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

New Data Protection Law Proposed in India! Flavors of GDPR

The much-awaited Personal Data Protection Bill, 2018 ("**Draft Bill**") was released by the Committee of Experts entrusted with creating a Data Protection Framework for India ("**Committee**") on Friday evening.

The Committee, chaired by retired Supreme Court judge, Justice Srikrishna, was constituted in August 2017 by the Ministry of Electronics & Information Technology, Government of India ("**MeitY**") to come up with a draft of a data protection law. After over a year of deliberations and a series of a public consultations followed by release of a white paper with preliminary views, the Committee has released a Draft Bill. The Draft Bill is accompanied by its report titled *"A Free and Fair Digital Economy Protecting Privacy, Empowering Indians"* (**"Report"**) which provides context to the deliberations of the Committee.

MeitY as the nodal ministry may accept, reject or alter such Draft Bill. Thereafter, the Draft Bill would need to be approved by the Union Cabinet before it is introduced in the Parliament for deliberations.

Some of the key highlights of the Draft Bill are:

- Extra-territorial application i.e. the Draft Bill is to apply to foreign data processors in so far as they have a business connection to India or carry on activities involving profiling of individuals in India.
- Differential obligations imposed based on criticality of data, i.e. differing obligations for Personal Data and Sensitive Personal Data;
- Obligations of the Data Controller (i.e. Data Fiduciary) : Notice (that is clear, concise and comprehensible), Purpose Limitation and Collection Limitation, maintaining data quality, storage limitation;
- Grounds for processing in addition to consent include use for employment purposes as well as emergencies.
- Intended to be made applicable to the State as well as private parties.
- Child Rights: Child is defined as someone who is less than 18 years of age. Profiling, tracking or behavioral monitoring of or targeted advertising towards children is not permitted.
- Rights of the Data Subject: Include Data Portability, Right to be forgotten as well as the right to correction of the data etc.
- Concept of Privacy by design and a data breach notification have also been introduced;
- High Risk Data Processors – A mandatory registration requirement has been imposed on data processors who conduct high risk processing. Such processors are required to implement: Trust Scores, Data Audits as well as a Data Protection Impact Assessment
- Data Localisation: A copy of all Personal Data must be stored in India; additionally the Government may notify certain types of personal data that should be mandatorily be processed **only** in India. The Government has retained with itself the power to exempt storage of copies of of Sensitive Personal Data, in some cases.
- Cross Border Data Flows: In addition to consent cross border transfers would also require the use of (a) model clauses; and (b) possible adequacy requirements, i.e. transfer to jurisdictions

approved by the Government;

- The Authority appointed under the Act will provide or endorse Codes of Practices.
- GDPR Style Penalties**:** Upto 4% of global turnover in some cases;
- Criminal penalties also introduced for limited cases;
- Phased manner of implementation once the law is implemented.

To summarize, whilst we believe that the Draft Bill does have its share of positives, in several places the Draft Bill is either ambiguous / not clear or imposes excessive obligations on Data Fiduciaries and prescribes disproportionate punishments. Several factors are left to be determined through Codes of Practices or to be determined by the Government at a later stage. Therefore, at this stage the full impact of the proposed law cannot be comprehended in entirety.

In several respects, we note the Draft Bill appears to have borrowed heavily from the recently notified E.U. General Data Protection Regulation ("**GDPR**"). Given the infancy at which the GDPR is at this stage, it would be imperative that law makers provide for enough flexibility for the law to be altered on the basis of global experiences. Further, we find that even the current basic law under the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*("**2011 Rules**") has yet not been implemented fully even after 7 years. Therefore, implementation will be key to this fairly detailed and somewhat cumbersome law.

We have set out in our detailed analysis below the possible implications that it may have on businesses, including offshore companies doing business in India. As we continue to read, debate and delve deeper into the wording of law, our views on several of these issues may evolve.

I. Applicability of the Draft Bill

A. Overview

Applicability of the Draft 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

B. What Kind of Data:

- Personal Data ("**PD**")[1] (data about or relating to a natural person (i.e.) who is directly or indirectly identifiable) of a Data Principal (the natural person whose data is being processed) being processed by a Data Fiduciary[2] or a Data Processor[3]; and
- Sensitive Personal Data ("**SPD**"), i.e. passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, etc.

---

[1] **"Personal data"** has been defined as *"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, or any combination of such features, or any combination of such features with any other information."*

[2] **"Data fiduciary"** means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

[3] **"Data processor"** means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

The definition of PD is extremely wide in comparison to the 2011 Rules. Barring a few provisions, the Draft Bill also applies to manual processing of PD. Thus, several non-digital businesses such as small grocery stores handling even non-sensitive PD are likely to be burdened with huge compliances, unless the Authority provides exemptions.

In addition, SPD has been treated differentially, i.e. placed on a higher pedestal requiring additional compliances as well as explicit consent for its processing.

For data localization purposes, an additional category of information is identified, i.e. "critical personal data", however, this term has not been defined at this stage.

We have discussed this in detail below.

C. *Extra Territorial Application*

In addition to being applicable to the processing of personal data collected within the territory of India, and collected by Indian citizens/companies; the Draft Bill is designed to have extra territorial application. It is linked to the processing of data of Indian Data Principals by Data Fiduciaries or Data Processors not present within the territory of India; if such processing is *"(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (b) in connection with any activity which involves profiling of data principals within the territory of India"*.

The Draft 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 a going concern, i.e., activities engaged in for the purpose of profit on a continuous and repetitive basis'.

The Draft Bill therefore incorporates both principles of territoriality and nationality in order to protect not only personal data of persons present in India; but also personal data processed by Indian companies, and personal data processed in India by foreign entities.

The Draft Bill has tried to ensure a balancing act between seeking to ensure the applicability of the Draft Bill to the PD of foreign residents, and at the same time has exempted, 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 Draft Bill in relation to applicability of the law uses a method of territorial nexus with India for establishing jurisdiction for the purposes of the Draft Bill. Under Section 2, if the data is processed by any person or entity within India, then the provisions of the Draft 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, the Committee appears to have been cognizant of the requests of the domestic data processing industry under Section 104 of the Draft Bill, which grants the Central Government the power to exempt the processing of personal data of Data Principals located outside India by Indian Data Fiduciaries, if pursuant to a contract executed with a person outside the territory of India.

D. *Extension of PD and SPD*

A quick comparison with the 2011 Rules with respect to the applicability to PD and SPD is provided

below:

- The 2011 Rules did not apply to PD but only to SPD.
- SPD under the 2011 Rules included only 6 categories: (i) password, (ii) financial information, (iii) health condition, (iv) sexual orientation, (v) medical records and history, and (vi) biometric information. The Draft Bill provides additional categories and also gives power to the Authority to identify any additional category as SPD.

Certain types of SPD are discussed below:

- Financial data: Financial data[4] has been defined to include an *account number, card or payment instrument issued by a financial institution*. 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. The architecture of the UPI makes it difficult for a third party to cause harm to the Data Principal merely by possessing the VPA. Harm, in the financial system is typically caused with the misappropriation of authentication information alongside login information and not one independent of the other.

  Therefore, the Draft Bill in its current construct would mean that storage, handling or other processing of standalone identifiers such as a VPA or a mobile number, at a standard of SPD 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 Draft Bill merely because they possess each other's payment identifiers.

  Ms. Rama Vedashree, CEO, Data Security Council of India ("**DSCI**"), a member of the Committee, recorded in a dissenting note that financial data should not have been included as SPD, stating that *"the concept of Sensitive Personal Data is primarily used for providing higher level protection to the data subject from instances of profiling, discrimination and infliction of harm that are identity driven. Neither financial data nor passwords fall into this category. It is also important to note, out of the 68 countries that presently have an overarching data protection regulation, none have categorized financial data or passwords as sensitive personal data."*
- 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, however, such inclusion could have far reaching consequences. E.g. it may affect certain functions dependent on data analytics of behavioral patterns, such as targeted advertisements, recommendations on search engines (for music and video streaming), energy efficiency technology (where energy efficiency may depend on each user's energy usage behavior analysis), and other similar services. It could possibly impact voice activated assistants and assistive technologies which are used by people with disabilities. Further, under Section 106, the Government has the overarching power of carving out certain kinds of biometric data as it may deem fit.

---

[4] Section 3(19) of the Draft Bill defines "Financial data" as "*any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history*"

- Religious or political beliefs: Interestingly, the Draft Bill also includes religious or political beliefs within the realm of SPD. However, in the Indian context, inclusion of these items do not appear to be entirely relevant.
- 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. This specifically includes a Data Principal's Aadhaar number and may also include Permanent Account Number issued for tax purposes.

E. Retrospective Applicability

The Report recommends that the Draft Bill will not apply to any processing activity completed prior to the law coming into effect. The Draft Bill will apply to any ongoing processing.

Practically this may be problematic for the following reasons:

- *Ongoing processing activity:* Given that the Draft Bill imposes obligations in relation to PD and the expanded definition of SPD, in all likelihood, data which is now covered under the Draft Bill 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 Draft Bill does not specifically clarify this.
- Further, where it is not necessary for data to be retained, then such data must be deleted in a manner to be specified. Therefore, upon the law being made applicable Data Fiduciaries may have to end up deleting data previously collected under the 2011 Rules as well as those streams of data for which they have not been granted specific consent.

F. Manual Processing

In the present day and age of digital data, the Draft Bill also interestingly leaves some room for analogue. Recognizing that large parts of the Indian hinterland continue to manually process personal data; the Draft Bill has provided for exemptions from certain provisions (as have been set out below) where '*personal data is processed through means other than automated means by a small entity*'.

'Automated means' has been defined to mean *'equipment capable of operating automatically in response to instructions given for the processing of data'*. This essentially appears to cover all forms of IT equipment on which data would be processed. Therefore, the scope of this limitation would appear to only apply to those persons who do not use any form of computer resources whilst processing PD.

Further, the only entity which is entitled to claim such an exemption is a data fiduciary which: (i) has a turnover of lesser than INR 20,00,000 (approx. USD 29,000); (ii) does not collect personal data for disclosure to others; and (iii) which does not process the data of more than one hundred Data Principals in any one day in the preceding twelve months.

Exemptions have been provided for certain provisions of the Draft Bill which consist of Notice, Data Portability, Right to be Forgotten, Transparency, Accountability measures etc.

The exclusion could have been wider. Further, startup exemptions for digital startups could also have been included.

II. Data Protection Obligations

A. Notice

The Data Fiduciary is obligated to provide a Data Principal with adequate notice prior to collection of PD as enumerated below,

- Extensive and detailed information must be provided in relation to the PD being collected, 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**").
- In a welcome move, concerns with regard to appropriate Notice have been attempted to be addressed by proposing that a Notice should be clear, concise and comprehensible and also specifies that a Notice may be issued in multiple languages whenever necessary. However, the Draft Bill is not clear as to when such multilingual notices maybe necessary.
- However, from a practical implementation perspective, we note that the information required to be shared in a Notice is extensive and detailed and is fairly granular. Some practical issues that are likely to arise are as follows:
    - 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 is 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 maybe 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 Authority has been empowered to add to the list of items to be disclosed in the Notice. It is hoped that, the Authority does not make Notice too cumbersome by including granular details, whereby it gets difficult to make it clear and concise as required under the Draft Bill.
- The Report indicates that the Authority, may issue / propose a model notice form, which may serve as a guidance to Data Fiduciaries. In a country as wide and diverse as India whilst a model notice form may serve as a good guidepost, Data Fiduciaries should be left free to decide on the form and manner of such Notice.

B. Grounds for Processing PD and SPD

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.

Processing for certain reasons such as (i) consent, (ii) employment, (iii) functions and security of the state, (iv) compliance with applicable law and legal proceedings, (v) exceptional instances such as medical emergencies, (vi) journalistic purposes, (vii) personal or domestic purposes, and (viii) research, archiving or statistical purposes are expressly recognized and lawful means for processing, for which consent is not required to be obtained from the Data Principal.

The Authority is also empowered to specify additional reasonable purposes for processing of PD and SPD.

C. *Consent*

The White Paper as well as Committee Report have devoted a significant amount of time to discussing consent and trying to find ways to fix the issues with consent under the 2011 Rules. Some key aspects relating to consent as laid down under the Draft Bill are discussed here:

- The Draft Bill lays down the test for 'valid consent' for PD, i.e. consent which is free, informed, specific, clear and capable of being withdrawn. Each of these terms are further explained.

  For SPD, explicit consent is required for which the terms "informed", "clear" and "specific" need to meet a higher threshold. The Codes of Practices to be issued or approved by the Authority are likely to provide further guidance to achieve valid consent / explicit consent.

- In an attempt to make consent more meaningful and prevent its abuse, the Draft Bill also provides that Data Fiduciaries should not be entitled to make the provision of their services / goods conditional solely on the Data Principal providing consent to collection and processing of PD *that is not essential or is not required for the provision of the services / goods by the Data Fiduciary*. Thus, businesses should be free to condition the provision of services on the receipt of consent from the Data Principal, provided that such consent is essential / required for the provision of services by the Data Fiduciary. Further, this clause may require Data Fiduciaries to expand the scope of their consent each and every time a new functionality is added.
- The Draft 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 Draft Bill. Or, 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 Draft Bill, the Data Fiduciary will need to prove absence of coercion. This goes against the basic principles of burden of proof.

D. *Ability to Process Data on grounds other than Consent:*

- In so far as other grounds of processing data are concerned, the provisions appear to be overall reasonable, however there are certain granular issues with respect to the applicability of each of these exemptions which will need to be evaluated.
- As far as the State's processing of PD goes, the Draft Bill has already drawn criticism from civil society members because it grants wide leeway to the State for the processing of data, only requiring that such data is "necessary" for a particular State function. (Note that for SPD, this has been tempered with stricter requirements). Ideally, State and non-State actors could have, to the extent practicable, been treated at par in the Draft Bill. The Draft Bill also suggests that if other laws require data processing, this law would not supersede them. This may go against the expectation of some that this would be the definitive law on data protection.

III. Aadhaar

The Report lays down that the State processes large amounts of PD in its capacity of the Data Fiduciary. Hence, the Draft Bill is proposed to be made applicable to the State.

General permission has been granted under the Draft Bill for the processing of PD for the

functions of the State and for the compliance of law under Sections 13 and 14.

Specifically, Section 13 also permits the processing of PD by the State for it to exercise its functions for providing benefits to the Data Principal and for the issuance of any certification, license or permit to a Data Principal by the State. Section 19 also provides for a general permission for the State to process SPD for the exercise of any (i) function of Parliament or any State Legislature and for the (ii) functions of the State for the provision of any service or benefit to the Data Principal as authorized by law.

The effect of these provisions is that consent of the Data Principal is not necessary for the collection of PD or SPD to achieve the State's mandated purposes. The provisions facilitate the functioning of the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016 ("**Aadhaar Act**") and the UIDAI .

However, these provisions only appear to exempt the applicability of the Draft Bill as far as consent in collection of the data is concerned (i.e., they grant a lawful ground for processing) and not from the other provisions. For instance, they do not exempt the UIDAI from the obligations to process data fairly under Draft Bill, nor do they exempt the employees of the UIDAI from the penal provisions of Section 96.

While the Report suggests certain amendments to the Aadhaar Act, interestingly, the same do not find place in the Draft Bill (although the Draft Bill suggests amendments to other laws such as the Information Technology Act, 2000 and the Right to Information Act, 2005).

The Report suggests that Aadhaar Act should be amended to bring it in line with the suggested data protection framework. The following amendments have been recommended under the Report: (i) autonomy to UIDAI in decision making and functioning independently of the user agencies, and (ii) UIDAI should be vested with powers akin to a traditional regulator for enforcement actions.

Additionally, the Report suggests that UIDAI should be vested with functions of ensuring effective enforcement, better compliance, consumer protection and prevention and redress of privacy breaches. It suggests that power should also be given to the UIDAI to impose civil penalties on errant or non-complaint entities (including requesting entities, registrars, and authentication agencies).

IV. Personal and Sensitive Personal Data of Children

Age of consent: The Draft Bill mandates that parental consent will be necessary for the processing of PD of children below the age of eighteen years. Whilst this principal is in line with the requirement under the Indian Contract Act, 1872 regarding the fact that a person must be a major (i.e. above 18 years) to form a valid contract. Other jurisdictions provide for a much lower threshold of the age of consent of children for the digital world. For example, the Children's Online Privacy Protection Act, 1998 in the US allows children of age 13 and above to consent, while the GDPR mandates age 16 as the threshold.

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

Data Fiduciaries who operate commercial websites/online services directed at children; or process large volumes of personal data of children will be notified as 'guardian data fiduciaries'.

Restrictions on Processing: These 'guardian data fiduciaries' shall be barred from undertaking any form of processing that could cause significant harm[5] to children, such as profiling, tracking, behavioral monitoring, or targeting advertising directed at children. The only entities exempted are those that exclusively provide counselling or child protection services.

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 Draft Bill. Education focused startups, who rely on targeted advertisements for example, may suffer due to the bar on processing of PD directed at children. Similarly, audio / video streaming platforms may not be able to offer suggestions based on individual preferences.

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

- The Draft Bill provides detailed rights to the Data Principal to access and correct their data. With regards to a right of review, the Draft 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 Draft Bill into a detailed step-wise process for how correction, completion or updating of the PD should be done.
  The Draft Bill requires businesses to provide the Data Principal with summaries of the PD being processed rather than the entire data dump.
- Additionally, specific obligations of Data Fiduciaries in this connection, e.g*., "to notify all relevant entities or individuals to whom such personal data may have been disclosed… where such action would have an impact on the rights and interests of the data principal"* seem quite onerous since it would appear that the Data Fiduciary bears the burden of communication to the other Data Fiduciaries who may also have an independent relationship with the Data Principal. This information may not be immediately accessible to most Data Fiduciaries, and an industry solution to share such information may have to be developed.

VI. Data Portability

In an attempt to grant users more control over their data, the Draft 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 Draft Bill however does not specify the technical specifications of such a format, or what would be threshold for 'common use' of the format.

The PD which would have 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; (iii) data which forms part of any profile on the Data Principal, or which the Data Fiduciary has otherwise obtained.**

In relation points (ii) and (iii) above, following issues arise:

[5] Please refer to Section XVII on Penalties.

- 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?
- 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.

Exemptions have been provided for instances where (i) the data processing is not automated; (ii) where the processing is necessary for compliance of law 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.

If the issue of competition was attempted to be addressed, the same should have been left to the market forces and Competition Commission of India.

Implementing data portability as a concept for all Data Fiduciaries may increase the cost of compliance, especially for start-ups. For instance, it has been argued that the data portability requirements under Article 20 of the GDPR impose a disproportionate cost on small and medium enterprises as they may lack the resources to understand and implement the law and to also implement systems for enabling the portability of the data[6]. On the contrary, by imposing such a high compliance burden uniformly and without regard to market position, a uniform data portability requirement may hinder competition in the market.

VII. Right to be Forgotten

The Draft Bill introduces a 'Right to be Forgotten' ("RTBF"). 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.

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 storage period limitation requires PD to be ordinarily be deleted once the purpose of processing has been achieved.

We note, that the RTBF appears to only apply against 'Data Fiduciaries'. Therefore, considering that 'Data Fiduciaries', by definition are those who require the disclosure of personal data and the 'determination of purpose', therefore it may be argued that public repositories of information such as a pure play search engine should not operate as a 'Data Fiduciary' and therefore be exempt from the application of this section.

VIII. Cross-border data transfers and data localization

A. Data localization and processing outside India

- As a general rule, PD can be processed outside India but at least one copy of all PD is stored on a server or a data center located in India.
- The Government may relax above requirement of local storage of a copy for certain PD on grounds of necessity or strategic interests of the State. (No further guidance is provided here). However, such relaxation is not permitted for SPD.

[6] http://ejlt.org/article/view/546/726

- Certain critical PD may be identified by the Government which should be processed only in servers / data centers India.

The Committee has suggested that such data be categorized based on enforcement and also strategic interests of the State. The Committee has suggested that data critical to the national interest of India be processed only in India. While such data is to be notified, the Committee has clarified that such data will include all kinds of data necessary for the wheels of the economy and the nation state to keep turning, specifically including "*health, government services, infrastructure data and system control software, etc*".

The Committee appears to be of the view that this localization requirement would align several interests for India, including effective enforcement of Indian law and promotion of growth in the Indian digital ecosystem. The Committee also seems aware of the costs involved in such a compliance of localizing data, but is of the view that (i) mere increase in costs cannot be a reason to introduce legal change, and (ii) costs incurred in storing / processing the data locally were not shown to override the benefits of such requirement.

Therefore, it appears that intention of the Committee was to make this obligation applicable only for PD and SPD belonging to Indian residents, however, this has not been made clear.

B. Data Transfer of PD

The Draft Bill proposes that PD may be transferred outside India only when:[7]

(i) The transfer is subject to standard contractual clauses or intra-group schemes (for within group entities, similar to binding corporate rules) approved by the Authority,[8] or

(ii) The Indian Government (in consultation with the DPA) prescribes a particular country or section within a country or a particular international organization for which the transfer is permissible,[9] or

(iii) The Authority approves a particular transfer(s) due to necessity.

In addition to either of points (i) or (ii) above being fulfilled, the Data Principal should also consent to such PD transfer.

Based on the views from the Report, the Committee was not in favor of a mutual legal assistance treaty (MLAT) mechanism with other countries for cross-border data transfers, due to the week enforceability of such mechanism. Hence, it appeared to favor use of approved clauses / schemes between the transferor and transferee, or specifically notifying certain countries / organizations that in its own view, meets adequate level of data protection and enforcement mechanism.

C. Data Transfer of SPD

SPD may be transferred outside India subject to either points (i) or (ii) above being fulfilled (similar to PD), and wherein the Data Principal has explicitly consented to such transfer.

The Draft 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 sever medical emergency, provision of medical treatment or health services or to provide

[7] Section 41 of the Draft Bill.

[8] 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.

[9] 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.

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 permissible where such transfer is necessary for a class of Data Fiduciaries or Data Principals and the enforcement of the Indian law is not hampered.

Overall, it appears from the Report that the Committee seemed in favor of allowing SPD to be transferred overseas without restriction in cases of necessity and prompt action, such as for medical emergencies.

D. Data Fiduciaries v. Data Processors

In instances where data is transferred by Data Fiduciaries to Data Processors, there should be a valid contract between both parties. The Data Fiduciary would also need to certify and periodically report to the Authority that the transfer was made under a contract adhering to the approved clauses / schemes.

The Data Processor (and its employees) is required to act under the instruction of the Data Fiduciary under the contract, unless required to do so under applicable law. Further, the Data Processor will not be able to further engage, appoint, use or involve another Data Processor on its behalf except with the Data Fiduciary's consent.

Further, if PD is transferred from a Data Fiduciary to a Data Processor under contractual clauses or intra-group schemes, the Data Fiduciary should bear any liability for the harm caused to due non-compliance of such clauses / schemes by the Data Processor

IX. Transparency and Accountability Measures

Chapter VII includes provisions for privacy by design, transparency, security safeguards, DPIA. Record-keeping, audits and data breaches. The Draft Bill also lays down certain additional obligations that are to apply to a specific class of Data Fiduciaries conducting high risk processing known as Significant Data Fiduciary.

X. Privacy by Design

The Draft Bill has proposed that Data Fiduciaries be obligated to incorporate / implement policies along the lines of a "Privacy by Design" principle, whereby privacy principles such as preventing harm, transparency, choice etc. in relation to processing and collection of PD are built into the architecture / systems of the Data Fiduciary. Resultantly, industry players would need 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. The impact of the fact that this obligation has been extended to a broader scope of collection of PD and not only SPD needs to be evaluated.

XI. Security safeguards

The Data Fiduciaries and Data Processors are required to implement appropriate security safeguards in relation to the PD. The obligations are wide, ambiguous and not specific, which may result in practical difficulties. For instance, whilst it is suggested that de-identification and encryption methods be implemented, there is no further clarity on specific requirements. Codes of

Practice will prescribe the standards of security safeguards. Thus, there is flexibility to develop different security safeguards for different nature of PD and Data Fiduciaries and Data Processors.

XII. PD breaches

The Fiduciary is required to notify the Authority in case of a PD breach where such breach is likely to cause harm to the Data Principal. Although no specific time period for reporting is prescribed in the Draft Bill, the notification is to be made as soon as possible. The Authority has been conferred with the power to prescribe specific time periods for breach notifications.

There is no specific requirement in the Draft Bill for reporting breach to the Data Principal. However, the discretion lies with the Authority to determine whether this should be done, after taking into account the severity of the harm that may be caused to the Data Principal or when the Data Principal may be required to take some action to mitigate the harm.

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

XIII. Significant Data Fiduciary ("SDF")

The Authority is empowered to notify certain Data Fiduciaries or entire classes of Data Fiduciaries as Significant Data Fiduciaries. The concept of a SDF appears to stem from the Committee's attempt at identifying and regulating entities that are capable of causing significantly greater harm to data principals as a consequence of their data processing activities. The Draft Bill proposes that such SDF register itself with the Authority to ensure that the Authority is able to track its activities.

Whilst identifying whether data fiduciaries should be categorized as a SDF, the Authority is required to consider the following parameters: volume of the personal data being processed, nature of data (sensitive or not), volume of personal data processed, type of processing activity undertaken (collection, use, disclosure), turnover of the data fiduciary, the risk of harm resulting from any processing undertaken, whether the data fiduciary is making use of any new kind of technology to carry out the processing activity, or the presence of any other harm which is likely to cause harm to the data fiduciary.

Once a Data Fiduciary is notified as a SDF, it is required to comply with the following:

- Data Protection Impact Assessment ("**DPIA**") – At the time of any (a) processing involving new technologies; or (b) large scale profiling; or (c) use of sensitive personal data such as genetic data or biometric data;, or (d) any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced until a report detailing the DPIA is submitted to the Authority. It is not clear when the first DPIA needs to be conducted, i.e. after the Draft Bill is introduced or at the time that fresh processing commences. Further, it is also not clear when / how often is such exercise to be repeated.
- Record Retention: Must maintain accurate and up-to-date records regarding particularly important processing operations, results of any security safeguard review, reports from DPIA;
- Trust Scores / Compulsory Audit: Must be done on an annual basis by an independent data auditor (empaneled with the Authority);
- Data Protection Officer: This position must be created by the Significant Data Fiduciaries as the point person for interaction with the Authority as well as responsible for implementing security measures. For those SDFs who are not in India they're required to appoint an Indian agent.

XIV. Data Protection Authority

The Draft Bill also contemplates the creation of an independent Data Protection Authority which hitherto did not exist in India.

The Authority has been given a wide range of powers under Section 60, which include inter alia enforcing the provisions of the Draft Bill, specifying residual categories of SPD, specifying circumstances a DPIA needs to be undertaken, registering Significant Data Fiduciaries and Data Auditors, etc. These functions appear to be multi-faceted as they are administrative, rule-making and quasi-judicial. In view of wide ranging rule making power, provisions have to be carefully examined to ensure that there is no excessive delegation.

In addition to its responsibilities of enforcing the provisions of the Bill, it is also heartening to see that inclusion of a Data Protection Awareness Fund, which will be funded out of the penalties recovered under the Draft Bill. In a country like India with a fast-growing digital population, the importance of educating the public on good data security practices cannot be overemphasised.

XV. Code of Practice

The Draft Bill includes elements of a self-regulatory approach for Data Fiduciaries. Authority may either itself issue code or approve the ones suggested by the Industry. It is pertinent to note that a similar provision existed in the 2011 Rules, which failed in implementation.

As the Codes of Practice are to be created within the confines of the Draft Bill, they offer an easy to use framework of best practices for data privacy which is fully compliant with the provisions of the Draft Bill. It also offers an innovative means for a Data Fiduciary to differentiate and brand itself in the market for its services. When determining whether a Data Fiduciary / Data Processor has breached provisions of the Draft Bill, the Authority may consider its compliance with such Codes of Practice.

In what appears to be an attempt to legitimise the use of Codes of Practices, the Draft Bill in various places appears to imply that the observance of Codes of Practice would be something that the Authority should evaluate whilst evaluating breach of the Draft Bill by Data Fiduciaries. For example, the Draft Bill specifically sets out that the non-observance of the Codes of Practice would be considered by the Adjudicating Officer or other judicial authority at the time of determining whether a Data Fiduciary has violated the provisions of the law.

XVI. Appellate Tribunal

Given that the Draft Bill provides for the Authority to have an adjudication wing as well, the Draft Bill also provides for the establishment of an independent Appellate Tribunal will hear the appeal from the order of the Adjudicating Officer of the Authority. The Appellate Tribunal has the powers of a civil court under the Code of Civil Procedure, 1908, but is not limited by its procedure. Appeals from the Appellate Tribunal lie directly to the Supreme Court.

XVII. Penalties, Offences and Compensation

The Draft Bill contemplates penalties to be paid to the government, compensation to the Data Principal as also criminal liability in certain cases. The Draft Bill as such differentiates between PD and SPD related offences and penalties depending on the level of harm caused to the Data

Principal (significant harm for PD offences v. harm for SPD offences).

A. Penalties and Offences

The Draft Bill goes down the GDPR route in terms of financial penalties by not only proposing the imposition of fixed financial penalties (ranging from rupees five crore to fifteen crore – (i.e. approx. USD 728,600- 2,185,800) but also penalty based upon a certain percentage (ranging from 2-4%) of its 'total worldwide turnover' in the preceding financial year, in some specific cases: processing of Children's PD, failure to implement security safeguards, data transfers, not taking prompt and appropriate action in case of a data security breach, DPIA, etc., Further, 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.

The Committee Report indicates that the intention behind such inclusion is that if the group companies have benefitted from any unlawful processing undertaken by the Data Fiduciary in India than such group entities should also be subject to penalties.

Further, in a surprising move, the Draft Bill includes criminal penalties (ranging from 3-5 years of imprisonment) for intentional, reckless and damage caused with knowledge, for certain offences such as:

- obtaining, disclosing, transferring or selling (or offer to sell) of PD, causing *significant harm* to a Data Principal;
- obtaining, disclosing, transferring or selling (or offer to sell) of SPD, causing *harm* to the Data Principal;
- re-identification and processing of previously de-identified PD, without the consent of the Data Fiduciary or Data Processor.

However, the terms *intentionally and knowingly* have not been specifically defined under the Draft Bill. Reference could possibly be drawn from the Indian Penal Code, 1860 ("**IPC**") and judicial pronouncements. Notably, all offences under the Draft Bill are categorised as cognizable and non-bailable.

The Draft Bill also provides for differential remedies in the case of *harm (for SPD related offences)* and *significant harm (for PD related offences)*. Harm has been defined to include *inter alia* bodily or mental injury, financial loss, loss of reputation, property, employment etc. Significant harm on the other hand has been defined to mean a harm that has an aggravated effect.

Specifically, the definition of harm also includes *any discrimination treatment* and *any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the Data Principal.* While the law against discrimination applies to State (i.e. under the Constitution on the grounds of religion, race, caste, sex or place of birth), there is no anti-discrimination law applicable to private bodies. In the absence of general anti-discriminatory law, such import into the data protection law seems misplaced.

The Draft Bill also provides for personal liabilities of officers of a company i.e. the company, director or responsible person, can be subject to criminal offences prescribed under the Draft Bill.

Punishment should be designed to prevent criminals from repeating their offences and should be correctional in nature. It is highly likely that threat of criminal sanctions may incentivize entities to cover up data breaches thus denying opportunities of remedial action to those affected by a breach. The law should focus on addressing issues with a data breach in an effective and timely manner and towards that end the law could also provide for alternate options such as settlement between the parties or of alternative dispute resolution mechanisms such as a formalized mediation

process.

Criminal punishment has nothing to do with prevention of offences and will only deter innovation and make business risk averse. 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".*

Further, since the Draft Bill contains a specific clause clarifying that other laws would continue to apply, there was no requirement to include specific criminal penalties under the Draft 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. It is pertinent to note that Rama Vedashree, CEO of DSCI and a committee member has also opposed the inclusion of such criminal offences in the Draft Bill, as it is draconian, excessive and impacts the enforcement mechanism. She mentioned that *"such enforcement tools should enable swift assessment and action to keep the process lean and approachable for the common man".*

B. Compensation

The Draft Bill further allows the Data Principal to apply to the Adjudicating Officer 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. The 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.

To reiterate, whilst we believe that the Draft Bill does have its share of positives, in several places the Draft Bill is either ambiguous / not clear or imposes excessive obligations on Data Fiduciaries and prescribes disproportionate punishments. It also seems to have certain unintended consequences for start ups/non digital businesses in terms of imposing exposing them to excessive compliances. Several important facets are left to be determined through Codes of Practices or to be determined by the Government at a later stage. Therefore, at this stage the full impact of the proposed law cannot be comprehended in entirety.

We hope that the law is made more balanced by diluting some of the draconian provisions as well as by issuing clarifications on the points that are not clear, after public consultation. Ideally, once the MeitY finalizes the draft, it should place such law in the public domain and provide stakeholders an opportunity to provide further inputs, before the law is placed before parliament. Given its wide ranging impact on businesses in India, another law that can negatively impact important initiatives such as 'Make in India' and 'Digital India' should be done with full transparency and engaging with stake holders. Unintended consequences of proposed draft Bill should be examined in detail and debated to avoid yet another legislation making Doing Business in India difficult and expensive.