THE PERSONAL DATA PROTECTION BILL, 2018

KEY FEATURES AND IMPLICATIONS

1. INTRODUCTION

The long awaited Personal Data Protection Bill, 2018 (the "**Bill**") was released on July 27, 2018 along with the report by the Committee of Experts under the chairmanship of Justice B. N. Srikrishna (the "**Report**"). The Committee, chaired by Justice Srikrishna, was constituted by the Ministry of Electronics & Information Technology, Government of India to put together a draft of data protection law for India. The Report elaborates on the Committee discussions and deliberations and throws light on the provisions of the Bill. The Bill may undergo further changes before it is adopted as law.

This is a keystone development in the evolution of data protection law in India. With India moving towards digitization, a robust and efficient data protection law was the need of the hour. The Bill has been drafted with an intention to fill in the vacuum that existed in the current data protection regime, and to enhance individual rights by providing individuals full control over their personal data, while ensuring a high level of data protection.

The Bill has been broadly based on the framework and principles of the General Data Protection Regulation (the "**GDPR**") recently notified in the European Union and on the foundation of the landmark judgement of the apex court: *Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors (W.P. (Civil) No. 494 of 2012)*, wherein the Supreme Court of India upheld the right to privacy as a fundamental right under the Indian Constitution. The Bill shall come in supersession of Section 43A of the Information Technology, 2000 (the "**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**IT Rules**") which was enacted under Section 43A of the IT Act.

2. KEY OBSERVATIONS

Some of our key observations on the Bill are outlined below.

2.1 Wide Definition of Sensitive Personal Data

The Bill has defined sensitive personal data to include personal data revealing or relating to password, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe. Such a broad definition of sensitive personal data (for instance, to include passwords and financial data) is not in line with international data protection laws, which have provided a much narrower definition for sensitive personal data.

Therefore, foreign companies and multinational companies would face a higher compliance requirement under the data protection law in India. Such companies may find it difficult to

adhere to these unique onerous compliance requirements, which would significantly affect their ease of doing business in India.

2.2 **Data Localization**

Every data fiduciary is required to store one serving copy of the personal data on a server or data centre that is located within the territory of India. The data fiduciaries are likely to find this obligation onerous, as it will increase operational costs for most of them. This restriction may also operate as a trade barrier and hinder the ability of global companies to transfer and process personal data across different jurisdictions.

Importantly, this requirement does not seem to be relevant in the context of a framework that seeks to protect the right to privacy of individuals. Hopefully there will be clarifications provided or interpretations evolve in the future allowing such copies of data to be backed up over periodic cycle instead of backing up on a real time basis and this may somewhat ease the burden of this obligation on data localisation.

One alternative that may have been provided is a choice for companies to either localise or have a representative like a data protection officer who is responsible for making available any data as needed by the Data Protection Authority.

2.3 **Scope of Applicability**

Under the Justice B. N. SriKrishna Report, an exception has been made based on the principle of territoriality. The Report states that any entity located in India only processing personal data of foreign nationals not present in India may be exempted from the application of the Bill by the Central Government.

However, this exemption has not been brought out in the Bill. It is likely that this exemption would be provided under the rules adopted under the Bill. But, in case no such exemption is provided under the rules, the scope and applicability of the Bill may be more over-reaching than the GDPR.

Further the term in connection with 'any business that is carried out in India', in relation to exercise of jurisdiction over any data fiduciary or data processor not located within India, is vague in nature and lacks specificity.

2.4 **Definition of Critical Personal Data**

The Bill states that critical personal data shall be only processed in a server or data centre located in India. This effectively means that such data cannot be transferred to any country outside India. It may be a challenge for businesses to service Indian consumers solely through the data centres in India. Further, the Bill does not define the term critical personal data or give any guiding principles for its determination.

2.5 **Excessive Liability**

The Bill imposes liability on the directors of a company or the officers in charge for the conduct of the business of the company at the time of commission of the offence. This seems to be draconian measure and takes an extreme stand as even most international legislations such as the GDPR do not provide, in case of data breach, for liability of the person responsible for the conduct of business.

Further, due to lack of clarity in the law, the directors and officers in-charge may be held liable to pay the same quantum of penalties as may be imposed on the company. Additionally, there is lack of clarity on the nature of liability imposed inter se between a data fiduciary and a data processor, or between multiple data processors in case of data breach.

2.6 **Repeal of Section 43A of IT Act and IT Rules**

The Bill comes in supersession of Section 43A of the Information Technology, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which was enacted under the same provision. However, there are certain provisions under the Rules, which are not specifically provided for under the Bill, for instance the disclosure of information in a privacy policy. There is lack of clarity on whether data fiduciaries need to have a separate privacy policy or whether the detailed notice requirements under the Bill would be sufficient compliance under the law.

2.7 **Employment**

Under the Bill, exemption to obtaining consent of the data principal for processing their data has been granted for certain employment related matters. However, this ground for processing of personal data can only be invoked if processing of personal data on the basis of consent is not appropriate giving regard to the employer-employee relationship between the data fiduciary and the data principal or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing activities. With the Bill coming into effect, it may pose a possible challenge for employers to continue retaining data of their former employees, obtained during the course of employment, post their separation from the employer.

2.8 **Periodic Review of Stored Personal Data**

Under the Bill, the data fiduciaries are under an obligation to conduct periodic review of the personal data stored with them so that it is not retained beyond the period necessary for the purpose of processing. The term periodic review is too general in nature and the Bill does not specify whether such periodic reviews need to be conducted monthly, bi-annually or annually. Further, this is mostly likely to increase operational costs for all companies.

2.9 **Notice**

Under the Bill, the data fiduciary is under an obligation to provide the data principal with adequate notice before collection of personal data. The notice is required to be clear and concise, and if necessary and practicable, the notice shall be in multiple languages. In a country like India with multiple languages, this may be an operational challenge and may increase the cost of compliance.

2.10 **Data Protection Authority – Scope of authority**

The Bill has vested the Authority with a wide range of administrative, discretionary, quasi-legislative and quasi-judicial powers. The exercise of powers vested in the Authority under the rules adopted under the Bill, should be in a manner to avoid any concentration of multiple conflicting powers and excessive delegation, thereby defeating the purpose of the Bill. Further, the Bill does not make any provision for filing of a class action suit or a representative suit in situations where a data breach affects large number of individuals.

2.11 **Status of TRAI Recommendations**

The Telecom Regulatory Authority of India recently released its Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector. The TRAI recommendations provide that till the adoption of a general data protection legislation, the existing rules/ license conditions applicable to telecom service providers for protection of users' privacy be made applicable to all the entities in the digital ecosystem.

Hence, it is uncertain whether the TRAI Recommendations offering sector-specific guidelines (such as encryption standards) will be applicable to data fiduciaries operating in the telecom sector along with the provisions of the Bill, or whether the TRAI Recommendations will cease to govern the privacy, security and ownership of data in the telecom sector.

2.12 **INDUSLAW View**

We believe that the Bill is a positive step towards building a well trusted and strong data protection framework in India. However, apart from the challenges and observations listed above, there are certain ambiguities that needs to be addressed and certain aspects that need to be subsequently notified or determined, before the final law can be fully implemented.

We have set out our analysis in detail below.

3. APPLICABILITY AND PURPOSE

Under the current personal data protection regime in India, which is governed by the IT Rules, all government bodies and related organizations have been excluded from its purview. However, in contrast to this, GDPR makes no such exception and its application is extended to all entities, depending on the processing of personal data. The Bill has been drafted along

this same principle and is applicable to all entities whether or not such entities are controlled or owned by the government.

The IT Act and hence the IT Rules applies to the whole of India and to any offence committed outside India by any person, if the conduct that amounts to an offence involves a computer, computer system or computer network located in India. The effect of the offence being felt in India or a threat to Indian security or the security of its citizens, and not presence of the offender in India, is the key to establishing jurisdiction.

The Bill has adopted an enhanced principle of extra-territorial scope from the provisions of GDPR. The Bill shall be applicable to processing[1] of personal data[2]: (i) where personal data has been collected, disclosed, shared or processed in any manner within the Indian territory; and (ii) where the processing has been undertaken by the government, by any Indian company, by any Indian citizen or any person or body of persons that has been incorporated under the Indian laws.[3]

So the Bill recognises the principle of territoriality and nationality in defining the scope of application. Further, the Bill shall also be applicable to processing undertaken by a data fiduciary[4] or data processor[5] not located within the territory of India (i) if such processing is in *connection with any business that is carried out in India* or if the there is *any systematic activity of offering goods and services to data principals*[6] within the territory of India (ii) in connection with any activity that involves profiling of data principals within the territory of India.[7]

The principal of extra-territorial application has been broadened under the Bill to cover offences, even in cases which do not involve a computer, computer system or computer network in India, considerably improving the privacy rights of the data principals. The long arm jurisdiction of the Bill would bring India at par with international standards of data protection. However, there is lack of clarity in the language of the law. The term 'in connection with any business that is carried out in India' is vague in nature and lacks specificity. Therefore, it would be advisable that above the term should be separately defined or an explanation should be provided.

---

[1] The term processing in relation to personal data has been defined under Section 2 (32) of the Personal Data Protection Bill, 2018 to mean an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

[2] The term personal data has been defined under Section 2(29) of the Personal Data Protection Bill, 2018 to mean 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.

[3] Section 2(1) of the Personal Data Protection Bill, 2018.

[4] The term data fiduciary has been defined under Section 2(13) of the Personal Data Protection Bill, 2018 to mean 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.

5 The term data processor has been defined under Section 2(15) of the Personal Data Protection Bill, 2018 to 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.

[6] The term data principal has been defined under Section 2(14) of Data Protection Bill, 2018 to mean any natural person whose personal data is being referred.

[7] Section 2(2) of the Personal Data Protection Bill, 2018.

The extra territorial jurisdiction of the Bill is in line with the terms of GDPR. However, there are certain difference between the two legislations. The GDPR shall be applicable if foreign data controllers (equivalent to data fiduciaries) or data processors are offering goods and services to the data subjects (equivalent to data principals) in the European Union. Processing of personal data in connection with business carried out in the European Union has been left out of its ambit.

Further, the Bill covers such processing of personal data in relation to a systematic activity of offering of goods or services to data subjects in India, unlike the GDPR which applies to all instances of offering of goods or services, including irregular and ad hoc processing of personal data. Further with regard to processing of personal data in relation of data subjects in the European Union, to monitor their behaviour, GDPR states that applies if such monitoring takes place within the territory of the European Union. In the case of the Bill, any processing of data involving profiling of data principals in India, regardless of where the profiling takes place, gets covered.

Under the Report, an exception has been made based on the principle of territoriality. It states that any entity located in India only processing personal data of foreign nationals not present in India may be exempted from the application of Bill by the Central Government. However, this exemption has not been brought out in the Bill. It is likely that this exemption would be provided under the rules adopted under the Bill. But, in case no such exemption is provided under the rules, the scope and applicability of the Bill may be more over-reaching than the GDPR.

Further, the Report has suggested that the Bill shall not be applicable retrospectively i.e. it shall only be applicable to on-going or future processing activities and shall not apply to processing activities that have been completed before the law comes into effect.

4. DATA PROTECTION OBLIGATIONS

The Bill sets out the data protection obligations that are required to be fulfilled for processing personal data of any data principal. The data protection obligations are as follows.

4.1 Fair and Reasonable

Processing of personal data shall be conducted in a manner that is *fair and reasonable* and in a manner that respects one's right to privacy.[8]

4.2 Data Quality

Ensure that the personal data that is processed is complete, accurate, not misleading and kept updated at all times.[9]

[8] Section 4 of the Personal Data Protection Bill, 2018.
[9] Section 9 of the Personal Data Protection Bill, 2018.

4.3 **Purpose, Collection, and Storage Limitation**

The personal data shall be processed only for purposes that are *clear, specific and lawful*. Processing of personal data shall be limited only to the purpose that has been specified or any incidental purposes reasonably expected by the data principal.[10]

With regard to collection of personal data, it shall only be limited to such data that would be necessary for processing.[11] Hence, broadly defined purposes, such as "improving user experience" or "marketing purposes" may not meet the standard set out under the Bill and there must be a reasonable nexus between the actual use of the personal data collected and the list of purposes stated in the notice to data principals.

Additionally, the personal data shall be retained only for the time period necessary to fulfil the purpose related to the processing.[12] The data fiduciary is under an obligation to undertake a periodic review of all its stored personal data to ensure that no personal data has not been retained for more than the necessary time period.[13]

The term *periodic review* is too general in nature and does not specify whether such periodic reviews need to be conducted monthly, bi-annually or annually. Although, such periodic review is likely to increase compliance costs for data fiduciaries, in the interest of privacy it is essential that provision should be retained and made more specific.

4.4 **Notice**

Notice is a significant step towards obtaining consent from the data principals for processing their personal data. Under the Bill, the data fiduciary is under an obligation to provide the data principal with adequate notice before collection of personal data, or as soon as reasonably possible if the personal data has not been collected directly from the data principal.

The notice shall be in a clear and concise, and if required and if practical, the notice shall be in multiple languages also.[14] Providing notice in multiple languages is an additional compliance for the data fiduciaries, considerably increasing their operational costs.

Among the other requirements regarding the contents of the notice, the notice shall state the purpose for which personal data is being processed and the categories of personal data collected. The data fiduciary shall provide its identity and contact details along with the contact details of the data protection officer (if applicable). In case, the personal data has not been collected directly from the data principal, the notice shall mention the sources from which the personal data has been collected.

[10] Section 5 of the Personal Data Protection Bill, 2018.
[11] Section 6 of the Personal Data Protection Bill, 2018.
[12] Section 10 of the Personal Data Protection Bill, 2018.
[13] Section 10 of the Personal Data Protection Bill, 2018.
[14] Section 8(2) of the Personal Data Protection Bill, 2018.

Other information such as name of the entities/ persons with which the personal data shall be shared, information regarding cross border transfer of personal data, the time period for which the personal data shall be retained shall also be included in the notice. Additionally, the notice shall also inform the data principal about its right to withdraw consent and the right to file a complaint against the data fiduciary.

If a credit score has been assigned to the data fiduciary, such credit score shall also be mentioned in the notice. The Data Protection Authority (the "**Authority**") has reserved it right to add additional information as it deems fit.

4.5 Accountability

The data fiduciary shall be accountable and responsible for protecting the personal data of the data principals. It is the responsibility of all data fiduciaries to ensure compliance with the provisions of the Bill.

The obligations of data protection are similar to the principles enumerated under GDPR, bringing the data protection obligations in line with international best practices.[15] The GDPR enumerates the following principles of data processing: lawfulness, fairness, transparency, purpose and storage limitation, data minimisation, accuracy, integrity and confidentiality and accountability.

However, under the IT Rules, the data protection obligations are limited only to the collection, use and storage of information falling in the category of sensitive personal information, excluding personal data from its ambit. Therefore, it is essential to extend the above data protection obligations to all personal data of a data principal, as achieved by the Bill.

Further, under the Bill a data fiduciary shall engage a data processor for processing personal data only through a valid contract between the two of them. However, there is a necessity that certain non-negotiable clauses be prescribed to be included in the contract between the data controller and the data processor. Further, the data processor is barred from sub-contracting with another data processor, unless there is specific clause in the agreement with the data fiduciary and data processor, allowing the same.[16] However, assuming that the data processor is permitted to sub-contract with another data processor, the Bill does not discuss the manner in which such multiple data processors would be liable for breach of any provisions of the Bill.

5. CATEGORIES OF DATA

The Bill categorises data into three different categories - personal data, sensitive personal data and critical personal data[17]. Personal Data has been defined under the Bill to mean "data

[15] Article 5 of General Data Protection Regulation, 2016.
[16] Article 37 of General Data Protection Regulation, 2016.
[17] Article 40 (2) of General Data Protection Regulation, 2016.

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 feature with any other information".[18]

The definition of personal data is in line with the definition of personal data enumerated under GDPR, Further, the definition also covers personal data that may indirectly lead to identification of a natural person. This is important as certain entities using modern technologies carry on targeting online advertisement and use an individual's online activities and pattern to customise their advertisements. Although such data gathered from one's online activities may not be identifiable individually, but when taken collectively, may result in identifying a person.

Sensitive personal data has been defined under the Bill to include personal data revealing or relating to password, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe.[19] Currently under the IT Rules, sensitive personal information includes only seven (7) categories of information, that are - password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information; and other details relating to the above categories for providing services, any of the above information received by body corporate to process data under lawful contract.[20]

Expanding the scope of sensitive personal data is not in consistent with the international standards and law, which would mean that foreign companies or multi-national companies would face stricter compliance requirements under the Indian law. Such companies may find it difficult to adhere to such onerous compliance requirements, which would significantly affect their ease of doing business in India.

However, on the positive side the remedies available to the data principal in case of data breach, extend to both breach of personal data and sensitive personal data, unlike under the IT Rules which provides for compensation only in case of breach of sensitive personal information of a data principal. With regard to the term critical personal data, the Bill does not provide any specific definition. However, it states that the Authority may notify certain categories of data to be critical personal data.

It remains to be seen whether there will be any additional data security requirements or compliances that will be prescribed in relation to critical personal data. Further, it has been stated that the Bill shall not be applicable to processing of anonymised data.[21] Even though anonymised data has been excluded from the ambit of the Bill, de-identified data continues to be treated as personal data and will be governed by the provisions of the Bill.

[18] Article 2(29) of General Data Protection Regulation, 2016.
[19] Section 2(35) of the Personal Data Protection Bill, 2018.

[21] Section 2(3) of the Personal Data Protection Bill, 2018.

6. GROUNDS FOR PROCESSING PERSONAL DATA AND SENSITIVE PERSONAL DATA

With regard to processing of personal data and sensitive personal data, the Bill provides the lawful grounds on which such data can be processed. Out of all, consent of the data principal is the primary ground for processing personal data or sensitive personal data. The others are the ground on which personal data or sensitive personal data can be processed without obtaining the consent of data principal. Such grounds of processing has been mentioned below. It is to be noted that the Bill does not provide for any separate grounds for processing critical personal data.

6.1 Consent

It is the basic ground for processing personal data or sensitive personal data[22]. The consent of the data principals shall be *free, informed, specific, clear and capable of being withdrawn*.[23] The burden of proof to establish that the consent has been giving lawfully lies with the data fiduciary.[24]

For processing sensitive personal data, in addition to the above requirements, the consent shall be provided *explicitly*, meaning that the data principal shall be informed about the possible consequences of the processing; it shall be clear without needing to refer to context in which it had been provided; and specific in the context such that the data principal has the choice to give separate consents for different purposes, operations and use of different categories of sensitive personal data relevant to the processing.[25]

This means that implied consent, inactivity or pre-checked boxes that indirectly signifies consent may no longer be acceptable modes of consent under the Bill. The GDPR also recognizes the importance of consent for processing personal data and the need for explicit consent for processing special categories of personal data.[26]

Even in India, the IT Rules, subject to certain other provisions, consent of the individual before collecting, disclosing or transferring sensitive personal information is required. However, in the case of performance of a contract, there is a difference between the two legislations.

Under the Bill, performance of a contract cannot be made contingent on the basis of the need for consent for processing personal data that is not necessary for the purpose. This is a departure from the current IT Rules, whereby entity can deny performance of a contract (such as delivery of goods or performance of service) if consent has not been given for processing personal data, regardless of whether such data is required to be processed in connection with performance of the contract or not.

---

[22] Section 12 of the Personal Data Protection Bill, 2018.
[23] Section 12 of the Personal Data Protection Bill, 2018.
[24] Section 12(4) of the Personal Data Protection Bill, 2018.
[25] Section 18 of Data Protection Bill, 2018.
[26] Article 9 of the General Data Protection Regulation, 2016.

It is evident that consent is a primary ground for processing personal data. However, consent shall not be the only ground on which consent shall be processed. The Bill makes provision for other grounds on which personal or sensitive personal data can be processed, without the need to obtain consent. Such grounds are as follows:

6.2 **Functions of the State**

Personal data or sensitive personal data (as the case may be) can be processed if such processing is necessary for the function of the parliament or any state legislature or for exercising any function of the state such as providing any service or benefit to the data principals, or for issuing any certificate, license or permit for any activity of the data principal.[27]

6.3 **Compliance with Law or Any Legal Order**

Personal data or sensitive personal data can be processed for complying with any provision of the law or any order of a court or tribunal.[28]

6.4 **Prompt Action**

Personal data and sensitive personal data can be processed without obtaining the consent of the data principal in situations where the processing is necessary to cater to medical emergencies; providing health services during any epidemic, outbreak of disease or any kind of threat to public health.[29] Further, processing of personal data can be undertaken for any prompt action that would be required in case of break down public order.[30]

6.5 **Employment Related Action**

Personal Data can be processed if it is necessary for employment related purposes such as recruitment, termination, assessment of performance, provision of any benefit to the data principal (employee), verification of attendance of the data principal.[31]

However, this ground for processing of personal data can only be invoked if processing of personal data on the basis of consent is not appropriate giving regard to the employer-employee relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing activities.[32]

Although such ground is a reasonable ground to process personal data, it is important to impose strict obligations on the employer (data fiduciary) to first take all reasonable steps to

[27] Section 13 of the Personal Data Protection Bill, 2018.
[28] Section 14 of the Personal Data Protection Bill, 2018.
[29] Section 15 of the Personal Data Protection Bill, 2018.
[30] Section 15 (c) of the Personal Data Protection Bill, 2018.
[31] Section 16(1) of the Personal Data Protection Bill, 2018.
[32]Section 16(2) of the Personal Data Protection Bill, 2018.

obtain the consent from its employee. Further, the law should clearly state that the burden of proof to establish that it was not reasonably possible for the employer to obtain consent shall strictly vest with the employer.

Additionally, many of the employers retain the personal data of their former employees for various purposes, several years post cessation of their employment. With the Bill coming into effect it may pose a challenge for employers to continue retaining data of their former employees, obtained during the course of employment, post their separation from the employer.

6.6 **Reasonable Purposes**

Personal Data can be processed for reasonable purposes as may be specified by the Authority. The Authority may specify the reasonable purposes for prevention and detection of unlawful activity including fraud, whistle blowing, mergers and acquisitions, network of information security, credit score, recovery of debt, processing personal data available in public. As such reasonable ground for processing of personal data will be set out by the Authority, there is a very limited scope for misusing this provision. Further, in this regard, the Authority would also be prescribing the safeguards for the protection of the rights of the data principals.

Under the current IT Rules, the scope of processing personal data without the consent is very limited. Information including sensitive personal information (as defined under IT Rules) can be shared with a third party without the consent of the information provider *only* with government agencies that are mandated under law to obtain such information, and for purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.[33]

Even under GDPR several grounds have been recognized for processing of personal data and sensitive personal data without the consent of the data subject. However, the scope under the GDPR is a little wider than the scope under Bill. For example, under GDPR, processing is also considered lawful without the consent of data subject, when such processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.[34]

7. PROCESSING OF PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

The Bill recognises and seeks to protect the personal data and right to privacy of children. Every data fiduciary is required to process personal data of children in a manner that protects and advances the rights and best interests of the child. Under the current IT Rules, there are no special provisions with respect to processing of personal data or sensitive personal data of

[33] Rule 6(1), proviso of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[34] Article 6(1) (b) of General Data Protection Regulation, 2016.

specifically for children. The provisions relating to processing of personal data and sensitive personal data of children are as follows.

7.1 Age limit

The Bill, defines a child to mean any data principal below the age of 18 (eighteen) years of age.[35] The age limit set out is in compliance with the provisions of the Indian Contract Act, 1872, but differs from the age limit set out in GDPR, which is 16 (sixteen) years of age.[36]

7.2 Parental Consent and Age Verification

To process personal data of children, the data fiduciary shall obtain the consent of the parents and incorporate age verification mechanism to verify the age of the child.[37] Similar obligations under the GDPR have been imposed upon the data controller.[38]

7.3 Guardian Data Fiduciaries

The Authority shall notify data fiduciaries as guardian data fiduciaries who (i) operate commercial websites or online services directed towards children, or (ii) process large volumes of personal data of children.[39] Guardian data fiduciaries shall not perform any kind of processing or profiling, tracking, behavioural monitoring of, or targeted advertising directed at, children, which causes significant harm[40] to children.[41]

However, if a guardian data fiduciary is exclusively involved in providing specified child counselling services or child protection services, it shall be exempted from obtaining parental consent.[42]

Under the GDPR, there is no such provision such as guardian data fiduciaries. However, such distinction under the Bill would be a valuable addition to the data protection regime in India, restricting all gaming websites regularly accessed by children, from exploiting the privacy rights of children.

8. RIGHTS OF DATA PRINCIPAL

The Bill grants certain rights to the data principals with regard to processing their person data, which are broadly based on the framework of the right granted to data subjects under GDPR. The rights granted to the data principals are as follows:

---

[35] Section 2(19) of the Personal Data Protection Bill, 2018.
[36] Article 8(1) of General Data Protection Regulation, 2016.
[37] Section 23(2) of the Personal Data Protection Bill, 2018.
[38] Article 8 (2) of General Data Protection Regulation, 2016.
[39] Section 23(4) of the Personal Data Protection Bill, 2018.
[40] The term significant harm has been defined under Section 2 (37) of the Personal Data Protection Bill, 2018 to mean harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm.
[41] Section 23(5) of the Personal Data Protection Bill, 2018.
[42] Section 23(7) of the Personal Data Protection Bill, 2018.

8.1 **Right to confirmation**[43]

The data principal has the right to obtain confirmation whether the data fiduciary is processing or has processed its personal data; obtain summary of the personal data that is being processed; obtain summary of the processing activities undertaken by the data fiduciary. Similarly, under GDPR, a data subject has the right to obtain confirmation from the data controller whether or not the personal data concerning him/ her is being processed. Also, under the GDPR, the data subjects have the right to access his personal data and all other information related to it.[44]

8.2 **Right to correction**[45]

The data principal has the right to demand correction of inaccurate or misleading personal data, completion of the personal data, which is incomplete and an update any personal data, which is out of date. Similarly rights to rectify and update inaccurate or incomplete personal data or information has been provided under GDPR and under the current IT Rules.

8.3 **Right to data portability**[46]

The data principal shall have the right to obtain their personal data from the data fiduciary in a *structured, commonly used and machine readable format,* where data has been processed through automated means. The data principal has a right to receive the personal data: (i) which the data principal has provided the data fiduciary, (ii) which is generated by the data fiduciary in the course of providing services or use of goods, and (iii) which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained.[47] In addition to the above, the data principal shall also have the right to transfer the abovementioned personal data to any other data fiduciary.[48]

However, the right to data portability shall not be applicable in certain situations such as- where processing is necessary for the function of the state, where processing is in compliance with an applicable law, or where processing would result in revelation of any trade secret of any data fiduciary or where it would not be technically feasible.[49]

Similarly, right of data portability has been provided to data subjects under GDPR.[50] Under the IT Rules, there is no specific provision whereby a data principal/individual has the right of portability towards its personal data.

[43] Section 24 of the Personal Data Protection Bill, 2018.
[44] Article 15 (1) of General Data Protection Regulation, 2016.
[45] Section 25 of the Personal Data Protection Bill, 2018.
[46] Section 26 of the Personal Data Protection Bill, 2018.
[47] Section 26 (1) of the Personal Data Protection Bill, 2018.
[48] Section 26 (2) of the Personal Data Protection Bill, 2018.
[49] Section 26 (2) of the Personal Data Protection Bill, 2018.
[50] Article 16 of General Data Protection Regulation, 2016.

8.4 **Right to be forgotten**

The Bill provides the data principals with a limited right to restrict or prevent the continuation of disclosure of any personal data by the data fiduciary where such disclosure (i) has finished its purpose and is no longer needed, (ii) the consent on the basis of which it was done has been withdrawn, or (iii) disclosure was made in contradiction to the provision of the Bill or any other law in force.[51]

This right may be exercised by the data principal by filing an application with the adjudicating officer[52]. Although the right to be forgotten is a part of our fundamental right to privacy, it is essential to balance such right with respect to the fundamental right to freedom of speech and expression of the general public. GDPR has also provided the data subjects with the right to erase their personal data (subject to certain conditions).[53] However, under the IT Rules, there is no specific provision whereby an individual has the option to exercise his or her right to be forgotten.

9. **TRANSPARENCY AND ACCOUNTABILITY**

The Bill has made provisions to bring in principles of transparency and accountability with respect to processing of personal data. The principles are in line with the principles of transparency and accountability provided under GDPR. The principles enumerated under the Bill are as follows.

9.1 **Privacy By Design**[54]

According to the Bill, the data fiduciaries are under an obligation to incorporate the principle of privacy by design whereby the data fiduciaries will have to incorporate various managerial, organization and business practices and technical systems to protect the personal data of the data principals and ensure the privacy of the personal data is not compromised at any stage of processing.

It shall also ensure that processing of personal data is being done in a fully transparent manner. It is also the responsibility of the data fiduciary to ensure that the technology that is being used for processing the personal data is commercially acceptable or according to certified standards, and that the right to privacy is not compromised while promoting the legitimate interests of the business. The data fiduciary at all times during the process of processing shall remain accountable for the security and privacy of the personal data of data principals. The current IT Rules mandates that the body corporate who collects, receives, stores, deals or handles information including sensitive personal information, shall have a privacy policy.

[51] Section 27(1) of the Personal Data Protection Bill, 2018.
[52] Section 27(4) of the Personal Data Protection Bill, 2018.
[53] Article 17 of General Data Protection Regulation, 2016.
[54] Section 29 of the Personal Data Protection Bill, 2018.

The privacy policy shall be displayed on the website of the body corporate, and it shall be clear and easily accessible, mentioning the kind of information it collects, the purpose for such collection, and the reasonable security measures adopted by the body corporate.[55]

Further, the language of the Bill is not clear as to whether a data fiduciary needs to have a separate privacy policy or just providing notice to the data principals (as per the provisions of the Bill) would suffice. This is particularly relevant given that the IT Rules, enacted under Section 43A of the IT Act will also stand simultaneously repealed with the coming into force of the Bill. Clarity in this regard needs to be incorporated under the Bill. Further, it is suggested that explicit provisions should be made under the Bill, whereby significant data fiduciaries (*as defined below*) should be required to have a privacy policy which shall be further displayed on its website.

9.2 **Transparency[56] and Security Safeguards[57]**

It is the obligation of the data fiduciary to take all reasonable steps to ensure that transparency is maintained at each stage of processing personal data. The data fiduciary shall make certain specified information available in an easily accessible form.

Further, the data fiduciary and data processor shall implement appropriate security safeguards for processing personal data, having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing.[58]

Periodic review of such security safeguards have to be undertaken by the data fiduciary and data processor.[59]

9.3 **Breach of Personal Data**

The Bill defines personal data breach as "*any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal.*"[60] It is the responsibility of the data fiduciary to notify a personal data breach to the Authority if such breach is likely to cause harm to any data principal.[61] The notification shall be made by the data fiduciary to the Authority as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. In contrast to the provisions of GDPR, whereby a breach of personal data shall be reported to the supervisory authority within the time period of 72 (seventy-two) hours after becoming aware of such

[55] Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[56] Section 30 of the Personal Data Protection Bill, 2018.
[57] Section 31 of the Personal Data Protection Bill, 2018.
[58] Section 31(1) of the Personal Data Protection Bill, 2018.
[59] Section 31(2) of the Personal Data Protection Bill, 2018.
[60] Section 2(31) of the Personal Data Protection Bill, 2018.
[61] Section 32(1) of the Personal Data Protection Bill, 2018.

breach[62], the Bill has left it to the discretion of the Authority to decide the timelines for reporting the breach.

Upon receiving notification, the Authority shall have the right to decide whether such breach should be notified to the concerned data principal or not, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.[63]

The discretion to report the breach to a data subject has been mentioned under in GDPR with specific ground for such notification. Under GDPR the data processors have the responsibility to communicate the incidence of such breach to the data subjects (data principals as defined under the Bill) if such data breach results in high risk to rights and freedom of natural persons.

However, if the data controller has implemented appropriate technical and organizational measures that render the personal data unintelligible to any person or has taken subsequent measures, which ensure that the high risk no longer exists, communication of the data subject about the breach shall not be required. The Bill should also similarly lay down specific grounds for reporting a personal data breach to the data principal.

9.4 **Significant Data Fiduciaries**

The Bill gives the power to the Authority to notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries based on the certain criteria such as volume of personal data that is processed, sensitivity of the personal data that is being processed, the turnover of the data fiduciary, risk or harm which results from any processing activities that is done by the data fiduciary, use of any new technology for processing by the data fiduciary, or such other relevant factors.[64]

No such classification between data fiduciaries or significant data fiduciaries have been made under the provisions of GDPR or under the IT Rules. As per the Bill, the notified significant data fiduciaries are under an obligation to register themselves with the Authority. Significant data fiduciaries have a higher responsibility to ensure transparency and accountability in the process of processing personal data.[65]

In addition to other responsibilities stated in the Bill, a significant data fiduciary shall conduct a data protection impact assessment[66] according to the provisions of the Bill, which ideally involves assessing all potential harms that may be caused to a data principal and assessing measures to minimise, mitigate or remove any risk of harm.[67] Further, significant data

[62] Article 8 of General Data Protection Regulation, 2016.
[63] Section 32 (5) of the Personal Data Protection Bill, 2018.
[64] Section 38 (1) of the Personal Data Protection Bill, 2018.
[65] Section 38 (3) of the Personal Data Protection Bill, 2018.
[66] Section 38 (3) of the Personal Data Protection Bill, 2018.
[67] Section 37 (3) of the Personal Data Protection Bill, 2018.

fiduciaries are responsible for conducting data audits, and maintaining such records as is prescribed under the Bill. [68]

Additionally, the significant data fiduciaries shall appoint an officer as the data protection officer who shall be responsible for (i) providing information and advice to the data fiduciary for fulfilling the obligations under the Bill, (ii) monitoring personal data processing activities of the data fiduciary to ensure compliance with the Bill, (iii) advising the data fiduciary, (iv) assisting and co-operating with the Authority as and when required, (v) acting as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary, and (vi) maintaining an inventory of all records maintained by the data fiduciary.

Under the Bill, a data protection officer shall be appointed by a significant data fiduciary whereas under GDPR, the obligation to appoint a data protection officer is on both the data processor and the data controller.

It should be made mandatory for all data significant data fiduciaries to obtain adequate insurance policies, commensurate with the quantum of data handled by them as well as the sector in which such data fiduciaries operate, covering any and all liability in case of data breach. Such insurance should cover their liability for any and all events relating to data breach. This is with a view to ensure that the aggrieved data principal is able to enforce the damages awarded by the Authority.

9.5 **Grievance Redressal**

Every data fiduciary shall have an effective grievance redressal mechanism to address the grievances of the data principals.[69] A data principal may raise grievances to the data protection officer (in case of significant data fiduciary), or to the designated officer (in case of other data fiduciaries).[70]

A grievance shall be effectively addressed within a period of 30 (thirty) days from its receipt. In case the grievance is not resolved within the above time frame and the data principal is not satisfied with the redressal or if the data fiduciary has rejected the grievance, the data principal has the right to approach the adjudication wing of the Authority.[71]

Appeals from the adjudicating authority shall lie with the appellate tribunal established under the Bill.[72] Appeals from the appellate tribunal shall lie with the Supreme Court of India.[73] This grievance redressal process is similar to the grievance redressal mechanism stated in the current IT Rules.

[68] Section 38 (3) of the Personal Data Protection Bill, 2018.
[69] Section 39 (1) of the Personal Data Protection Bill, 2018.
[70] Section 39 (2) of the Personal Data Protection Bill, 2018.
[71] Section 39 (3) of the Personal Data Protection Bill, 2018.
[72] Section 39 (4) of the Personal Data Protection Bill, 2018.
[73] Section 87 of the Personal Data Protection Bill, 2018.

Under the IT Rules, a body corporate has the obligation to appoint a grievance redressal officer and the contact details of such grievance redressal officer shall be clearly displayed on website of the body corporate. It is essential that the Bill incorporates the requirement to display the contact details of the data protection officer (in case of significant data fiduciaries) or designated officer on their website.

This will enable the data principals to easily contact the concerned officer resulting in speedy grievance redressal. Therefore, incorporating a robust grievance redressal mechanism would pave the way for a trusted data protection regime in India.

10. CROSS BORDER TRANSFER OF PERSONAL DATA

The Bill imposes strict regulations on the transfer of personal data outside the territory of India.

10.1 Data Localisation

As per the Bill, every data fiduciary shall store one serving copy of the personal data on a server or data centre that is located within the territory of India.[74] However, the central government has the right to exempt certain categories of personal data from the above requirement[75] on the grounds of necessity or strategic interests of the State, but sensitive personal data in no way will be exempted from the above requirement.[76]

The obligation to store a copy of the personal data that is being transferred outside India, within the territory of India may not be accepted and may be criticised as it is likely to increase operational costs for most entities, especially for start-ups. This will also hinder the ability of global companies to transfer and process personal data across different jurisdictions. Even under the GDPR, there is no obligation to store a copy of the personal data in the member country to which the data relates. This may affect ease of doing business with India.

10.2 Critical Personal Data

The Bill imposes and absolute restriction on processing of critical personal data (personal data as notified by the Central Government) stating that such critical personal data shall be only processed in a server or data centre located in India.[77] This effectively means that such data cannot be transferred to any country outside India. It may be a challenge for businesses to service Indian consumers solely through the data centres in India. It is important to have the term critical personal data clearly defined to avoid confusion or misrepresentation.

[74] Section 40 (1) of the Personal Data Protection Bill, 2018.
[75] Section 40 (3) of the Personal Data Protection Bill, 2018.
[76] Section 40 (4) of the Personal Data Protection Bill, 2018.
[77] Section 40 (2) of the Personal Data Protection Bill, 2018.

10.3 **Conditions for Cross Border Transfer**

The Bill has laid down the conditions for transferring personal data outside the territory. Such of these conditions are as follows.[78]

(a) Transfer of data is according to standard contractual clauses or inter-group schemes that have been approved by the Authority;

(b) The central government in consultation with the Authority has prescribed a country or section within a country or a particular international organization where such transfers are permissible based on the adequacy of the data protection framework in such country and monitoring of circumstances applicable to such data; or

(c) A particular transfer is approved by the Authority on grounds of necessity.

Along with the above 3 (three) conditions the data principal shall consent and explicitly consent to the transfer of personal data and transfer of sensitive personal data, respectively.[79] Further, the Bill also lays down additional requirement for transferring sensitive personal data clearly (as notified) outside the territory of India.[80]

Under the current IT Rules, sensitive personal information or any information may be transferred to a body corporate or person outside India that ensures the same level of data protection that is to be adhered under these Rules. Further, the transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate and provider of information or where such person has consented to data transfer.[81]

11. **DATA PROTECTION AUTHORITY**

The Bill establishes an independent body called the Data Protection Authority[82] of India. Currently, there was no such independent authority under the present data protection regime in India. The Data Protection Authority shall possess all characteristics of a body corporate.[83] The Authority shall consist of a chairperson and 6 (six) whole time members.[84]

The Bill has vested the Authority with a wide range of powers.[85] Such powers may be divided into the broad head of administrative, discretionary, quasi-legislative and judicial powers. It remains to be seen the manner in which the exercise of powers vested in the Authority shall be prescribed under the rules adopted under the Bill, to avoid any concentration of multiple conflicting powers and excessive delegation, thereby defeating the purpose of the Bill.

[78] Section 41(1) of the Personal Data Protection Bill, 2018.
[79] Section 41(1) (d), Section 41 (1) (e) of the Personal Data Protection Bill, 2018.
[80] Section 41 (3) of the Personal Data Protection Bill, 2018.
[81] Rule 7 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[82] Section 49 of the Personal Data Protection Bill, 2018.
[83] Section 49 (2) of the Personal Data Protection Bill, 2018.
[84] Section 50 (1) of the Personal Data Protection Bill, 2018.
[85] Section 60 of the Personal Data Protection Bill, 2018.

Further, the Bill does not make any provision for filing of a class action suit or a representative suit in situations where a data breach affects large number of individuals.

12. EXEMPTIONS

The Bill list down certain categories that are exempted from application of the Bill in whole or part. The exempted categories are- security of state, prevention detection, investigation or contravention of law, processing for purposed related to legal proceedings, research, archival or statistical purposes, personal or domestic purposes, journalistic purposes or processing done by small entities.

13. PENALTIES AND OFFENCES[86]

The Bill takes the road of GDPR by imposing different penalties for contravention of various provisions. In additional to penalties, the Bill also provides for imprisonment for offences such as obtaining, transferring or selling personal data in contravention to the Bill, re-identification and processing of de-identified personal data. All offences under the Bill are cognizable and non-bailable.[87]

Further, the Bill imposes liability[88] on the directors of a company or the officers in charge for the conduct of the business of the company at the time of commission of the offence. This seems to be draconian measure and takes an extreme stand as even international legislations such as the GDPR do not provide for liability in case of data breach, of the person responsible for the conduct of business of the company, in addition to the company itself. Further, due to lack of clarity in the law, the directors and officers in-charge may be held liable to pay the same quantum of penalties as may be imposed on the company. Additionally, there is lack of clarity on the nature of liability imposed inter se between data fiduciary and a data processor, in case of data breach.

In addition to the penalties and imprisonment, the Bill also gives right to the data principals to claim compensation for data principals who have suffered harm as a result of violation of any provision of the Bill.

14. TRAI RECOMMENDATIONS AND THE PERSONAL DATA PROTECTION BILL, 2018

The Telecom Regulatory Authority of India had released its Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (the "**TRAI Recommendations**") on 16 July, 2018. The TRAI Recommendations highlights the importance of data privacy and data protection in the sector which is driven by telecommunications and digital services. The Bill, to some extent, has incorporated the TRAI Recommendations.

[86] Chapter xi and Chapter xiii of the Personal Data Protection Bill, 2018.
[87] Section 93, of the Personal Data Protection Bill, 2018.
[88] Section 95 of the Personal Data Protection Bill, 2018.

The TRAI Recommendations also state that entities collecting and processing data are mere custodians or fiduciaries and do not have any primary rights over such data. TRAI Recommendations on rights of individuals with respect to choice, notice, consent, portability and right to be forgotten, in the telecommunication sector have been recognised and incorporated under the Bill, subject to certain limitations. The Bill has also incorporated the principles suggested in the TRAI recommendations, which are: privacy by design, data minimisation, purpose limitation and collection limitation.[89]

The TRAI Recommendations stresses the importance of conducting a hybrid model of audit (which would be a combination of both technology based and human based audit).[90] Under the Bill, audit obligations have been made compulsory for significant data fiduciaries. With regard to cross border flow of data, the Bill has incorporated TRAI's Recommendation suggesting the need to localise sensitive critical data such as financial data, data related to healthcare.[91]

However, there is no particular definition of critical sensitive data under the Bill and it is up to the Central Government to notify personal data as sensitive personal data.[92] However, the TRAI recommendations provide that till the adoption of a general data protection, the existing rules/ license conditions applicable to telecom service providers for protection of users' privacy be made applicable to all the entities in the digital ecosystem. [93] Hence, it is uncertain whether the TRAI Recommendations offering sector-specific guidelines will be applicable to data fiduciaries operating in the telecom sector along with the provisions of the Bill, or whether the TRAI Recommendations will cease to govern the privacy, security and ownership of data in the telecom sector.

This is relevant because certain recommendations, such as encryption standards, are critical to the telecom sector and may not be adequately addressed with the provisions of the Bill, which are more generic in nature.

DISCLAIMER

This article is for information purposes only. Nothing contained herein is, purports to be, or is intended as legal advice and you should seek legal advice before you act on any information or view expressed herein.

Although we have endeavoured to accurately reflect the subject matter of this article, we make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this article.

No recipient of this article should construe this article as an attempt to solicit business in any manner whatsoever.

[89] Para 2.57 of TRAI Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector.
[90] Para 2.91 of TRAI Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector.
[91] Para 2.143 of TRAI Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector.
[92] Section 40 (2) of the Personal Data Protection Bill, 2018.
[93] Para 2.39 of TRAI Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector.

Authors: Suneeth Katarki | Namita Viswanath | Ivana Chatterjee

Date: August 3, 2018

Practice Areas: Technology, Media & Telecommunications