Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE MUMBAI BKC NEW DELHI MUNICH NEW YORK

93 B, Mittal Court, Nariman Point, Mumbai 400 021, India
tel +91 22 6669 5000, fax +91 22 6669 5001

www.nishithdesai.com

The key points to note in the PDP Bill are as follows:

I. Amendments to Current Law

The PDP Bill, when enacted, will replace Section 43A[1] of the *Information Technology Act, 2000* and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* ("**Current Law**") which currently, in tandem with sectoral laws, provide for the data protection framework in India.

II. Applicability

The PDP Bill applies to the processing of personal data ("**PD**") of natural persons, of which sensitive personal data and critical personal data are subsets. The natural person whose data is being processed is referred to as a "**Data Principal**". Further, the proposed law applies to both manual and automated processing.

i. Retrospective Applicability

The PDP Bill is silent about retrospective applicability, i.e. applicability to data collected before the law coming into effect and if the provisions would apply to such data. However, the PDP Bill will apply to any ongoing processing once introduced.

Practically this may be problematic for the following reasons:

[1] **Section 43A: Compensation for failure to protect data**

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008) Explanation: For the purposes of this section (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. (iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

Ongoing processing activity: In all likelihood, substantial PD would not have historically been obtained with consent. Thus, for any continued processing necessary consents may need to be obtained. This may mean renegotiation of previously concluded contracts, because if Data Principals do not give consent, the Data Fiduciaries may refuse to provide goods or services. However, the PDP Bill does not specifically clarify this.

Deletion of data: Data Fiduciaries may have to delete PD previously collected or PD for which they have not been granted specific consent unless specific consent is taken. Also, for consent given earlier Data Principals would also have the right to withdraw consent and request erasure of the data.

ii. Definitions

Several definitions in the PDP Bill are currently open-ended. ***This could create uncertainties in the manner in which the PDP Bill will be interpreted, implemented and enforced.***

For instance, the definition of harm includes references to *"(i) 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; and (ii) any observation or surveillance that is not reasonably expected by the data principal."*, which are ambiguous and open-ended.

iii. Personal Data

PD is data about or relating to a natural person who is directly or indirectly identifiable, having regard to any (or combinations of) characteristic, trait, attribute or any other feature of the identity of such natural person.

The definition of PD is extremely wide in comparison to the Current Law. Barring a few provisions, the PDP Bill also applies to manual processing of PD, where certain exemptions may be granted. However, there are no thresholds for which the exemptions can be granted. Thus, several non-digital businesses handling even non-sensitive PD are likely to be burdened with huge compliances, unless the DPA provides exemptions.

iv. Sensitive Personal Data

Sensitive Personal Data ("**SPD**") is a subset of PD and consists of specified types of data, such as financial data, health data, official identifier, sex life, sexual orientation, biometric data,[2] genetic data,

[2] The PDP Bill specifically bars the processing of biometric data, unless such processing is *"permitted by law"*. Notably, the provision is quite wide and the scope of which biometric data may not be processed seems to be unclear.

transgender status, intersex status, caste or tribe, religious or political belief, etc. The DPA has the power to declare further categories of data as SPD.

There are certain additional compliance requirements for SPD, such as the data localization and restrictions on processing. We have covered these below. As a result of these additional compliance requirements, the BFSI and Pharmaceutical industries are likely to get affected as both 'financial data' and 'biometric/health data' have been retained as categories of SPD. Our specific observations are below:

Financial data:. The definition of financial data ought to have been restricted to 'authentication information' for financial instruments alone. Information such as a bank account number, is independently less likely to cause harm to the Data Principal, as opposed to a bank account number in combination with a password used for authenticating transactions. For example, with the advent of the usage of mobile phone numbers as primary means to enable digital payments, they are often used in lieu of bank account numbers as the identifiers for mobile wallets. Similarly, the Unified Payments Interface ("UPI") has made peer-to-peer financial transfers easily accessible through use of Virtual Payment Addresses ("VPAs"), which sometimes merely consist of mobile phone numbers with short codes as suffixes. This makes it difficult for a third party to cause harm to the Data Principal merely by possessing the VPA. Harm, is typically caused with the misappropriation of authentication information alongside login information and not one independent of the other.

Therefore, the PDP Bill in its current construct would cause inconvenience to those individuals who use the system regularly to transact among each other as they would have to technically comply with the stringent provisions of the PDP Bill to the extent of standards prescribed for SPD, merely because they possess each other's payment identifiers.

Biometric data: In addition to fingerprints, iris scans, facial images, biometric data has been defined to include 'behavioral characteristics'. The said term is not defined. Prima facie, it could possibly impact voice activated assistants and assistive technologies which are used by people with disabilities. Further, the Government has the overarching power of carving out certain kinds of biometric data from processing, as it may deem fit.

Religious or political beliefs/ caste or tribe: Interestingly, the PDP Bill also includes religious or political beliefs / caste or tribe within the realm of SPD. However, in the Indian context, the inclusion of these items does not appear to be entirely relevant as they might be disclosed via individuals' surnames!

Official identifiers: Official identifiers have been defined to include any number, code or other identifier, assigned to a Data Principal under a provision of law for the purpose of verifying the identity. Aadhaar has been removed from the definition of official identifiers, as compared to the

draft Bill of 2018. However, the definition is still broad enough to include Aadhaar, as it includes any number or identifier used for the purpose of verifying the identity of a Data Principal.

v. Processing

Processing has been defined very broadly, to include an operation or set of operations performed on PD, and may include operations such as collection, organization, storage, alteration, retrieval, use, alignment or combination, indexing, disclosure, etc.

vi. Data Fiduciaries and Data Processors

Entities processing PD may be either "**Data Fiduciaries**" (the entity that determines the purpose and means for processing) or "**Data Processors**" (the entity that processes PD on behalf of a Data Fiduciary). While most obligations under the PDP Bill are on Data Fiduciaries which include notice and consent, implementing operation framework for the enforcement of user rights, and transparency and operability measures; there are limited obligations on Data Producers, such as the necessity to implement security safeguards.

vii. Anonymized Data

Anonymized data (i.e., data which cannot identify a Data Principal) largely falls outside the scope of the PDP Bill. The extent to which large datasets can be truly anonymized (an irreversible process) is still a matter of global debate, but for the purposes of the PDP Bill, anonymization is presumed to be possible, and the discussion here is on that basis. However, there is an ongoing worldwide debate on whether data can truly be anonymized, as there may always be identifiers from which it may be re-identified as PD.

The Central Government may direct any Data Fiduciary or Data Processor to provide any anonymized personal data or other non-personal data in order to enable **better targeting of service delivery** or to **aid evidence-based policy making** in a manner as may be prescribed. It is unclear whether this data would have to be provided only to the State or to private parties as well; In addition, terms of the provision of such data, such as fair compensation, have not yet been specified. The PDP Bill also reserves the power of the Central Government to frame policies for the promotion of the digital economy, to the extent such policies do not govern PD.

Interestingly, a committee under the chairmanship of Mr. Kris Gopalakrishnan was set up recently to recommend a framework to regulate non-personal/community data. That committee has not yet submitted its report. In our view, this aspect should be kept out of the PDP Bill, and this committee

should be allowed to conduct public consultations before giving their recommendations on non-personal data.

viii. Extra Territorial Application

In addition to being applicable to the processing of PD collected within the territory of India and collected by Indian citizens/companies; the PDP Bill is designed to have extra territorial application.

Applicability of the PDP Bill		**Processing**		**Data Principal (only Natural Persons)**	
		In India	Overseas	Located in India	Located overseas
Data Fiduciary / Processor	Located in India	✓	✓	✓	✓ Unless specifically exempted, such as in the case of outsourcing contracts.
	Located overseas	✓	✓ If in connection with any business carried on in India, or any systematic activity of offering goods or services to Data Principals within India; or in connection with any activity which involves profiling of Data Principals within India.	✓	X

The PDP Bill does not define what would amount to 'carrying on business in India'. For reference, the Australian Privacy Principles without defining 'carrying on business' have interpreted it to generally

involve conducting some form of commercial enterprise, 'systematically and regularly with a view to profit'; or to embrace 'activities undertaken as a commercial enterprise in the nature of an ongoing concern, i.e., activities engaged in for the purpose of profit on a continuous and repetitive basis'.

The PDP Bill has tried to ensure a balance between seeking to ensure the applicability of the PDP Bill to the PD of foreign residents processed in India, and at the same time has provided for exemptions, where necessary to promote data processing activities in India.

For instance, the definition of PD is not limited to Indian citizens/residents; as Section 2 of the PDP Bill in relation to applicability of the law uses a method of territorial nexus with India for establishing jurisdiction for the purposes of the PDP Bill. Under the PDP Bill, if the data is processed by any person or entity within India, then the provisions of the PDP Bill will apply. This could possibly go on to show that India is seeking to provide an equivalent level of data protection to the data of foreigners, hence increasing the chances of gaining 'data adequacy' status from the EU.

However, in view of the fact that India has a well-developed domestic data processing industry the Central Government has been given the power to exempt the processing of personal data of Data Principals located outside India by Indian Data Processors, if pursuant to a contract executed with a person outside the territory of India.

III. Major Obligations

i. Notice

The Data Fiduciary is obligated to provide a Data Principal with adequate notice prior to collection of PD either at the time of collection of the PD or as soon as reasonably practicable if the PD is not directly collected from the Data Principal ("**Notice**"). To fulfill the Notice requirement, certain key information is required to be provided to the Data Principal by the Data Fiduciary, such as:

- The purposes for which the data is to be processed;
- The nature and categories of PD being collected;
- The right of the Data Principal to withdraw their consent, and the procedure for such withdrawal, if the PD is intended to be processed on the basis of consent; and
- information regarding any cross-border transfer of the PD that the Data Fiduciary intends to carry out, if applicable.

This Notice should be clear, concise and comprehensible and specifies that a Notice may be issued in multiple languages whenever necessary. ***However, the PDP Bill is not clear as to when such multilingual notices maybe necessary.***

From a practical implementation perspective, we note that the information required to be shared in a Notice is extensive, detailed and fairly granular. Some practical issues that are likely to arise are:

- *Details about individuals and entities with whom such PD may be shared is required to be provided upfront in the Notice itself. It is not clear whether the names of such entities are required to be disclosed or only the categories. We believe that the final law should clarify that broad categories should be sufficient as at the time of collection of the PD the Data Fiduciary is unlikely to have access to the names of all entities who may process such PD.*
- *The source from where such PD is collected is also required to be disclosed. Ascertaining the source in a complex data sharing architecture may get very difficult, especially where multiple group companies or related entities may be involved. Further, it may also result in notice fatigue amongst Data Principals, due to the multiplicity of Notice(s) that may need to be sent out by Data Fiduciaries.*
- *The DPA has been empowered to add to the list of items to be disclosed in the Notice. It is hoped that, the DPA does not make Notice too cumbersome by including granular details, whereby it gets difficult to make it clear and concise as required under the PDP Bill.*

ii. Purpose and Collection Limitation

Data Fiduciaries processing PD are required to do so in a fair and reasonable manner so as to ensure the privacy of the Data Principal.

Data Fiduciaries may only be able to collect data from Data Principals that is necessary for the purposes of processing and the processing of data may be done only (a) for the purposes specified to the Data Principal; or (b) for any other incidental purpose that the Data Principal would reasonably expect the PD to be used for, given the context and circumstances in which the PD was collected and the purpose for collection. Therefore, using data for new (or previously unspecified) purposes should therefore need fresh consent.

iii. Storage Limitation

PD may be retained only until the purpose of collection is completed. ***It is recommended that Data Fiduciaries have a data retention policy in place outlining the length of time they will hold on to the personal information of its users, as there is a positive obligation to delete such data in certain situations***.

Data Principals have the right to request the deletion of their data at any time, with the Data Fiduciary confirming removal from its systems and from the systems of any other companies who were processing the data on its behalf. ***However, it must be noted that in a digital ecosystem, the complete deletion of data and confirmation that no digital footprints remain is questionable.***

iv. Transparency of Processing.

The PDP Bill requires Data Fiduciaries to implement measures which facilitate and demonstrate transparency and accountability measures. These measures are intended to provide adequate information to Data Principals on the manner in which their data is being processed and also provide notification on data breaches.

The PDP Bill requires Data Fiduciaries to provide the following information relating to their processing of PD, in the manner as may be specified by regulations:

- Categories of PD being collected.
- The purpose for which such PD is being processed.
- Categories of data processed in exceptional situations or any exceptional purposes of processing. that create a risk of significant harm.
- The existence of, and the procedure to exercise Data Principal rights.
- Information relating to cross border transactions generally carried out by the Data Fiduciary.
- Where applicable, the Data Trust Score of the Data Fiduciary.

The above list is not exhaustive, since the PDP Bill also reserves the provision to add *'any other information as may be specified by regulations'.*

In addition to the above, the Data Fiduciary is also required to inform the Data Principal of 'important operations' in the processing of PD. However, what constitutes 'important' has not been defined under the PDP Bill and is left to the regulators. This requirement assumes significance since it would impact compliance levels by Data Fiduciaries. It is therefore necessary that only important (rather than routine) operations in data processing are eventually included in this requirement by the regulator.

IV. Grounds for Processing PD and SPD

The PDP Bill provides that PD cannot be processed without consent, except for a specific ground set out in the PDP Bill:

i. Processing on the basis of consent

- The PDP Bill lays down the test for 'valid consent' for PD, i.e. consent which is free (as per the Indian Contract Act), informed (considering whether the information required under the notice provision has been provided), specific (considering whether the Data Principal can determine the scope of consent for the purpose), clear (indicated through affirmative action

in a meaningful way) and capable of being withdrawn (considering the ease of withdrawal of such consent compared to the ease with which consent was granted).

- For SPD, explicit consent is required after meeting the following *additional* requirements: 1) the Data Principal must be informed of the purpose of processing which is likely to cause significant harm; 2) the consent has to be clear and may not be inferred; 3) the Data Principal must be provided a choice of separately "consenting to the purposes of, operations in, the use of different categories of, SPD" that may be relevant to processing.

- In an attempt to make consent more meaningful and prevent its abuse, the PDP Bill also provides that Data Fiduciaries cannot make the provision of their services / goods conditional on the consent of the Data Principal to collect and process PD *that is not necessary for the provision of the services / goods by the Data Fiduciary*. Accordingly, a Data Fiduciary may condition the provision of services on the consent of the Data Principal, provided that such processing is *necessary* for the provision of services by the Data Fiduciary. Considering the increasingly complex nature of personalized services derived from processing of multiple fields of PD, the determination of whether some PD is necessary for the particular of specific services could become a complicated exercise based on the unique circumstances of each product or service in consideration.

- ***The PDP Bill places the burden on the Data Fiduciary to show that consent meets all the elements specified above. However, this aspect needn't have been specified in the PDP Bill. The principle as per the Indian Evidence Act could have been adopted here as well, i.e. the party which alleges a particular fact, needs to prove it. When any fact is especially within the knowledge of any person, the burden of proving that fact is upon him. For proving free consent, with the current scheme under the PDP Bill, the Data Fiduciary will need to prove absence of coercion. This goes against the basic principles of burden of proof.***

Consent Manager:

The PDP Bill has introduced the concept of 'consent managers', identified as Data Fiduciaries who will enable Data Principals to gain, withdraw, review and manage consent through "accessible, transparent and interoperable" platforms. These consent managers are to be registered with the DPA and will be subject to certain regulations as the DPA may specify.

The idea of 'consent managers' is innovative but relatively untested. It appears intended to mitigate the concern of 'consent fatigue' and help educate the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on implementation of consent managers.

It appears from the role of the consent manager that they are supposed to be acting as a service provider to Data Principals to manage their consent. If that were the case, consent managers should not be categorized as Data Fiduciary, or a separate category of Data Processors who may be subject to limited compliances. In order to qualify as Data Fiduciaries under the PDP Bill, the consent managers would have to determine the purpose and means for processing of data.

ii. Processing on grounds other than consent

PD may be processed without consent for specified grounds including:

(i) If processing is "necessary" for: (a) the performance of certain State functions (i.e., the provision of any service or benefit to Data Principal, or the issuance of any certificate, license or permit); or (b) "under any law" that is made by Parliament or a State legislature;

(ii) prevention, investigation or prosecution of any offence or any other contravention of any law;

(iii) compliance with court orders;

(iv) in connection with legal proceedings;

(v) in connection with disasters or medical emergencies;

(vi) employment-related purposes (where the Data Principal is an employee of the Data Fiduciary);

(vii) journalistic purposes;

(viii) personal or domestic purposes;

(ix) classes of research, archiving or statistical purposes specified by the DPA; and,

(x) Reasonable purposes as specified by regulations issued by the DPA: "Reasonable purposes" may include prevention of unlawful activity, credit scoring, recovery of debt, network and information security, among other items. Interestingly, a new ground – *the operation of search engines* – (which did not find place in the draft Bill of 2018) has been included as a reasonable purpose for which PD may be processed without consent. These reasonable purposes may be specified after taking into consideration factors such as the interest of the Data Fiduciary in processing for that purpose, whether it is reasonably expected for consent to be taken, and the reasonable expectations of the Data Principal having regard to the context of processing.

SPD may be processed without consent on all the grounds specified above except employment-related purposes. The DPA is given the power to specify additional safeguards for the purposes of "repeated, continuous or systematic collection" of SPD for profiling.

With respect to the State's processing of PD, the Bill grants fairly wide leeway to the State (see (i) and (ii) above). Ideally, State and non-State actors could have been treated at par in the PDP Bill, to the extent that such treatment did not impede compelling State interests.

From the perspective of businesses, it is a welcome move that consent has been made a prominent ground for the processing of PD and SPD. This has been done in spite of voices to the contrary suggesting the exclusion of consent as a ground altogether. The 'reasonable purposes' provision leaves discretion with the DPA to notify additional purposes for which consent may not be required to process PD. However, contracts between parties has not been specifically identified as a ground for processing without express consent. As these grounds are to be specified by the DPA, there may be an opportunity for industries' to make representations for additional grounds to be added.

V. Personal and Sensitive Personal Data of Children

Age of consent: The PDP Bill mandates that parental consent will be necessary for the processing of PD of children (i.e., persons below the age of eighteen years).

Obligations of Data Fiduciaries: Data Fiduciaries are to verify the age of children and seek parental consent before processing their PD.[3] Thus, the obligation to ensure age gating / verification and the necessary tools will have to be implemented by businesses. Age verification mechanisms are to be specified by regulations.

Guardian Data Fiduciaries: Data Fiduciaries who operate commercial websites / online services directed at children; or process large volumes of PD of children will be notified as 'Guardian Data Fiduciaries'. These fiduciaries are barred from undertaking activities such as profiling, tracking, behavioral monitoring, targeting advertising directed at children, or any form of processing that could cause significant harm to children.

These provisions may lead to practical implementation issues for the following reasons:

There are certain platforms which are targeted / focused on young adults aged 14-18 such as casual gaming, education, or even specific video platforms. Seeking parental consent in each of these cases would not only be difficult but also impractical.

Businesses catering to those below 18 might be affected by this PDP Bill. Education focused startups, who rely on targeted advertisements for example, may suffer due to the bar on processing of PD

[3] The only entities exempted from the parental consent requirement are those guardian data fiduciaries who provide exclusive counseling or child protection services.

directed at children. Similarly, audio / video streaming platforms may not be able to offer suggestions based on individual preferences.

VI. Rights of Data Principals: Right to Confirmation and Access / Right to Correction

The PDP *Bill* provides detailed rights to the Data Principal to access and correct their data.

With regards to a right of review, the PDP Bill grants rights to: (a) a confirmation about the fact of processing; (b) a brief summary of the PD being processed; and (c) a brief summary of processing activities. Similarly, the right of correction has been developed in the PDP Bill into a detailed step-wise process for how correction, completion or updating of the PD should be done. The PDP Bill also grants the right to request for erasure of PD which is no longer necessary for the purpose for which it was processed.

In addition, the PDP Bill also grants Data Principals, the right to access in one place and in a manner as may be prescribed via any regulations (a) the identities of all the Data Fiduciaries with whom their PD has been shared; and (b) details as to the categories of their PD which has been shared with such Data Fiduciaries, which seems quite onerous.

The PDP Bill requires businesses to provide the Data Principal with summaries of the PD being processed rather than the entire data dump. This may require some effort on the part of Data Fiduciaries.

VII. Data Portability

In an attempt to grant users more control over their data, the PDP Bill introduces a provision with respect to Data Portability, whereby Data Principals may seek from the Data Fiduciary, their PD in a 'structured, commonly used and machine-readable format'. The PDP Bill however does not specify the technical specifications of such a format, or what would be threshold for 'common use'.

The PD to be provided to the Data Principal would consist of: (i) data already provided by the Data Principal to the Data Fiduciary; (ii) data which has been generated by the Data Fiduciary in its provision of services or use of goods; (iii) data which forms part of any profile on the Data Principal, or which the Data Fiduciary has otherwise obtained.

Exemptions have been provided for instances where (i) the data processing is not automated; (ii) where the processing is necessary for compliance of law, order of a court or for a function of the State; and significantly, (iii) where compliance with the request would reveal a trade secret for a Data Fiduciary, or would not be technically feasible.

In relation to points (ii) and (iii) of the PD to be provided to Data Principals above, following issues arise:

- *It is not clear whether this provision would include the passing of the 'ownership' or 'title' of the processed data to the Data Principal or mere transfer.*
- *It is not exactly clear as to what would constitute data which is 'generated' by the Data Fiduciary, which would also be in the nature of PD? Would this extend to derivative data as well? This may result in digital businesses(s) having to forcibly share user information which may also include information / methodologies gathered by data analytics, with competitors. Hence, this may act as a disincentive for data technology innovation.*
- *It Is also not clear what constitutes 'data which forms part of the profile of the Data Principal', especially the manner in which this 'profile data' would differ from PD of the Data Principal.*

Crucially, the right to data portability may be exercised not only against SDF's but any Data Fiduciary. This includes large platforms that collect PD but also smaller companies and startups that may collect PD for the purpose of improving their services. *While large platforms may be able to sufficiently comply with these requirements but it may be difficult for smaller companies who may not have the resources to spare from their core services*. For instance, major platforms are now introducing tools to enable transferring photos from one platform to another. But introducing the obligation to provide PD in this format may be onerous for smaller companies, particularly when the standard of providing such PD is not specified. *Standards that are "commonly used" differ between developers and the general populace may not be well versed with the technicalities of various formats. Besides, the purpose of seeking such data is also important. The format for a user wanting to inspect their PD may be quite different from a format for a user wanting their PD to move to a different service. Some of these practical issues are not adequately addressed by the PDP Bill and need to be fleshed out more thoroughly.*

VIII. Right to be Forgotten

The PDP Bill introduces a 'Right to be Forgotten'. **The right can be exercised by a Data Principal only through an order of an adjudicating authority who will determine the reasonability of the request for erasure.** This right appears to apply with regard to publishers or intermediaries who may be regarded as Data Fiduciaries, such as content streaming platforms, e-commerce platforms, aggregators etc.

A Data Principal can request for an order directing the Data Fiduciary to 'restrict or prevent continuing disclosure of PD'. It is not clear at this stage whether this provision requires the Data Fiduciary to disable 'continuing disclosure' or whether it requires the Data Fiduciary to also delete the PD. In any event, a Data Principal is empowered to request for erasure of PD, which is no longer necessary for the purpose for which it was processed and the storage period limitation requires PD to be ordinarily be deleted once the purpose of processing has been achieved.

IX. Data localization

From the earlier draft, local data storage requirements have been substantially reduced. The PDP Bill now provides that SPD may be transferred outside India, but a copy of the data should be stored in India. Further, certain critical PD may be identified by the Government which should only be processed in India. Further, PD may be freely transferred and stored outside India. The intention behind the PDP Bill appears to be to make the data localization obligation applicable only for PD and SPD belonging to Indian residents, however, this has not been made clear, as the data localization obligation applies generally to SPD under the PDP Bill presently.

A few concerns arise:

Mixed data sets: It is very likely that data will be collected and stored as a mixed data set, comprising of both PD and SPD. Since, it may be practically difficult to separate the SPD from such a data set, the entire data set would have to be stored locally, due to the element of SPD. For example, as stated earlier in the Indian context, surnames of individuals would demonstrate the caste / religion of Data Principals. This may result in data collected containing items of SPD, even though it was not intended.

Critical personal data: The PDP Bill does not give any guidance/examples on what data would compromise or be notified as critical personal data. Delegation of the right to determine / notify critical PD to the Government without specific guidance under the PDP Bill grants excessive powers to the Government in relation to PDP Bill, which may not be preferable.

Data collected directly by foreign entities: It is to be determined whether data collected directly by foreign entities would be subject to the localisation requirement.

X. Cross Border Transfers

The PDP Bill proposes that SPD may be transferred outside India only when:

a. The transfer is subject to a contract or intra-group scheme (for within group entities, similar to binding corporate rules) approved by the DPA,[4] or

b. The Indian Government (in consultation with the DPA) prescribes a particular country or section within a country or a particular international organization (or class thereof) for which the transfer is permissible,[5] or

[4] The Authority may only approve standard contractual clauses or intra-group schemes that effectively protect the Data Principal's rights, including in relation to further transfers from the transferee of the PD.

[5] This would be subject to the Indian Government finding that the other country or section within a country or international organization shall provide for an adequate level of data protection for the PD, as well as effectiveness of enforcement by authorities.

c. The DPA approves particular transfer(s) for a specific purpose.

In addition to either of points (a) or (b) above being fulfilled, the Data Principal should also explicitly consent to such data transfer.

SPD may be transferred outside India subject to either points (a) or (b) above being fulfilled (similar to PD), and wherein the Data Principal has explicitly consented to such a transfer. The PDP Bill however also empowers the Indian Government to notify specific SPD that may be transferred outside India, without restriction:

- To a party outside India engaged in provision of health services or emergency services and where the transfer is required for prompt action such as to respond to a severe medical emergency, provision of medical treatment or health services or to provide safety or assistance to individual during any disaster or break-down of public order, and
- A particular country or section within a country or a particular international organization prescribed by the Indian Government for which the transfer is deemed permissible.

It appears that the Government favors the use of approved clauses / schemes between the transferor and transferee, or specifically notifying certain countries / organizations that in its view, meets adequate level of data protection and enforcement mechanism.

In addition, it is unclear as to whether the restrictions and compliances pertaining to cross border transfer of SPD would apply in the instance of direct collection of SPD of Indian Data Principals by Data Fiduciaries outside India, or if the restrictions may only apply to transfer of SPD from Data Fiduciaries in India (post collection from the Data Principal) to third parties outside India.

XI. Breach notifications

If there is a breach of PD processed by the Data Fiduciary which is likely to cause harm to the Data Principal, the Data Fiduciary should notify the Data Protection DPA of such breach. The notifications should contain certain particulars, either submitted to the DPA together or in phases. The DPA may determine if the Data Principal should also be notified of such breach.

There is no specific time period prescribed under the PDP Bill for the breach notification reporting, however, such reporting is to be done as soon as possible. The Data Protection DPA, once set up, may prescribe a certain time period for reporting.

The data breach reporting provisions prima facie appear reasonable and practical.

XII. Significant Data Fiduciary

The DPA is empowered to notify certain Data Fiduciaries or entire classes of Data Fiduciaries as SDFs.[6] The concept of an SDF appears to stem from the attempt at identifying and regulating entities that are capable of causing significant harm to Data Principals as a consequence of their data processing activities.

Accordingly, the PDP Bill proposes that such SDF register itself with the DPA and prescribes greater levels of compliances to be undertaken by such SDF, such as carrying out data protection impact assessments prior to significant processing activities, record keeping, independent data audits, and the appointment of a data protection officer.

The factors to be taken into account for the notification of SDFs are quite subjective, leaving significant discretion with the DPA. Certain obligations like a data protection impact assessment prior to commencing data processing may slow down time-sensitive Big Data exercises and have a chilling effect on experimental processing activities.

Social Media Intermediaries

New provisions have been introduced with regard to 'social media intermediaries'[7]. Any social media intermediary that has more users than a certain threshold DPA *and* whose actions may have a significant impact on electoral democracy and other public interest factors may be notified by the Central Government as an SDF. Accordingly, such a social media intermediary would be required to register itself with the DPA and comply with the other SDF obligations discussed above. In addition, the Bill requires any such social media intermediaries that are notified as a SDF to enable voluntary verification for its users in a manner that may be specified. It is not clear whether this will be specified by the DPA or the Central Government.

The definition of 'social media intermediary' has certain subjective elements, which could be contentious:

- ***Whether an organization "primarily" enables online interaction between users, since even gaming and education platforms (for instance) enable interaction between users; and***

[6] The Data Protection Authority may from time to time notify certain Data Fiduciaries (or class of Data Fiduciaries) as 'Significant Data Fiduciaries' ("**SDFs**") based on:

a. *volume of personal data processed;*
b. *sensitivity of personal data processed;*
c. *turnover of the data fiduciary;*
d. *risk of harm by processing undertaken by the fiduciary;*
e. *use of new technologies for processing; and*
f. *any other factor causing harm to any data principal from such processing.*

[7] A 'social media intermediary' is defined as "an intermediary who *primarily or solely enables online interaction* between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services" but does not include any intermediaries that primarily — (a) enable commercial or business-oriented transactions; or (b) provide access to the Internet; or (c) are in the nature of search-engines, on-line encyclopedias, e-mail services or on-line storage services.

- ***The scope of the term "commercial or business-oriented transactions" in light of ad-based revenue models.***

The introduction of these new provisions seems to be outside the overall scope of the PDP Bill and does not fit within the broad purpose of the PDP Bill as set out under the "Statement of Objects and Reasons". As per the "Statement of Objects and Reasons", the PDP Bill seeks to bring a strong and robust data protection framework for India and to set up an authority for protecting personal data and empowering the citizens' with rights relating to their personal data ensuring their fundamental right to "privacy and protection of personal data", which does not cover regulation of social media intermediaries.

In addition, the Supreme Court in *Justice K.S Puttaswamy v. Union of India*[8] has observed that the right to remain anonymous may form a part of the fundamental right to privacy. While there seems to be no conclusive ruling in India to this effect, in the United States, the right to publish anonymously is protected as part of the right to free speech. In the case *McIntyre v. Ohio Elections Commission*, the US Supreme Court said that "*Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.*" Similarly, it can also be argued that right to speak anonymously is protected by Article 19(1)(a) of the Constitution of India.

While it is possible for social media intermediaries to make verification a part of their terms and conditions for users to register on the platform (which is a matter of contract between the platform and its user), a provision that mandates social media intermediaries to verify identities of its users and then identify their accounts as verified accounts may not be preferable. However, the current provision only prescribes voluntary verification of users. It is also important to note that anonymity may operate for at least two distinct levels – anonymity of the user with respect to the company that operates a platform, and anonymity of the user with respect to other users on the platform. ***The Government could consider requesting social media intermediaries to verify user accounts for the purpose of the company that operates the platform (in order to comply with law enforcement agencies, etc.) while allowing the users to retain anonymity with respect to other users on the platform.***

XIII. Sandbox

The PDP Bill has empowered the DPA to create a sandbox in public interest for the purpose of encouraging innovation in Artificial Intelligence, Machine Learning or other emerging technologies.

Eligibility: Data Fiduciaries whose privacy by design policies have been certified by the DPA are eligible to apply.

[8] Judgment issued by the Supreme Court in Writ Petition (civil) No 494 of 2012, dated August 24, 2017.

Application: Data Fiduciaries applying for inclusion in the sandbox will have to submit the term for which it intends to use the sandbox (which cannot exceed 12 months), the innovative use of technology, Data Principals participating and any other information as may be specified by regulations.

Term: The maximum period a Data Fiduciary may use the sandbox is 3 years.

Exemptions: Participation in the sandbox will exempt the participating Data Fiduciary from certain obligations:

- To specify clear and specific purposes for collection of PD;
- Limitation on collection of PD;
- Restriction on retention of PD; and
- Any other obligation under purpose and collection limitations under Sections 5 and 6 of the PDP Bill.

The DPA is empowered to specify the penalties applicable to Data Fiduciaries participating in the sandbox, along with the compensation that can be claimed by Data Principals from such Data Fiduciaries. ***From a reading of the PDP Bill, it appears that no additional penalties would be applicable to such Data Fiduciaries other than those specified by the DPA.***

The DPA should keep in mind existing sectoral sandboxes while issuing these regulations.

XIV. Data Protection Authority

The PDP Bill also contemplates the creation of an independent data protection authority (DPA). The DPA has been given a wide range of powers and responsibilities, which *inter alia* include:

- making regulations under the PDP Bill,
- specifying the additional information to be included in a notice which the Data Fiduciary is required to provide to the Data Principal at the time of collection,
- specifying reasonable purposes of processing of PD without consent,
- prescribing regulations in respect of processing of children's PD,
- certification of privacy by design policy,
- approval of codes of practice,
- registration of 'consent managers', and
- notifying entities as SDFs

The DPA also has the power to undertake actions that are crucial for a majority multi-national corporate groups, such as the power to approve a contract or intra-group scheme by laying down conditions for cross-border transfer of SPD and critical PD.

These functions are multi-faceted as they include powers and duties which are administrative, rule-making and quasi-judicial in nature. ***The wide range and extent of delegation of legislative powers to the DPA appears to be excessive delegation of legislative powers to the DPA, which should be adequately addressed***.

XV. Codes of Practice

The PDP Bill contemplates codes of practice (similar to a self-regulatory mechanism) also to be issued by the DPA or approved by the DPA if submitted by an industry or trade association, an association representing the interests of Data Principals, any sectoral regulator / statutory authority or any departments of the Central or State Government.

These codes of practice should address more granular points of implementation including related to various compliances under the PDP Bill, such as on notice requirements, retention of PD, conditions for valid consent, exercise of various rights by users, transparency and accountability measures, methods of destruction / deletion / erasure of PD, breach notification requirements, cross-border data transfers, etc.

XVI. Privacy by design

Similar to the GDPR, the PDP Bill stipulates that Data Fiduciaries implement a policy along the lines of a "Privacy by Design" principle.[9] Further, subject to regulations made by the DPA, Data Fiduciaries may submit their privacy by design policy to the DPA for certification, which upon examination / evaluation by the DPA or its authorized officer shall be certified to be in compliances with the requirements under the PDP Bill. Such a certified policy has to be published on the website of both the Data Fiduciary and the DPA.

Hence, industry players would have to include privacy and its related principals as a part of their systems / architecture at the time of launching their business / operations itself and not as an afterthought. However, the fact that the certification requirement from the DPA is not mandatory may ease the compliance burden overall.

XVII. Exemptions

The PDP Bill also has provisions that exempt certain kinds of data processing from its application.

[9] The policy needs to contain/ specify (a) the organizational / business practices and technical systems in place to prevent harm to the Data Principal; (b) their obligations under the PDP Bill; (c) certification that the technology used to process PD is in accordance with commercially accepted / certified standards; (d) that legitimate business interests, including innovation are achieved without compromising privacy interests; (e) protection of privacy is ensured throughout the life cycle of processing of PD (from point of collection to deletion); (f) PD is processed in a transparent manner; and (f) the Data Principal's interests are accounted for at each stage of processing of PD.

Outsourcing

In what may be a welcome provision for the Outsourcing industry, the Central Government can exempt the processing of PD of Data Principals that are not within the territory of India. This can be done in respect of processing by data processors who are contracting with foreign entities. Indian outsourcing entities processing foreign individuals' data therefore may be exempt from the provisions of the PDP Bill.

Indian captive units of foreign multinationals may look forward to availing this exemption as far as foreign individuals are concerned.

Government and public interest

With respect to the Government's own processing of information, the Central Government has the power, on various grounds of public interest,[10] to direct the inapplicability of any or all provisions of the Bill to any agencies of the Government, subject to safeguards which are to be prescribed by rules.

Notably, the grounds of discretion are fairly broad and allow the government significant leeway to provide exemptions from the application of the PDP Bill, whereas civil society had expressed the hope that the PDP Bill would ensure that Government's use of personal data would be restricted to necessary and proportionate instances. Individuals will hence observe keenly whether the safeguards to be prescribed by rules under the PDP Bill will meet the principles laid down by the Supreme Court in its 2017 Right to Privacy judgment.

Processing of personal data in the interests of criminal investigation and prosecution, including "prevention", is also exempt from most provisions of the PDP Bill. ***Unlike the above provision, this exemption has not been conditioned with safeguards to be prescribed by rules. With law enforcement agencies gaining*** en masse ***access to biometric and facial recognition information, often cited to be in the interests of prevention of crime, civil society will have a significant concern on whether all such data is exempt from the safeguards in the PDP Bill.***

Small businesses; personal/domestic purposes

Certain provisions, such as the requirement to provide notice, transparency and accountability, and rights of the Data Principal, are also inapplicable in the case of PD processed by a 'small entity' where such processing is not automated. A small entity may be defined by the DPA after considering the

[10] This may be done when the Central Government is satisfied that it is necessary to do so either (a) in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order; or (b) to prevent incitement to the commission of any cognizable offence relating to any of the grounds in (a) above.

turnover of the Data Fiduciary, the purpose of collecting PD and the volume of PD processed. This provision appears intended to cover small brick-and-mortar businesses.

Other exemptions

Exemptions from many provisions of the Bill are also granted in other circumstances in connection with judicial functions, legal proceedings, and research, archiving, and journalistic purposes.

XVIII. Penalties, Offences and Compensation

The PDP Bill contemplates various streams of enforcement: penalties to be paid to the Government, compensation to the Data Principal, as well as criminal liability in certain cases.

i. Financial Penalties

The PDP Bill follows the GDPR route in terms of financial penalties by not only proposing the imposition of fixed financial penalties (ranging from Rupees 5 crore to 15 crore (i.e. approx. USD 728,600-2,185,800)) but also penalties based upon a certain percentage (ranging from 2-4%) of a Data Fidcuairy's 'total worldwide turnover' in the preceding financial year. Penalties arise in a variety of cases: violation of processing obligations, failure to implement security safeguards, cross-border data transfers, and not taking prompt and appropriate action in case of a data security breach, among others. The term 'total worldwide turnover' not only includes the total worldwide turnover of the Data Fiduciary but also that of its group entities, if such turnover of the group entity arises as a result of processing activities of the Data Fiduciary.

ii. Criminal Penalties

The PDP Bill prescribes criminal penalties for re-identifying de-identified data without appropriate consent. These criminal penalties are not limited to Data Fiduciaries or Data Processors, but 'any person', who knowingly, or intentionally reidentifies and processes PD, and extend to imprisonment for a term not exceeding three years or a fine which may extend to INR 2,00,000 (approx. USD 2,815).

The PDP Bill has diluted the criminal penalties proposed in the draft bill of 2018 (which suggested criminal sanctions for the processing of PD/SPD which caused harm to the Data Principal) by providing for criminal sanctions only for the re-identification of PDP. However, it is still not clear whether this criminal sanction is appropriate. Penalties as harsh as imprisonment may not be appropriate in a data processing context, where a right to compensation is already provided to the individual. Professors Elizabeth Pollman & Jordan M. Barry in their paper on Regulatory Entrepreneurship recognize that "if a law provides for the incarceration of the executives of a company that violate it, that may deter the guerrilla growth strategies that some modern regulatory

entrepreneurs employ". Rather, the threat of financial penalties and compensation may act as a sufficient deterrent.

Further, since the PDP Bill contains a specific clause clarifying that other laws would continue to apply, there was no requirement to include specific criminal penalties under the PDP Bill, as IPC and IT Act would continue to apply. For example, data theft may, in rare cases, if required may be punished under theft of IPC.

iii. Compensation

The PDP Bill importantly allows the Data Principal to apply to the adjudicating authority to seek compensation either from the Data Processor or the Data Fiduciary, for harm suffered as a result of any infringement of any provision in the law. ***Given some of the subjective provisions in the PDP Bill and a specialized forum for redress, this may lead to a stream of data protection litigation. This will in turn help provide guidance on subjective provisions.***

iv. Class action

The PDP Bill also appears to allow for the institution of class action suit by Data Principals who have suffered harm by the same Data Fiduciary or Data Processor. These Data Principals or an identifiable class of Data Principals can institute a single complaint on behalf of all such Data Principals for seeking compensation for harm suffered as a result of any infringement of any provision of the PDP Bill.

XIX. Road Ahead

As the PDP Bill is pending with the Parliamentary Committee, the industry should submit its views and recommendations to ensure the members of the Parliamentary Committee take into account the unforeseen implications of the current draft of the PDP Bill, and focus on the pain points for the industry. The industry should also take proactive steps to formulate rules and codes of practice, which can be submitted to the DPA.

Further, as it is unclear whether the PDP Bill will apply retrospectively and whether there is any transition period, companies may start making efforts to implement the broad framework that is mandated under the PDP Bill. In particular, any necessary system upgrades should be implemented.