February 24, 2020

Ms. Meenakshi Lekhi
Hon'ble Member of Parliament & Chairwoman
Joint Committee on The Personal Data Protection Bill
Parliament of India
New Delhi

Re: USIBC Comments on the Draft Personal Data Protection Bill (PDPB)

Dear Ms. Lekhi,

Thank you for the opportunity to provide detailed comments on India's PDPB. Creating a privacy framework that is balanced, flexible, globally interoperable, and ensures the free movement of data while protecting consumers is central to India's digital transformation, the promotion of India's global competitiveness, and the *Digital India* vision of the Prime Minister – in particular the objective of creating a $1 trillion digital economy by 2025.

The U.S.-India Business Council ("USIBC") welcomes the opportunity to provide our recommendations to enhance the PDPB, and ensure a strong future for the U.S.-India digital economy. This submission includes three elements. First, we provide a high level summary of our priority issues, consent, and suggested enhancements of the PDPB. Second, we offer line-by-line input to the bill, which includes specific ideas along with a rationale. Lastly, we present analysis that compares India's PDPB to that of the General Data Protection Regulation ("GDPR").

Upfront, we recognize the challenge and complexity of the task, and acknowlege that many countries around the world, including the United States, are updating or establishing privacy regimes based on a judicious and thoughtful approach linked to global best practices and interoperability across leading digital nations. This historic Indian Supreme Court ruling in August 2017 that declared privacy to be a fundamental right for Indian citizens, provides the foundational legal framework from which multiple Indian institutions must subsequently craft and implement a privacy policy framework that not only adheres to an evolving legal standard, but critically, must balance the socio-economic benefits of innovation and efficiency, with lawful limits on enforcement and national security.

Realizing this challenge ahead, in 2017 USIBC stood up a dedicated India Privacy Working Group, which includes a leadership council and membership from multiple industry sectors – digital economy, financial services, media and entertainment, life sciences, retail, manufacturing, legal services, and others – that created a community of interest, developed a body of legal understanding for privacy within an Indian context, and brought together experts and regulators from the United States, Japan, the European Union and Singapore to facilitate India's development of a light-touch privacy regulatory regime.

USIBC supports principles and practices that balance privacy, innovation and global interoperability, while designing a regime that is aligned to work within existing legal structures in an effective and efficient manner. Accordingly, the U.S. Chamber of Commerce has developed a set of privacy principles, to help achieve a privacy framework that is balanced, flexible, globally interoperable, and protects the free movement of data

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

while protecting consumers. These principles are applicable to both India, the United States, and our mutual digital trading partners.

1. A comprehensive framework of regulation that ensures certainty and consistency
2. Risk-focused and contextual privacy protections
3. Transparency in collection, uses and sharing of consumer data
4. Industry neutrality
5. Flexibility to develop adaptable, consumer-friendly privacy programs
6. Harm-focused enforcement
7. Enforcement that promotes efficient and collaborative compliance
8. International leadership that promotes the free flow of data and interoperability between global frameworks
9. Encouragement for privacy innovation
10. Risk-based approaches to data security and breach notification

The following represent USIBC's key recommendations for the Draft Bill to ensure a privacy regime that bears in mind the important economic benefits created by flexible approaches to the use of data, and the importance of enabling cross-border data flows:

- ***Remove the data localization requirement and instead focus on transfer methods***. At present, the Draft Bill includes an extremely broad data localization requirement that will impose significant burdens on all businesses operating in India, including Indian organisations targeting global markets for their innovative solutions. Specifically, we are concerned with the requirement to locally store "sensitive data" – a category of data that may be expanded at any time – and the requirement to locally store and process so-called "critical data." There is no clarity on what may be notified as critical personal data, creating long-term uncertainty in India's data transfer regime. We must also highlight that the requirement for data fiduciaries to obtain explicit consent from data principals, in addition to undertaking the contractual safeguards outlined, is duplicative and creates an unjustified barrier for transfers of data out of India. Finally, we note that India is a net digital trade exporter and that India's globally competitive services sector requires open access to foreign markets. By instituting a data localization requirement, the Government of India would be endorsing measures that undermine a vital source of its own growth and innovation. India and the United States must find a mechanism that ensures data continues to flow between both economies and the rest of the world.

- ***Expand grounds for data processing***. The current Draft Bill appears to require data fiduciaries to wait for regulatory approval and regulatory specification before they can rely on the "reasonable purpose" ground for processing, which raises significant practical issues, in particular in terms of predictability and timing. By acknowledging multiple legal grounds for processing personal data, the Draft Bill will enable companies to engage in data processing in a flexible manner. Without multiple legal grounds for processing data, data fiduciaries must rely on the consent of data principals, thereby minimizing the value of consent through "consent fatigue." Similar to other data protection laws, Indian laws should recognize fulfillment of contractual obligations and processing business contact information as lawful grounds for processing.
- ***Clarify that the law would not apply to foreign national data processing***. The scope of the Draft Bill should be modified such that the provisions are not applicable to foreign national data being

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

processed in India under a contract. This should not be left to a notification process by the Central Government as it brings in process and business uncertainty.

- ***Clarify the definitions of personal data and anonymized data***. Under the Draft Bill's approach, if there is any possibility that data could be used to identify a person—no matter how remote that risk is—that data qualifies as personal data. India should recognize international best practices and approaches to anonymization that permit data fiduciaries to engage in "reasonable efforts" to anonymize data.
- ***Remove provisions allowing Government access to non-personal data under the bill.*** The objective of the Draft Bill is the protection of personal data. Expanding the scope to include provisions on non-personal data distracts from task of advancing this objective. The provision appears to suggest that the Government could notify formats for sharing data, without any governance structure or recourse available to entities to deny or discuss its use, mode of sharing and other aspects. The provision also raises serious concerns about competition, market access, intellectual property, and data privacy, as providing large amounts of information to the government may not be privacy-protective. We suggest that it be removed.
- ***Establish clear standards for what constitutes a "significant data fiduciary" and amend the obligations such that they are less burdensome.*** The Draft Bill is unclear on how the significant data fiduciary will be determined, what criteria will be used, and whether a designee may challenge the designation. In addition, there is language that appears to allow for the data protection authority, in its opinion, to designate *any* company as a significant data fiduciary. The absence of clear parameters may create unnecessary confusion and lead to negative unintended consequences to business development and the availability of services to individuals. Moreover, the obligations on data fiduciaries are already sufficiently exhaustive and the same should not be added on to based on factors such as turnover and employee strength.
- ***Remove social media identity verification.*** A social media intermediary will be governed by the applicable Intermediary Guidelines Rules, 2011 and amendments, likely to be notified soon.
- ***Clarify fair and reasonable.*** The Draft Bill addresses the issue of informed consent by stating that the data must be processed in a "fair and reasonable" manner that ensures the privacy of the individual. However, it does not specify what constitutes "fair and reasonable". This may lead to inconsistent and uncertain interpretations.
- ***Eliminate residency requirement for data protection officer (DPO)***. This requirement imposes substantial and unnecessary costs on foreign companies, who must hire an India-based DPO even if they already employ a DPO in another country; the burden is greatest for SMEs and entrepreneurs.
- ***Reform restrictions on processing data of under-18s***. The Draft Bill defines "child" as anyone under the age of 18, without recognizing the significant distinctions between those aged 17 and those aged 12. We suggest a more reasonable threshold aligned with modern privacy trends.
- ***Reform excessive penalties***. The Draft Bill's civil penalties and its provisions creating criminal liability for executives, are excessive and will deter companies from doing business in India. Criminal liabilities, in particular, may deter constructive cooperation between data fiduciaries and India's future data protection authority. We believe that a greater emphasis should be put on accountability measures – already acknowledged by the Draft Bill – as a powerful factor to minimize privacy risks and encourage better data protection outcomes.
- ***Provide sufficient time for implementation***. The Draft Bill is silent on when the Bill will come into effect and be enforced. The Government of India will need significant time and investment of resources to establish the future Indian Data Protection Authority, which will be charged with

additional rulemaking responsibilities on core aspects of the Bill. In addition, in the absence of any provisions for transition, the Bill does not provide sufficient time for the business community to implement its requirements. As a principle, timelines should be defined in a phased manner for entities to prepare and comply with each standard / code of practice / or rule, with the transition period starting from the date of notification.

USIBC appreciates the challenge ahead – and indeed the larger global privacy discussions before us. We are committed to assisting you in your efforts. USIBC and our members hope that our comments will be given a timely and sympathetic consideration. We welcome an opportunity to meet you at your convenience, and are happy to provide further information or clarification in relation to the issues in this representation. In the meanwhile, please do not hesitate to contact my staff or me: Jay Gullish, jgullish@usibc.com, and Abhishek Kishore, akishore@usibc.com, in Washington, D.C., and Aditya Vasishtha, AVasishtha@usibc.comin New Delhi. I would like to personally thank you for your leadership, and the Council and its members hope to discuss these recommendations at your convenience.

Nisha Biswal

President
U.S.-India Business Council (USIBC)

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

USIBC Response to the Draft Personal Data Protection Bill, 2019

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER I PRELIMINARY Section 1(2)	It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint…	The current implementation period for the Draft Bill is uncertain. An adequate time period should be provided for implementation in the Bill itself. It must be noted that, in the European Union, around 2 years time was provided for the implementation of GDPR even though its predecessor, the Data Protection Directive, had already been effective since 1995. Moreover, the EU already had well-established data protection authorities in place. In India, the implementation of the privacy regime would be a much-needed fresh start for regulators and for domestic industry. This Bill has cross sectoral impact and will require variety of Industry ranging from automotive, retail, oil & gas PSUs, power companies, health services and many others to learn and comply.	USIBC recommends that there should be a minimum time of 24 months for entities to prepare and comply with each standard / code of practice / or rule, with the transition period startingfrom the date of notification. Therefore, we believe that a phased introduction plan should: • Provide for timelines for formation of the Data Protection Authority • State a minimum period of 24 months be made available for applicability of any particular rule/ standards / code of practice from the date of its notification. This period should exclude the stakeholder consultation period that the Authority needs to undertake before notification of such standard/code of practice or Rule. For data processors dealing with foreign national data, there might be a need for additional timelines, as they would require international contract re-negotiations.
CHAPTER I PRELIMINARY Section 2 (A) (c) (ii)	in connection with any activity which involves profiling of data principals within the territory of India.		USIBC recommends to revise the clause as follows: *"in connection with any systematic activity which involves profiling of data principals within the territory of India"*
CHAPTER 1 PRELIMINARY Section 2 (B)	shall not apply to the processing of anonymised data, other than the anonymised data referred to		USIBC recommends to revise the clause as follows: *"shall not apply to the processing of anonymised data, or any processing of business contact*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	in section 91.		*information of a data principal in relation to their employment, business or profession with the data fiduciary, where business contact information means personal data relating to a data principal, including their name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information, that has not been provided by the data principal solely for personal purposes."* USIBC also recommends to insert Section 2 (c) as follows: *"To the extent any personal data collected prior to the date of enactment of this Act has been collected in compliance with the Information Technology Act, 2000, such personal data shall be deemed to be collected, processed and transferred in compliance with this Act."*
CHAPTER I PRELIMINARY Section 3(2)	"anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority;	Anonymisation is usually viewed as a risk management process where the risk of re-identification is assessed and managed. This requires an assessment of various technical, administrative and legal controls and factors.	USIBC recommends laying down a risk-based approach to anonymization upfront to avoid any confusion. These standards should include a reference to reasonable efforts and mention the factors which would be considered (e.g. "in which a data principal cannot reasonably be identified, taking into account technical, operational and legal controls to minimize the risk of re-identification"). Examples of such standards include those

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
			promulgated by Singapore and Canada. It is important to arrive at a reasonable "standard of anonymisation" as anonymised, psuedonymised, or depersonalised and/or aggregated data is essential for research, for systems optimization, for risk management and numerous other uses that provide benefits to governmental policy uses and commercial uses that can result in benefits to consumers. These standards could be developed by independent standardization bodies. USIBC recommends amending the following definitions as provided below: *"anonymisation" in relation to personal data, means such process of transforming or converting personal data to a form in which a data principal cannot reasonably be identified, taking into account all of the means reasonably likely to be used to identify the data principal, including the costs of and amount of time required for identification, the available technology at the time of the processing and technological developments.*
CHAPTER 1 PRELIMINARY Section 3(7)	"biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological,	Inclusion of "facial images" in this definition has what is likely an unintended result: any video or photograph of a human being, regardless of quality, or suitability for measurements or technical processing operations, is arguably "biometric data".	USIBC recommends to change the definition to: *"biometric data" mean personal data resulting from measurements or technical processing operations carried out on physical, or physiological, characteristics of a data principal, which allow or confirm the unique identification of that natural person.*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;		
CHAPTER I PRELIMINARY Section 3(8)	"child" means a person who has not completed eighteen years of age;	The personal data of children deserves special protection given the risks that children may face. At the same time, children require sufficient autonomy to further their development and advance their digital literacy. Protections for children should take into account their unique sensitivities while also fostering their independent growth. A more balanced approach to children's protections would allow families to make decisions about how much parental involvement there should be in their children's digital lives, without mandating parental consent for all children under the age of 18. As a practical matter, it is also difficult for data fiduciaries that operate principally online to distinguish the activities of older adolescents from those of adults, as they tend to view the same news, sports, and entertainment content as adults.	USIBC recommends to change the definition to: *"child" means a person who has not completed at least thirteen years of age;*
CHAPTER I PRELIMINARY	"harm" includes— (i) bodily or mental injury;	Indian employment law permits termination on medical grounds in	USIBC recommends that the definition of harm should not include ambiguous or subjective factors,

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
Section 3(20)	(ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal;	combination with several other factors, that may be considered by employer.	such as “humiliation,” “fear of being observed or surveilled,” and unexpected observation or surveillance. Similarly, the denial of benefits or services based on an evaluative decision should not per se be considered a harm, absent discriminatory intent or similar factors.

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER I PRELIMINARY Section 3(21)	"health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, 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;	By definition, health data, including this registration data, is sensitive personal data, subject to numerous processing restrictions. In many circumstances, registration data (where it does not associate the data principal to the provision of specific health services) is not sensitive or revelatory of the data principal's health status.	USIBC recommends to change the definition to: *"health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services where the data directly or by implication associates the data principal to the provision of specific health services;*
CHAPTER I PRELIMINARY Section 3(28)	"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;	The definition of personal data in the 2019 Bill is a more expansive than the 2018 Bill and includes "any inference drawn from such data for the purpose of profiling." This inclusion appears to widen the definition of personal data to include data about or relating to a natural person who is not directly or indirectly identifiable through it. This would have implications for the processing activities of data fiduciaries in relation to inferred data (in terms of needing valid consent/ explicit consent from the data principals before processing such inferred data as well). Additionally, a broad definition of personal data incentivizes data fiduciaries to link and retain data in order to respond to data principals' requests to access	USIBC recommends the clause to read as *"personal data" means data about or relating to a natural person who is reasonably identifiable, directly or indirectly, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information;* *Information about deceased persons does not constitute personal data.*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
		personal data.	
CHAPTER I PRELIMINARY Section 3(36)	"sensitive personal data" means such personal data, which may, reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.	The definition of SPD under the Bill includes categories of data that are routinely processed, such as data related to payment systems. Data that can be used to infer SPD (for eg., using a person's home address to infer their financial data) can also be considered SPD. Inclusion of financial data or other data that is routinely processed will significantly add to compliance costs of businesses. Further, the Bill allows the central government to expand the list of SPD to include additional categories of personal data, creating an uncertain environment for businesses.	USIBC recommends to change the definition to: *"sensitive personal data" means such personal data, which constitutes—* *(i) health data;* *(ii) official identifier;* *(iii) sex life;* *(iv) sexual orientation;* *(v) biometric data;* *(vi) genetic data;* *(vii) transgender status;* *(viii) intersex status;* *(ix) caste or tribe; or* *(x) religious or political belief or affiliation.*
CHAPTER II OBLIGATIONS OF DATA FIDUCIARY	Every data fiduciary shall give to the data principal a notice, at the time of collection of the		USIBC recommends to revise the clause to: *"Every data fiduciary shall give to the data*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
Section 7 (1)	personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—		*principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable or within the duration agreed by the data principal, containing the following information, namely:—"*
CHAPTER II OBLIGATIONS OF DATA FIDUCIARY Section 7 (1) (g)	the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;	The privacy notice requirements are onerous. It'll be extremely difficult to share names of all 3rd party data processors with whom companies might share data. Also there is a lot of overlap between Section 7 and Section 23. It is also not clear why there are two provisions governing the same issue.	USIBC recommends that this requirement on giving details of individuals / entities should be changed to categories of entities. *(g) the categories of individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable*
CHAPTER II OBLIGATIONS OF DATA FIDUCIARY Section 9(1) & (4)	(1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by	Regulations should be outcome based. This is all the more important, given the dynamic nature of technology, and therefore regulators prescribing 'manner of deletion' may be counterproductive. The requirement to retain data only till 'necessary' is strict and may result in a technical violation of the law. The 2018 Bill recommended by the Justice Srikrishna Committee allows retention till 'reasonably necessary' to fulfil the purpose of processing.	USIBC recommends to revise the provision to: *(1) The data fiduciary shall not retain any personal data beyond the period reasonably necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing, provided that it may retain the personal data beyond this period in order to comply with any legal requirement.* *(4) Where it is not reasonably necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations. Data*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	regulations.		*fiduciaries may anonymize data when the period for retention has expired.* USIBC recommends that the sections should be modified to clearly state the objectives and should permit the data fiduciary to implement its own systems and procedures, provided the objectives are met. The law should permit data fiduciaries to apply safeguards to personal data, including de-identification and encryption, in order to enable its use for research, product development, or other beneficial purposes. Also, there should be no requirement of DPA approval.
CHAPTER II OBLIGATIONS OF DATA FIDUCIARY Section 11 (2) (c)	specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;	All uses for scientific research purposes are unknown in advance. Hence, a "Broad Consent" should be allowed in case of data processing for scientific research purposes.	USIBC recommends to change the definition to: *specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing, except for cases of data processing for scientific purposes;*
CHAPTER II OBLIGATIONS OF DATA FIDUCIARY Section 11 (3) (c)	after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.	In practice, a data fiduciary should already be only collecting the minimum data necessary to perform a specific task or provide a specific service. Requiring even more granular choices seems to in fact allow data fiduciaries to collect more sensitive personal data than is necessary and we therefore suggest removal of this provision.	USIBC recommends to delete this provision.

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT Section 12 (a) (ii)	the issuance of any certification, licence or permit for any action or activity of the data principal by the State;	It is unclear whether processing for the purposes of assessing, maintaining, or furthering the quality, effectiveness, and safety of a medical device or pharmacological compound is allowed without consent. Given the status of medical device regulatory schemes within India, it is not clear that Indian medical device or other regulations create a sufficient basis for processing sensitive personal data to comply with explicit legal mandates pursuant to Section 12(b).	USIBC recommends to revise the clause as follows: *"the issuance, supervision, monitoring, or regulation of any certification, license or permit for any action or activity of the data principal by the State;"*
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT Section 12 (c)	for compliance with any order or judgment of any Court or Tribunal in India;		USIBC recommends to revise the clause as follows: *"for compliance with any order or judgment of any Court or Tribunal in India or any jurisdiction to which the data fiduciary is subject to;"* USIBC also recommends to add a subsection Section 12(g) as: *" for the purposes of assessing, maintaining, or furthering the quality, effectiveness, and safety of a medical device or pharmacological compound"*
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT	Notwithstanding anything contained in section 11 and subject to sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing	For the purpose of employment, related services / benefits to employee, companies need to process sensitive personal data including financial data and health data, and such processing, and decisions resulting from such processing,	Processing of sensitive personal data necessary for various purposes related to employment (including payment of employees, fraud prevention, immigration, termination of employment, etc.) should be a valid ground. Considering most of the employee data is sensitive, we recommend that

Section	Proposed Rulemaking	Observations	Recommendations
Section 13(1) (a)	is necessary for— (a) recruitment or termination of employment of a data principal by the data fiduciary;	should be permitted under the employment exemption from the consent requirement.	"reasonable purpose" for the recruitment & employment should cover sensitive personal data as well.
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT Section 14(1)	(1) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into consideration— (a) the interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the effect of the processing activity on the rights of the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing.	We recommend removing the subjective assessments and the requirement of DPA notification of reasonable grounds.	USIBC recommends to revise the clause as follows: *"(1) In addition to the grounds for processing contained in sections12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes, after taking into consideration—* *(a) the interest of the data fiduciary in processing for that purpose;* *(b) any public interest in processing for that purpose; and* *(c) the effect of the processing activity on the rights of the data principal."*

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT Section 14(2)	Processing of personal data for other reasonable purposes.	The Bill places a heavy focus on consent and does not contain a residuary ground to facilitate routine processing activities. While the 'reasonable purposes' ground is an attempt to allow processing for business operations, linking this to the approval of the DPA is overly restrictive, and discounts the dynamic nature of technology.	The concept of "reasonable purposes" allows some flexibility, but it is conditional on Authorities regulations. The list of "reasonable purposes" may be expanded and set out upfront in the bill along with permitting the DPA expanding/notifying it later. USIBC recommends the current list to be revised as follows: *14(2) For the purpose of sub-section (1), the expression "reasonable purposes"shall include—* *(a) prevention and detection of any unlawful activity including fraud;* *(b) whistle blowing;* *(c) mergers and acquisitions;* *(d) network and information security;* *(e) credit scoring;* *(f) recovery of debt;* *(g) processing of publicly available personal data;* *(h) the operation of search engines;* *(i) processing pursuant to a contract;* *(j) marketing and advertising;* *(k) processing to improve products and services;* *(l) exercising, establishing, or defending of legal claims or compliance legal obligations.* *(m) processing is necessary for compliance with*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
			a legal obligation to which the controller is subject *(n)* residuary *"legitimate interests" purpose, which can be determined by the data fiduciary.*
CHAPTER III GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT	Section 14 (1) and (3) Processing of personal data may be permitted for such reasonable purpose "as may be specified by regulations" Section 15 (2) Additional safeguards may be specified by regulation for processing of sensitive personal data	Having these obligations be subject to regulations, or subject to the approval of the DPA, may be too prescriptive, disrupt existing business relationships, cause uncertainty among investors in emerging business models, and discounts the dynamic nature of technology.	USIBC believes that processing should be permitted to protect the legitimate interests of the data subject (it is currently permitted only to process it in case of medical or health emergencies), or the data fiduciary/ processor (unless these legitimate interests are overridden by the fundamental interests of the data subject).
CHAPTER IV PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN Section 16(3)	The manner for verification of the age of child under sub-section (2) shall be specified by regulations, taking into consideration— (a) the volume of personal data processed; (b) the proportion of such personal data likely to be that of child; (c) possibility of harm to child arising out of processing of personal data; and (d) such other factors as may be prescribed.	Imposing a requirement on data fiduciaries to verify the age of children, even when they might not have knowledge that they are processing children's data, could require virtually all data fiduciaries to institute age gates on their websites and other services that collect data. Moreover, given the variety of organizations that would be affected, it is doubtful that the data protection authority would be able to specify how to verify a child's age in a practical manner in all possible cases.	USIBC recommends that the new requirement of "mechanism for verification of age of minors" should apply only where the data fiduciary has knowledge that it is processing children's data and determination of how to verify age should be left with Data Fiduciary as provided in the earlier draft. If not, then the mechanism should be clarified upfront. USIBC recommends the current list to be revised as follows *(2) The data fiduciary shall, before knowingly collecting any personal data of a child, verify his age and obtain the consent of his parent or guardian, taking into consideration—*

Section	Proposed Rulemaking	Observations	Recommendations
			(a) the volume of personal data processed; *(b) the proportion of such personal data likely to be that of child;* *(c) possibility of harm to child arising out of processing of personal data; and* *(d) the extent to which the data fiduciary directs its services at children.*
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 17(3)	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.	The requirement to provide all this information "in one place" is unclear and may not be possible for many organizations. Similarly, it is impractical (and often not useful) to provide the identities of all third parties, as these may not be known -- or providing categories may often be more descriptive for data principals. It would also be extremely onerous for a data fiduciary to be able to keep track of all the data sharing that may occur after the data is initially shared with a third party.	USIBC recommends to revise the clause as: *(3) The data principal shall have the right to access the identities or categories of the data fiduciaries with whom personal data has been shared together with the categories of personal data shared with them, in such manner as may be specified by regulations.* USIBC also recommends adding a new sub-Section 17(4): *17(4) The data fiduciary shall not be required to fulfill a request under sub-section (1) to the extent that fulfilling the request would:* *(a) impair the security or integrity of any products or services provided by the data fiduciary, or inhibit steps taken by the data fiduciary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify and repair errors in any products or services; or*

Section	Proposed Rulemaking	Observations	Recommendations
			(b) prove impossible or involve disproportionate effort.
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 18(1)(d)	The erasure of personal data which is no longer necessary for the purpose for which it was processed.	A lot of organizations perform research/analytics work where they draw conclusions & inferences from personal data because "inference drawn from such data", is now included as personal. Deletion of this data from research studies might not be possible. In addition, organizations have back up systems that archive the data for disaster recovery purposes. These back ups should be permitted, subject to the required data protections standards. There may also be audit or other regulatory purposes for which the data will need to be retained, again subject to the data protections standards.	USIBC recommends that it be subject to limitations similar to those in the GDPR given that the deletion of data can frustrate fraud detection and prevention, product improvement, research, etc. USIBC recommends adding the following new sub-Section 18(2): *18(2) The data fiduciary shall not be required to comply with a request to delete personal data if:* *(a) it is necessary for the data fiduciary to maintain the personal data in order to enable the data fiduciary to pursue a reasonable purpose pursuant to Section 14, provided that such personal data shall not be made publicly available; or* *(b) personal data is processed for research, archiving, or statistical purposes in accordance with Section 38.*
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 19	Right to data portability	Following experiments in other jurisdictions, the Government of India has proposed to grant its citizens an explicit right to data portability. USIBC cautions the Government that a right to data portability is rife with implementation concerns and may pose risks to individuals. First, as Peter Swire has observed,	USIBC recommends that any proposal related to data portability be weighed against these considerations. We urge the Government to recognize the technical challenges and costs associated with responsibly implementing such a right and with making it meaningful to the citizens of India. We further recommend that the development of common approaches to data transference, reception, and use, such as standards or codes of practice, be done on an industry-led and

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
		granting individuals a single file with all of their information means that "one moment of identity fraud can turn into a lifetime breach of personal data."[1] Swire has also cautioned that portability rights may not improve consumer welfare, as it is likely that dominant market players will entice users to give them more data, disadvantaging their competitors and new market entrants. Second, data portability raises privacy issues for third parties that may be captured, intentionally or unintentionally, by an individual's file. Third, as mentioned in the draft Bill, data portability may capture inferred information about an individual, causing confidentiality and intellectual property liabilities for businesses.	voluntary basis.
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 20 (1) (c)	The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure […] was made contrary to the	The right to 'continuing disclosure' is a new and undefined term and that it is presently unclear whether such data only applies to disclosure of data shared by users or data generated in the course of processing. It is suggested that the scope	USIBC recommends the clause to be revised as follows: *"was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.*

[1] Peter Swire & Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust & Privacy

Section	Proposed Rulemaking	Observations	Recommendations
	provisions of this Act or any other law for the time being in force	of this right be clarified in the Bill.	*(1A) Provided that the even after the exercise of the right under sub-section (1), the data fiduciary may continue to utilize the data without any public disclosure for:* *(a) Detection of security incidents, protect against malicious, deceptive, fraudulent, or illegal activity;* *(b)Internal uses that are aligned with the data principal's relationship with the data fiduciary;* *(c) for engaging in scientific, historical, or statistical research; or* *(d) to comply with a legal obligation."* We also recommend adding a definition of the right to restrict "continuing disclosure" to limit the same to certain kinds of public disclosure with potential for harm, etc along with exceptions. In the absence of a clear definition, it is not evident what kind of disclosure should be discontinued.
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 20 (3)	The Adjudicating Officer shall, while making an order under sub-section (2), having regard to— (a) the sensitivity of the personal data; (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life;		USIBC recommends the clause to be revised as follows: *"The Adjudicating Officer shall, while make an order under sub-section (2), having regard to—* *(a) the sensitivity of the personal data;* *(b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;* *(c) the technical feasibility and the cost involved in granting the right;* *(d) the role of the data principal in public life;* *(e) the right to exercise free speech or any other*

Section	Proposed Rulemaking	Observations	Recommendations
	(d) the relevance of the personal data to the public; and (e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.		*rights provided by law;* *(f) the relevance of the personal data to the public;* *(g) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented;"*
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 21 (1)	The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations	The requirement of "consent managers" under the 2019 Bill may in practice create risks in relation to access and deletion of user data stored by data fiduciaries as such requests have a higher than normal probability of proving malicious in nature and it is necessary for additional verification checks to be carried out that are best carried out by data principals directly making requests.	USIBC recommends the the revised clause as: *"The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing or in electronic format to the data fiduciary directly with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations"*
CHAPTER V RIGHTS OF DATA PRINCIPAL Section 21 (5)	The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall	This limited exemption from the requirement to a data principal's right to restrict or prevent the continued disclosure of personal data does not take	Additional reasons why data fiduciaries are obliged to comply with right to be forgotten request should be added, such as those included in GDPR including conducting research meeting certain conditions, and

Section	Proposed Rulemaking	Observations	Recommendations
	harm the rights of any other data principal under this Act	into account additional reasons why an individual should not be permitted to have his/her data restricted from futher processing. Such additional reasons included public interest reasons such as a stable credit economy.	other compelling legitimate interests. Legitimate interests should include processing permitted by certain applicable laws, such as the Credit Information Companies (Regulations) Act.
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 22(1) & (2)	Every data fiduciary shall prepare a privacy by design policy…. Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations.	As companies develop products, privacy and security by design are essential features of offerings that offer significant competitive advantage. Disclosures of technical systems that ensure privacy by design could in effect lead to disclosure of trade secrets and confidential information. With significant technical content, there are concerns on how the regulator would certify the privacy policy.	USIBC recommends that the requirement of disclosure of technical system details and certification be done away with, as this may lead to disclosure of trade secrets and confidential business information and a complex process for approvals that may lead to delays. The DPA should issue broad guidelines and specify the objectives and should permit data fiduciaries to formulate their own policies, which shall include privacy by design. Further, it appears that the submission of a privacy by design policy is only voluntary – and such certification will make a data fiduciary eligible to participate in the sandbox proposed under the Bill. However, the clause begins with 'subject to the regulations made by the Authority' raising doubts as to whether the requirement is voluntary or mandatory. The Bill should clarify that submission is voluntary. USIBC recommends the clause to be revised as under: *22. (1) Every data fiduciary may prepare* ***a voluntary privacy by design policy,*** *containing—* *(a) the managerial, organisational, business practices and technical systems designed to*

Section	Proposed Rulemaking	Observations	Recommendations
			anticipate, identify and avoid harm to the data principal; *(b) the obligations of data fiduciaries;* *(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;* *(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;* *(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;* *(f) the processing of personal data in a transparent manner; and* *(g) the interest of the data principal is accounted for at every stage of processing of personal data.* *(2) Subject to the regulations made by the Authority, the data fiduciary may submit a declaration that its privacy by design policy prepared under sub-section (1) to the Authority is compliant with the requirements as specified by regulations.* *(3) The privacy by design policy under sub-section (2) shall be published on the website of the data fiduciary.*
CHAPTER VI TRANSPARENCY AND	(1) Every data fiduciary shall take necessary steps to maintain transparency in processing		USIBC recommends the clause to read as under: *23. (1) Every data fiduciary shall take necessary*

Section	Proposed Rulemaking	Observations	Recommendations
ACCOUNTABILITY MEASURES Section 23	personal data and shall make the following information available in such form and manner as may be specified by regulations— (a) the categories of personal data generally collected and the manner of such collection; (b) the purposes for which personal data is generally processed; (c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm; (d) the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same; (e) the right of data principal to file complaint against the data fiduciary to the Authority; (f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (5) of section 29; (g) where applicable, information regarding cross-		*steps to maintain transparency in processing personal data and shall specify the information on its website—* *(a) the categories of personal data generally collected and the manner of such collection;* *(b) the purposes for which personal data is generally processed;* *(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;* *(d) the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;* *(e) the right of data principal to file complaint against the data fiduciary to the Authority;* *(f) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and* *(g) any other information as may be specified by regulations.*

Section	Proposed Rulemaking	Observations	Recommendations
	border transfers of personal data that the data fiduciary generally carries out; and (h) any other information as may be specified by regulations. (2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations. (3) The data principal may give or withdraw his consent to the data fiduciary through a consent manager. (4) Where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal. (5) The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as		

Section	Proposed Rulemaking	Observations	Recommendations
	may be specified by regulations. Explanation.—For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.		
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 24(1) Section 24(2)	(1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including— (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; (c) steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.	Data processors and data fiduciaries are expected to undertake implementation and review of security safeguards. It appears that there is a joint obligation on the fiduciary and processor to implement 'security safeguards. Often the data processor may not have visibility to the personal data and may not be aware of the particular risks unless informed by the data fiduciary. The data fiduciary is in the best position to understand the benefits and risks of their processing activities and provides instructions to the data processor based on their knowledge of the data subjects, personal data collected and processed, the risks associated with processing. Therefore, the responsibility for determining and implementing security safeguards should be vested with data fiduciaries and should	USIBC recommends Section 24 - be modified to reflect that the primary responsibility for the identification of relevant security standards, and safeguards under the law and its implementation is on the data fiduciary based upon the data fiduciary's assessment of the risks associated with the processing. Data fiduciary must ensure that these are enshrined in the contract (ref 31(1)) for the Data processor to implement as per instructions. We propose that high level guidelines be given as to the adequacy of the security safeguards, and organizations be permitted to apply their own technology solutions to these. Instead of using 'necessity' as the standard, the Bill should require businesses to have 'appropriate' technical and organization measures.

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

Section	Proposed Rulemaking	Observations	Recommendations
	(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly	not be extended to data processors. The contract between a data fiduciary and data processor should necessarily identify the applicable security safeguards and standards to be adopted by the data processor. Security safeguards are dynamic. Making these over prescriptive can hinder organization's ability to apply appropriate security safeguards. Additionally, the Bill requires both data fiduciaries and processors to implement 'necessary' security safeguards, but it does not clarify the nature of such safeguards. For instance, the GDPR requires 'appropriate' safeguards to be implemented, and prescribes factors such as the costs of implementation, nature, scope, context and purposes of processing, and risk for rights and freedoms of natural persons. In addition to the lack of factors, the DPA has the power to specify security standards through codes of practice under section 50. This means that a security safeguard put in place by a data fiduciary or processor may have to be revised from time to time.	
CHAPTER VI	Every data fiduciary shall by	It should be clarified that only breaches	USIBC recommends to revise the clause as follows:

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 25 (1)	notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.	with a high probability of material harm to individuals should be reported. Further, data breaches that are sensitive and could expose technical details of the data processor should be carefully evaluated before making it public. We recommend India adopt the Canadian standard of "real risk of significant harm", along with the guidance provided by the Office of the Privacy Commissioner of Canada so as to provide sufficient clarity as to the kind of data breaches that should be reported to the DPA. Details of data breaches may be confidential, and neither data fiduciaries nor the Authority should be required to report the details of such breaches publicly. Instead, a requirement to make general, high-level details probably achieves a better balancing of interests. Further, it must be considered that a failure to comply with this section would lead to stiff fines.	*(1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to result in a real risk of significant harm to any data principal.*
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 26 (1) , (2), (3) and (4)	(1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:— (a) volume of personal data	This addition is unnecessary as the obligations on data fiduciaries are already sufficiently exhaustive and the same should not be added on to based on factors such as turnover and employee strength. All companies, including information technology companies, deal	USIBC recommends deletion of this clause or in the alternate, proposes the revised clause as follows: *(1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm by processing by the data fiduciary; (e) use of new technologies for processing; and (f) any other factor causing harm from such processing. (2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations. (3) Notwithstanding anything in this Act, if the Authority is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations specified in sections 27 to 30 to such data fiduciary or class of data	with a variety of clients, and not all projects or engagement have the same risk profile. Therefore, the volume of data being handled and nature of technology deployed will differ on a case by case basis. Large employers should not be imposed with additional compliance obligations and penalized for creating employment. Clarity should also be provided that an entity classified as a significant data fiduciary may also act as a processor to entities that are not significant data fiduciaries. In such instances, provisions related to significant data fiduciaries should not apply. Further, the provision may end up discouraging innovations by penalising use of new technology. The addition of social media intermediaries as a category is also unnecessary as they do not pose any special category of harm and this incremental requirement goes against constitutional protections of equality. Further, the requirement for significant data fiduciaries to register with the DPA should be revisited, since registration requirements will only add to	*(a) sensitivity of personal data processed;* *(b) risk of harm by processing by the data fiduciary;* *(c) any other factor causing harm from such processing.* USIBC recommends to delete Clause (2), (3) and (4)

Section	Proposed Rulemaking	Observations	Recommendations
	fiduciary as if it is a significant data fiduciary. (4) Notwithstanding anything contained in this section, any social media intermediary,— (i) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and (ii) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary: Provided that different thresholds may be notified for different classes of social media intermediaries.	administrative burdens of the DPA.	
CHAPTER VI TRANSPARENCY AND	Upon completion of the data protection impact assessment, the data protection officer	Many organizations have a multitude of impact assessments covering systems and products. Submitting them all for	USIBC recommends that the data protection impact assessment should only be reviewed by the organization's internal data protection officer. The

Section	Proposed Rulemaking	Observations	Recommendations
ACCOUNTABILITY MEASURES Section 27(4)	appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations.	approval will be extremely onerous to both the DPA and the organizations. This will cause a massive amount of work for the DPA and could cause great inefficiencies.	requirement of submitting it to the Authority for review should be removed. The Authority will have access to this documentation if it opens an investigation into a data fiduciary, which provides sufficient accountability.
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 28 (3) & (4)	(3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed. (4) Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.	A social media intermediary will be governed by the applicable Intermediary Guidelines Rules, 2011 and amendments, likely to be notified soon. Moreover, the notification of social media intermediaries is also unsound from the perspective of Article 14 of the Indian Constitution.	USIBC recommends to delete these provisions.
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY	The Authority shall register in such manner, the persons with expertise in the area of information technology,	Currently, the law does not set forth the criteria for independence, but some precedent can be found in the European Union's General Data Protection	USIBC recommends a Section 29 (4) (a) as: *The independence requirement for data auditors can be satisfied by an employee of the data fiduciary*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
MEASURES Section 29 (4)	computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors under this Act.	Regulation, which gives Data Protection Officers independent status, while allowing them to be employed by the Controller or Processor whose data processing practices they oversee.	
CHAPTER VI TRANSPARENCY AND ACCOUNTABILITY MEASURES Section 30(3)	The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.	Many organizations have global operations, products and systems that are harmonized under a central DPO. Requiring also a local DPO places unnecessary costs and creates inefficiencies.	USIBC recommends the clause to read as under: *The data protection officer appointed under sub-section (1) shall represent the data fiduciary under this Act and shall be accessible to individuals and regulators in India.*
CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA Section 33(1)	Subject to the conditions in subsection (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.	Personal data that is collected by industry and employers, in many cases, is a mix of both personal and sensitive personal data. Therefore, the mandate to store sensitive personal data will necessitate data fiduciaries and processors in India to either store all data in India or disaggregate the data free of sensitive personal data and then transfer the subset abroad. Additionally, a requirement to keep two datasets updated in real time when processing may take place elsewhere is infeasible. Such data storage practices will not be efficient for	Data localization disrupts businesses, adds to cost of compliance, reduces choice, limits competition, deteriorates data security, and deprive Indian industry of the cloud economy and its inherent efficiencies, without adding to the ability to offer enhanced privacy and protection of data. USIBC recommends: • Data localization requirements should not be enshrined in the Personal Data Protection law. •To ensure consistency in India's data transfer regime, sectoral regulators promulgating storage or processing rules on personal data should be required

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

Section	Proposed Rulemaking	Observations	Recommendations
		businesses. Therefore, the proposed data localization requirements may have the same effect of mandating localization for all data in the medium to long run. Generally, many countries do not place restrictions on the cross-border transfer of personal data as long as the data fiduciary assumes responsibility for protecting the personal data. For instance, Philippines' Data Privacy Act of 2012 allows offshore transfer of personal data but the data fiduciary remains accountable for its protection. Similarly, Australia requires organizations to take reasonable steps to ensure that the overseas recipient of personal data does not breach the Australian Privacy Principles and the transferring organization remains accountable for the overseas recipient's acts. This ensures that the data fiduciary assumes responsibility for the protection of the data, without having to enforce any localization requirements.	to notify the Data Protection Authority, which will then engage in public consultations, including with industry, on its consistency with India's Personal Data Protection Act. • Government to Government dialogue for data sharing and access should be expedited. For instance, India can explore entering into executive arrangements with countries through laws such as the United States' Clarifying Lawful Overseas Use of Data Act, and seek to improve existing data sharing arrangements, such as Mutual Legal Assistance Treaties.
CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA	The critical personal data shall only be processed in India. Explanation —For the purposes of sub-section (2), the expression "critical personal	There is no clarity on what could be notified as critical personal data. The provisions introduce considerable uncertainty in business for the following reasons:	USIBC recommends that the classification of critical personal data should be done away with.

Section	Proposed Rulemaking	Observations	Recommendations
Section 33(2)	data" means such personal data as may be notified by the Central Government to be the critical personal data.	If a broad class of personal data is classified as critical personal data, this could lead to stringent data localization norms, thereby disrupting businesses. Globally, we have learnt that the process of recognizing destinations to be adequate for data transfers is time consuming, requiring several rounds of Government to Government discussions, that could last for several years and that, in the context of the European Union, may be subject to legal challenge. Therefore, such time that destinations are recognized as adequate, transfer of critical personal data may be completely prohibited, posing challenges for businesses in India.	
CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA Section 34 (1)	The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer,	The requirement for fiduciaries to obtain consent from data principals—in addition to an approved data transfer mechanism—does not advance data protection outcomes. Rather, a consent requirement imposes an additional barrier to cross-border digital commerce for Indian and foreign firms alike. Moreover, the requirement for explicit consent ignores the "reasonable purposes" ground for processing sensitive personal data under section 14 of the Bill. Section 14 was introduced as an	USIBC recommends that the explicit consent requirement be an independent ground of transferring sensitive personal data. USIBC recommends the clause to read as under: *"The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, OR where—"*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
		acknowledgement that consent is not always possible or practical in some situations (e.g. mergers and acquisitions, fraud prevention, cyber security, debt recovery). Correspondingly, consent is not always the most appropriate ground for allowing the transfer of sensitive personal data. For example, in order to fight cross-border fraud, defend networks against criminals who work across multiple borders, it may not be practical or advisable to seek the fraudsters or criminals' consent to process their financial data. For example, for debtors who flee across borders, and the transfer of financial data may need to pursue them in foreign jurisdictions, these debtors may use the consent requirement to block debt recovery efforts. The effect of requiring explicit consent under section 34(1) is that an entity that uses financial data for fraud prevention purposes and needs to provide it to counterparties overseas who will help protect or defend against such fraud (e.g internal investigations, merchants or banks overseas who are impacted by the fraud), will only be able to do so if it has obtained explicit consent under section 34(1) notwithstanding that the processing	

Section	Proposed Rulemaking	Observations	Recommendations
		already meets the reasonable purpose ground of processing. This significantly reduces the ability of companies to fight against cross-border fraud, cyber attacks, and debt recovery action.	
CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA Section 34 (1) (a)	The transfer is made pursuant to a contract or intra-group scheme approved by the Authority;	This is overly restrictive since all three permissible modes of transfer are dependent on the DPA or the government's approval. This may add to administrative burdens of the DPA/ the government, and any delay in approvals or certifications will delay transfers, impacting business opeations. In particular, the requirement to have contracts or intra-group schemes approved by the DPA is prescriptive and onerous, and could lead to government scrutiny of commercial contracts, some of which could have confidential technical details.	USIBC recommends to change the clause as: *The transfer be allowed using any one of the following methods: standard contractual clauses, intra-group schemes, or explicit consent, and that in the case of cross-borders data transfers that are required by the laws of countries outside of India, these transfers be allowed without restriction or availability of any of the legitimization mechanisms listed in Section 34 (1) (a), (b), and (c).*
CHAPTER VIII EXEMPTIONS Section 37	The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered	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	USIBC recommends to change the clause as: *"Notwithstanding any provisions of this Act, this Act shall not apply to the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any*

Section	Proposed Rulemaking	Observations	Recommendations
	into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.	notified as per category (ref sections 33, 34). Government can access data from both data fiduciaries and data processors, that includes non-personal data/ anonymized data (ref section 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. Notification on a case to case basis will disrupt ongoing and upcoming contract finalization and will impact confidence of clients outsourcing data processing to India. Scope of the bill should be modified such that the provisions are not applicable to foreign national data being processed in India under a contract. This should not be left to a notification process by the Central Government as it brings in process and business uncertainty.	*company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law."*
CHAPTER VIII EXEMPTIONS Section 40	Sandbox for encouraging innovation etc.	A clear path forward needs to be provided at the end of the Sandbox exemption period, otherwise innovators may be forced to revert to existing laws, negating the purpose of the Sandbox.	USIBC suggestion is to have a mandatory review process for the Bill, where the DPA will give a recommendation on whether or not any changes to law/rules/ standards are required, as an outcome of the sandbox initiatives.

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER IX DATA PROTECTION AUTHORITY OF INDIA Section 42	Composition and qualifications for appointment of Members.	The investigative and enforcement powers of Data Protection Authorities as well as their independence are a centre-piece of .many modern data protection regimes. It is of key importance to have an independent data protection authority that has investigative and enforcement powers. Lack of correct enforcement of sound legislation will be detrimental to the success of the legislation. It is important to ensure meaningful enforcement by primarily targeting sanctions at those ill-intended actors, who wilfully or in a grossly negligent way breach their legal obligations and cause harm to users. Legitimate players invest significant resources in not only complying with legal obligations, but often in putting in place data management practices, technologies and security measures that go beyond these requirements to ensure customer data of all types is treated with the respect and earnest that it deserves. Flexibility and discretion in enforcement should be made available to authorities in addition to fines. The proposed amendments will make it much harder for the DPA to be empowered and effective as the entire governing structure will be appointed exclusively by the government.	We recommend the Authority to include independent members and members from the judiciary. Additionally, the DPA must be made financially independent, perhaps receive funds the Consolidated Fund of India, to ensure true independence

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
CHAPTER IX DATA PROTECTION AUTHORITY OF INDIA Section 50	Codes of practice	These may be prescriptive, may reduce flexibility, and could rapidly become outdated with the advent of new technology. Further, there is a need for consultations with the industry and stakeholders before any standard, code of practice and rules are notified. While this has been specified for the purpose of code of practice, it should be extended to be a best practise for the DPA to adopt. Another issue is the technical expertise of the DPA to issue codes of practice for various issues. These issues mentioned in section 50 will require industry-level knowledge and expertise, which the DPA members may not necessarily be equipped with. Additionally, codes of practice should not be framed as prescriptive regulations, rather these should emerge as operational guides from the industry to ehance data protection outcomes.	USIBC believes that the codes of practice should be voluntary. Data fiduciaries and data processors should have sufficient flexibility to implement their own systems and practices, as long as the objectives behind the codes of practice are met. It must be noted that a similar approach has been followed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data) Rules 2011, where the Government stated that ISO27001 was one such standard that entities could follow. These Rules stated that personal data was to be protected using managerial, technical, and other measures commensurate with the nature of the data being protected. The Bill should also expressly mention that the DPA will hold consultations with industry bodies and associations of any class of data fiduciaries and processors, along with other stakeholders, before issuing a code of practice.
CHAPTER IX DATA PROTECTION AUTHORITY OF INDIA Section 50 (6) (k) (l) & (o)	(k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VI;	With technological evolution, standards and codes of practices are constantly evolving, with respect to data privacy and security. The Personal Data Protection Bill has given the Authority the responsibility to develop, approve and issue standards/codes of practice for	USIBC recommends that the Data Protection Authority should allow a data fiduciary or data processor to demonstrate before the Authority, or any court, tribunal or statutory body, that it has adopted an equivalent or a higher standard than that stipulated under the relevant code of practice, and therefore will be considered compliant. Such

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	(l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 24; (o) appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 25	protection of privacy and enforcement of the provisions of the bill. However, there is no flexibility to adopt a new and a better, more appropriate standard specific to a niche technology, that may not have been notified by the authority. This flexibility to demonstrate adherence to better and higher standards have been removed from the Personal data protection Bill 2019 and needs to be reinstated.	flexibility is important for business innovation and efficiency. Additionally, the code of practice prescribed under section 50(6)(o) should only be revised as: *(o) appropriate action to be taken by the data fiduciary in response to a personal data breach under section 25*
Chapter X PENALTIES AND COMPENSATION Section 57	Penalties for contravening certain provisions of the Act	Given the nature of technology, there may be significant ambiguity around data fiduciaries and processor's obligations under the Bill. Hence, a phased approach can be considered where the DPA can build up a body of precedents and jurisprudence, and where lower fines and penalties may be imposed for some time.	The quantum of penalties should be lower at the start, and can be revised in due course, once sufficient clarity has emerged.
Chapter X PENALTIES AND COMPENSATION Section 64(5) & 64(6)	(5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to	**T**he Bill correctly makes data fiduciary primary liable**,** recognizing that data processors can only act on behalf of the data fiduciaries (S. 10) However, while penalties and compensation levied on data processors is limited to the processor liability (64(1)) if they act contrary to the instructions of the data fiduciary pursuant or outside of the contract or not incorporated adequate	There must be clear separation of liability of data processor from data fiduciary • The accountability principle in the bill should be consistently applied to Rules, SOPs and Standards being developed by the Data Protection Authority, Government, Sectoral regulators**.** • Primary liability to comply with all provisions of the Bill and to pay compensation to data principal rest with the

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
	ensure effective and speedy compensation to thedata principal. (6) Where a data fiduciary or a data processor has, in accordance with sub-section (5) paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.	security safeguards, clause 64(6) imposes obligation on the data processor to pay the entire amount of compensation, on behalf of data fiduciary and others. In effect, the Bill allows a data processor to be penalized, despite their neither having a full visibility or understanding on why and how personal data was collected, the purpose and objective of such collection, nor any control over the acts or omissions of the data fiduciary or other data processors.	data fiduciary, and any compensation payable by the processor should be limited to the harm caused due to violation of contractual terms and conditions.
Chapter X PENALTIES AND COMPENSATION Section 65	No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or any other law for the time being in force		Only administrative fines and penalties should be provided for, whether as compensation to individuals and/or penalties to be paid to the government. Goals of promoting compliance with the law can be achieved via these damages and fines/penalties without needing to permit private causes of action. Private causes of action and class actions will not serve to promote the objectives of the law without also creating uncertainty in the marketplace, increased costs and a deterrence to investment.

Section	Proposed Rulemaking	Observations	Recommendations
Chapter XIII OFFENCES Section 83	non-bailable and cognizable offences	Apprehension of stringent penalties in an uncertain technology environment	Such offences should exclude criminal penalties for individual employees of a company or provide for remedies such as bail, based on discretion of the court, after considering bona fide deployment of technology. Such offences should also be made compoundable offences.
Chapter XIV MISCELLANEOUS Section 91(2)	The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-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. Explanation.— For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data.	Government can access data from both data fiduciaries **and** data processors, that includes nonpersonal data/ anonymized data. The draft bill does not cover non personal data under its ambit, and there is no reason to include this clause in a bill that seeks to protect personal data. There is also a concern that Non-personal data has wide implications and could include proprietary information, insights, trade secrets, algorithms, source codes etc. The provision appears to suggest that the Government could notify formats for sharing data, without any governance structure or recourse available to entities to deny or discuss its use, mode of sharing and other aspects. Further this clause undermines the existing business practices wherein the data processor is contractually bound by the data fiduciary and cannot share data (personal or non-personal) or any insights thereof, as they belong to the client of the data processor on whose behalf the data	USIBC recommends to remove this clause. *Instead, it is possible to incentivize data sharing and increase data availability without requiring the mandatory disclosure of non-personal data. The creation of a framework to enable voluntary data market-places will help to address information asymmetry, facilitate price discovery for data, and incentivize collaboration between different stakeholders in the AI ecosystem. Adopting a voluntary data market-place scheme will also reduce the potential concerns relating to intellectual property rights, adverse impact on incentives for innovation, and other legal risks which arise from a forced disclosure of non-personal data.*

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE

Section	Proposed Rulemaking	Observations	Recommendations
		processing entity is conducting data processing activities as per instructions and contract. **This will have a huge impact on business confidence of clients and foreign nationals, of data processing companies in India as they would be apprehensive of Government of India's access to data.** **This clause effectively can bypass the control of the data fiduciary and obligations of data processor under its contract with data fiduciary.** Further, implications and concerns of the stakeholders should be evaluated carefully, before such requirements are imposed even if it is outside of this data protection bill	
Chapter XIV MISCELLANEOUS Section 92	No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law	Restrictions in processing biometric data can be brought in by a Government notification. This can potentially impact many technology solutions that are being developed for authentication and controlled access such as Fin Tech, mobile access etc that are essential for the success of Digital India and inclusion programs. Given the low literacy levels biometrics will be an easy way for citizens to access, identify and interact	USIBC recommends to delete this section.

Section	Proposed Rulemaking	Observations	Recommendations
		with devices and solutions. Controlling that will impinge on the same. Also, given the large use of biometrics as well as other sensory inputs for people with disabilities to interact with technology and leverage its strengths would also get hampered and drive exclusion.	
CHAPTER XIV: MISCELLANEOUS Sections 93 & 94	Power to make rules	The Bill has significantly expanded the rule-making powers of the government in section 93, despite the DPA being proposed as an independent regulatory body under the Bill. Section 93 gives excessive rule-making powers to the government which are neither subject to the scrutiny of any non-government body or Parliament. Despite being given such wide powers under sections 93 and 94, neither provision provides for stakeholder consultations to be carried out before the framing of such rules or regulations. Framing such rules and regulations in a growing digital economy like India without holding a stakeholder consultation can result in a mismatch between industry requirements, global practices and regulatory frameworks.	USIBC recommends that both sections 93 and 94 should provide for a stakeholder consultation process to be carried out, which would compulsorily involve industry bodies, association of any class of data fiduciaries or processors and other stakeholders including the public. This will allow the government and the DPA to frame subordinate legislation that is practical and is in line with prevalent global practices.

Section	Proposed Rulemaking	Observations	Recommendations
		This can make it difficult for businesses to operate in India, and ultimately force them to exit the Indian market, thereby affecting the economy by limiting availability of quality services and employment generation in the country.	

Appendix I: Comparison of GDPR and PDPB – Refer separate attachment

1615 H Street, NW, Washington, DC 20062 | 202-463-5679 | info@usibc.com | usibc.com

U.S. CHAMBER OF COMMERCE