III. Restrictions and conditions on Cross-Border Transfer of Sensitive Personal Data and Critical Data, at Page 15.</i></p> <p>Lastly, we request the JPC to clarify whether for the purposes of technical compliance, the rewording, i.e. “continue to be stored in India” would require a live mirroring of all SPD so transferred, or a mere storage of a copy of the SPD within India. We recommend that this requirement be removed altogether for reasons and use-cases highlighted in this submission.</p>
26.	<p>Given that “explicit consent” is the only ground for processing of sensitive personal data, the new Clause 34 of the Bill, requires “explicit consent” as the first precondition, in addition to the other substantive conditions that remained in the earlier draft. Additionally,</p> <p>a. It has been clarified that “critical personal data” can be</p>	<p>Please refer to <i>Part 2: Major Concerns, under III. Restrictions and conditions on Cross-Border Transfer of Sensitive Personal Data and Critical Data, at Page 15.</i></p>

S. No.	Provision	NASSCOM-DSCI Remarks
	<p>transferred outside for prompt action grounds, or to such countries where the Central Government is of the opinion that transfer will not prejudicially affect the security or strategic interests of the state.</p> <p>b. The obligations to periodically report on the compliance of intra-group schemes has been removed, and instead the approval of contractual transfers and intra-group schemes by the Authority has been made subject to such schemes providing for effective protection, and liability of the data fiduciary in instances of harm arising out of transfers.</p>	
Exemptions (Chapter VIII)		
27.	The exemption on the ground of “security of the state” under Clause 25 of the Bill has been expanded to any agency of the Government with regard to any or all of the provisions of the Act.	We recommend that any exemption granted to any agency of the Government, should be the outcome of a detailed assessment of the potential harms to individual’s rights and freedoms, in consultation with the DPA.
28.	Clause 104 of the earlier draft relating to the Central Government’s power to exempt certain data processors processing foreign personal data, has been re-numbered and included as Clause 37 of the Bill, thereby moving the provision from “miscellaneous” to “exemptions”.	Please refer to <i>Part 2: Major Concerns, under IV. Power to Exempt certain Data Processors, at Page 17.</i>
29.	A new provision for sandboxes has been included as Clause 40 of the new draft. The sandbox will be created by the Authority, and any entity whose “privacy by design policy” is approved by the Authority shall be eligible to enter the sandbox subject to meeting other criteria to be specified by the Authority (for a total maximum period of 36 months – or two extensions not amounting to more than 36 months). By reason of inclusion in the sandbox, the	<p>We welcome the inclusion of regulatory sandbox provisions and believe that these will be crucial in ensuring sustained innovation in the technology ecosystem in India.</p> <p>The JPC may also consider granting an exemption on cross-border transfers to participants in the regulatory sandbox.</p>

S. No.	Provision	NASSCOM-DSCI Remarks
	<p>following provisions would not be applicable –</p> <ul style="list-style-type: none"> a. Clear and specific purpose under Clauses 4 and 5 b. Collection limitation under Clause 6 c. Other obligations relating to Clauses 5 and 6 d. Data retention under Clause 9 	
Data Protection Authority of India (Chapter IX)		
30.	<p>Chapter IX of the Bill establishes the DPA, and specifies its composition, administrative specifics, funding, and its powers and functions (Clause 49 of the Bill) – including its rulemaking powers, power to approve codes of practices, initiating inquiries both <i>suo moto</i> as well as on the basis of complaints received, etc.</p>	<p>Please refer to <i>Part 2: Major Concerns, under VI. Data Protection Authority, at Page 22.</i></p>
Penalties and Compensation (Chapter X)		
31.	<p>An amendment has been made to the provisions dealing with procedure to be followed by Adjudicating Officers, by adding a new proviso to sub-clause (1) stating that no inquiry under this section will be initiated in the absence of a complaint from the Authority.</p>	<p>We welcome this clarification, as it adds a layer of safeguards, and ensures that data fiduciaries do not have to bear the costs of cooperating with investigations initiated without sufficient basis.</p>
Offences (Chapter XIII)		
32.	<p>The offences relating to obtaining, transferring or selling of personal data or SPD contrary to the Act (Clause 90 and 90 of the earlier draft) have been deleted.</p> <p>The only retained offence is re-identification and processing of de-identified personal data. (Clause 82 of the Bill)</p>	<p>We welcome the deletion of the offences relating to obtaining, transferring or selling of personal data or SPD.</p> <p>Please refer to <i>Part 2: Major Concerns, under VII. Lack of appropriate grading of Criminal Offences, at Page 24,</i> for our detailed submissions on this.</p>

S. No.	Provision	NASSCOM-DSCI Remarks
33.	<p>A new sub-clause has been added in Clause 83 of the Bill to clarify that no court may take cognizance of any offence under the Act, save for on the basis of a complaint by the Authority.</p> <p>Consequently, the power to investigated offences by a policy officer not below the rank of Inspector has been deleted. Accordingly, the order of a magistrate will have to be issued before commencing investigation into offences.</p>	<p>We welcome the introduction of adequate safeguards for initiating a prosecution of offence under the Bill. However, we continue to maintain that criminal offences should not be included in the Bill.</p> <p>Please refer to <i>Part 2: Major Concerns, under VII. Lack of appropriate grading of Criminal Offences, at Page 24</i>, for our detailed submissions on this</p>
<p>Miscellaneous (Chapter XIV)</p>		
34.	<p>The provision on non-applicability of the Bill to non-personal anonymised data has been qualified, and a new Clause 91 has been included. The clause provides:</p> <p>a. A clarification that the Bill will not prevent the Central Government from framing any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies do not govern personal data; and</p> <p>b. That the Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to <i>provide any personal data anonymised or other non-personal data</i> (non-personal data being defined as not being personal data) to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed</p> <p>c. That the Central Government will be required to annually disclose all directions that are</p>	<p>Refer to <i>Part 2: Major Concerns, under V. Provisions Dealing with Non-Personal Data, at Page 19</i>.</p>

S. No.	Provision	NASSCOM-DSCI Remarks
	passed pursuant to this provision.	
35.	Clause 92 of the Bill empowers the Central Government to prohibit the processing of certain categories of biometric data, by way of notification.	Refer to Refer to <i>Part 3: Areas Requiring Clarification, under V. Other Issues Requiring Clarity, at Page 30.</i>