SAMVĀD: PARTNERS

August 8, 2018

PERSONAL DATA PROTECTION BILL, 2018

INTRODUCTION:

The Central Government published the draft Personal Data Protection Bill, 2018 (the PDP Bill) on July 27, 2018. The PDP Bill follows from the recommendations put forward by the Justice Srikrishna Committee on data security. The PDP Bill is a one-of-a-kind legislation in India which seeks to address the issue of data protection in India and to implement the right to privacy. Prompted by the 2017 decision of the Supreme Court in *Justice Puttusamy vs Union of India*, the PDP Bill recognizes the existence of a fundamental right to informational privacy enforceable against non-state actors. The timing of the PDP Bill is interesting, having come out within just a little more than 2 months after another paradigm-changing legislation, the European Union's General Data Protection Rules (GDPR), became enforceable. Even a preliminary reading of the PDP Bill yields the observation that its owes much to the GDPR, borrowing much of the scaffolding by which the processing of data and the actors involved in such processing are understood, utilizing many elements of the GDPR's rights-based framework and creating a regulatory structure with strictures similar in certain ways to the GDPR's. The PDP Bill adopts a consent-based approach establishing obligations between a person processing personal data and the person providing such data.

The PDP Bill is presently pending before both the Houses of Parliament for further discussions and amendments, if any, before it is notified as a law.

BACKGROUND

Presently, the only substantial law governing data privacy in India is the Information Technology Act, 2000 ("IT-Act") and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("IT-RS Rules").

APPLICABILITY vis-à-vis EXEMPTIONS:

The PDP Bill is applicable to any data processing activities which are carried on in India or by an Indian entity. The PDP Bill would only apply to foreign entities if such entities (i) have a business connection in India; or (ii) systematically offer goods and services in India; or (iii) engage in profiling of individuals in India. In all such cases, a foreign entity is required to appoint a representative in India. Much like the GDPR, the term "processing" is expansive in scope and, inter alia, includes the collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, and use of data. The wide ambit of the PDP Bill ensures that entities outside India which process the personal data of an individual in India would come under the purview of the Bill. The expanded scope of applicability of the PDP Bill is a change from the present limited scope of the IT-RS Rules which only apply to bodies corporate and persons located in India.

The PDP Bill provides for certain exemptions when processing is carried out pursuant to (i) security of the state; (ii) prevention, detection, investigation and prosecution of contraventions of law; (iii) processing for the purpose of legal proceedings; (iv) research, archiving or statistical purposes; (v) personal or domestic purposes; (vi) journalism; and (vii) manual processing by small entities. It is relevant to note that the scope of exemptions under the PDP Bill are wider than the scope of exemptions under the GDPR.

PLAYERS IN THE BILL:

The key participants in the PDP Bill are the (i) data principal who is the natural person from whom the personal or the sensitive personal data is collected; (ii) data fiduciary who determines the purposes and means of processing the data; and (iii) data processor who processes the data on behalf of the data fiduciary and who may also be the data controller in some cases. Where the data processor is not the data fiduciary, the data processor is required to enter into contract with the data fiduciary and such contract will govern the activities of the data processor. An exemption has been given to a data processor from the requirement of maintaining records. The PDP Bill has also defined the roles and responsibilities of each key player with regard to the processing of data.

DATA PROTECTION AUTHORITY TO BE CREATED:

Pursuant to the Bill, an independent Authority will be constituted as a body corporate having perpetual succession and a common seal within 3 months from the notified date[1]. The Authority will comprise of a chairperson and six whole time members having specialised knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects. The Authority would be empowered to exercise functions as mentioned in the PDP Bill and also be permitted to have offices across India. The IT-RS Rules did not envisage any kind of regulatory structure to deal with data protection. Accordingly, the authority created under the PDP Bill will be the first authority to regulate data protection in India.

OBLIGATIONS OF THE DATA FIDUCIARY:

- Notice / Privacy Policy: Under rule 5 of the IT-RS Rules, a body corporate or any person on its behalf who is collecting information directly from a person is required to take steps to ensure that the person providing data has knowledge of (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.

  The PDP Bill has similar but much more detailed provisions pursuant to which a data fiduciary is required to provide a notice to a data principal at the time of collection of data. The contents of the notice are more comprehensive than the requirements under Rule 5 of the IT-RS Rules. In addition to the requirements under Rule 5 of the IT-RS Rules, the notice should inter alia contain (a) the right of the data principal to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; (b) the source of such collection, if the personal

[1] Any date within 12 months from the date of enactment of the bill

data is not collected from the data principal;(c)information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; (d) the period for which the personal data will be retained or where such period is not known, the criteria for determining such period; (e) the existence of and procedure for the exercise of data principal rights; (f) the procedure for grievance redressal; (g) the existence of a right to file complaints to the Authority;

- Fair and Reasonable Processing: Under Rule 5 of the IT-RS Rules, a body corporate is permitted to collect information for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf.

  On similar lines, the PDP Bill also imposes an obligation on the data fiduciary to process personal data in a fair and reasonable manner that respects the privacy of the data principal.

- Purpose Limitation: Both the PDP Bill and the IT-RS Rules contain provisions to the effect that only such information should be collected as is necessary for processing.

- Storage Limitation: Both the PDP Bill and the IT-RS Rules state that personal data collected should be retained only for a period as long as may be reasonably necessary to satisfy the purpose for which it is processed.

  The PDP Bill imposes an additional obligation on the data fiduciary to mandatorily conduct a periodic review in order to determine whether it is necessary to retain the personal data in its possession.

- Data Quality: While the IT-RS Rules do not specifically impose any obligation regarding data accuracy or quality, they grant a right to the data principal to rectify any information provided. Rule 5(6) of the IT-RS Rules limit the obligation on a body corporation collecting for being responsible for the authenticity of the personal information or sensitive personal data or information provided by the provider of the data.

  The PDP Bill states that a data fiduciary should take reasonable steps to ensure that the personal data to be processed should be complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.

- Grounds for Lawful Processing: The IT-RS Rules do not specifically state lawful grounds for processing of personal information or sensitive personal information. The PDP Bill specifically states the grounds which constitute lawful processing of data. Such grounds include (a) obtaining consent from the data principal for the processing of personal data. The consent should be free, informed, specific and capable of being withdrawn; (b) processing for any function of the state/Parliament; (c) processing permitted in compliance with law, order of court or tribunal; (d) processing of personal data in the capacity of an employer of the data principal; and (e) processing for reasonable purposes. Grounds to determine reasonable purposes include (a) interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the effect of the processing activity on the rights of

the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing.

- Processing of Sensitive Personal Data: Rule 3 of the IT-RS Rules defines Sensitive Personal Data as personal information relating to (a) passwords; (b) financial information; (c) physical, physiological or medical information; (d) sexual orientation; (e) medical records or history; (f) bio-metric information; (g) any detail related to the above which is provided to the body corporate collecting information. The IT-RS Rules obligate a body corporate to seek consent from the provider of sensitive personal data regarding the purpose of usage of such data before collection of the data. Further, processing of sensitive personal data under the IT-RS Rules is only permitted (a) for a lawful purpose in connection with the activities of a body corporate collecting such data; or (b) the collection of sensitive personal data is necessary for the purpose.

  Sensitive Personal Data under the PDP Bill has been defined as personal data revealing, related to, or constituting (a) passwords; (b) financial data; (c) health data; (d) official identifier; (e) sex life; (f) sexual orientation; (g) biometric data; (h) genetic data; (i) transgender status; (j) intersex status; (k) caste or tribe; (l) religious or political belief or affiliation; or (m) any other category of data specified by the Authority. Sensitive Personal Data should be processed only when explicit consent has been obtained. The PDP Bill defines the criteria of explicit consent as being consent which is (a) clear; (b) informed and (c) specific. Further, processing of Sensitive Personal Data is permitted for (a) carrying out functions of the State; (b) compliance with law or any order of any court or tribunal; (c) undertaking prompt action in situations of (i) medical emergency; (ii) restoring public order; (iii) restoring public health

- Other Obligations: In addition to the primary obligations mentioned above, the PDP Bill also imposes obligations with respect to (a) conducting an annual audit by an independent data auditor for audit of the data fiduciaries policies and the conduct of its processing of personal data; (b) maintenance of records; (c) conducting a data impact assessment; (d) appointing a data protection officer; (e) ensuring grievance redressal within a maximum period of 30 days etc.

- Unfettered rights to state actors: An important introduction by the PDP Bill is the unfettered right to process data by state actors. A reading of the PDP Bill brings out the clear lack of restrictions on processing data by state actors, thereby granting them broad powers with regard to data processing.

- Privacy obligations: The data fiduciary is required to implement policies and measures to ensure that the privacy of the data collected is maintained by inter alia ensuring that managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal.

RIGHTS OF CHILDREN:

The IT-RS Rules did not specifically provide for protection of data belonging to children.

Taking a lead from the GDPR, the PDP Bill has also imposed additional restrictions while processing data of children. The PDP Bill defines children as persons below the age of 18 years. The PDP Bill introduces mechanisms for age verification and parental consent to be taken by

data fiduciaries in order to process the personal data of children. The PDP Bill has also introduced a concept of guardian data fiduciaries, which was absent in the GDPR. Guardian data fiduciaries are data fiduciaries who operate commercial websites or online services directed at children or who process large volumes of personal data of children. Guardian data fiduciaries are barred from profiling, tracking, or behavioral monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child

RIGHTS OF A DATA PRINCIPAL:

The IT-RS Rules does not adopt a rights-based approach in protecting individual data. The IT-RS Rules do provide for certain options the including the option to opt-out of providing information, the option to withdraw consent and the option to rectify their personal data.

The first line of the preamble of the PDP Bill, on the other hand, recognizes the need to protect personal data as a facet of information privacy in the context of privacy being a fundamental right. In order to implement a rights-based regime, the PDP Bill expressly grants a data principal rights such as the (a) right to access and confirmation; (b) right to rectify the data provided. However, a data fiduciary has the power to decline a data correction request by a data principal by providing justifiable reason. Further, the data fiduciary should take reasonable steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion or updating; (c) right to data portability; and (d) right to be forgotten subject to certain conditions such as (i) Withdrawal of consent; (ii) Personal data has served the purpose and is no longer necessary; (iii) Disclosure of personal data is made contrary to the provisions of law.

DATA BREACH:

The IT-RS Rules do not specifically state the procedure which is required to be followed by a body corporate upon the occurrence of a data breach. Rule 8 of the IT-RS Rules state that upon the occurrence of a data breach, the body corporate may be required to demonstrate compliance with security control measures as per their documented information security programme and information security policies.

The PDP Bill has also laid down a procedure to be followed in case of a data breach by a data fiduciary or data processor. In the event of data breach, the data fiduciary is required to notify the Authority of such breach of personal data likely to cause harm to the data principal. The notification to the Authority should contain the following particulars: (a) nature of personal data which is the subject matter of the breach; (b) number of data principals affected by the breach; (c) possible consequences of the breach; and (d) measures being taken by the data fiduciary to remedy the breach.

Further, the aforesaid notification is required to be provided within a specified time period 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.

Upon receipt of notification, the Authority will determine whether such breach should be reported by the data fiduciary to the data principal and also direct the data fiduciary to take appropriate remedial action as soon as possible. The data fiduciary should also conspicuously post the details of the personal data breach on its website. The PDP Bill also imposes an

obligation on the data fiduciary to adopt any urgent measures to remedy the breach or mitigate any immediate harm caused due to such data breach.

CROSS BORDER TRANSFER OF DATA:

The IT-RS Rules state that a body corporate must seek prior permission of the information provider before disclosing such information to a third party except where such transfer was mandated under law.

The PDP Bill has strengthened the protection afforded to a data principal in case of a cross-border transfer. The PDP Bill has introduced a 'data localisation' requirement on the data fiduciary to ensure that at least one copy of the data collected is stored on a server or data centre located in India. This requirement may be relevant for entities operating in India with data storage happening remotely. This requirement may require entities to configure their business models appropriately to be in compliance with the Bill. Further, the PDP Bill permits cross border transfer only under compliance with certain conditions the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority such as:

a) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organization is permissible only if the relevant personal data shall be subject to an adequate level of protection;

b) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or

c) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or

d) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data required to be stored only on servers and data centres located in India and as notified by the Central Government.

PENALTIES:

As per Section 43 A of the IT Act, if a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, in negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The IT Act does not state any cap on the compensation payable to an aggrieved party.

Similar to the GDPR, the PDP Bill also envisages penalties extending up to INR 5,00,00,000 or two per cent of total worldwide turnover of the preceding financial year, whichever is higher, for non-compliances with the procedural requirements of the PDP Bill such as appointment of a data protection officer, conducting a data audit, conducting a data impact assessment etc. In contrast, non-compliance with the requirements of the PDP Bill regarding processing of personal

or sensitive personal data may lead to higher penalties extending upto INR 15,00,00,000 or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher.

Conclusion:

In summary, the PDP Bill envisages a much more detailed and stringent regime for data protection in India than was covered by the IT-RS Rules. The PDP Bill's proposed introduction of a data protection authority and a regulatory structure for dealing with data protection is also at variance with the IT-RS Rules. It is important to note that, while the provisions of the PDP Bill envisage stringent regulatory system for private entities, they provide wide exemptions for the processing of data by the State, provided such processing is considered 'necessary' for the functioning of the State or the provision of State services/benefits or certifications/licenses. One advantage of the PDP Bill is that it provides broad parity to Indian industries with the GDPR which may go a long way towards ensuring that authorities in the EU grant a recognition of adequacy with Indian industries that are compliant with the final act that results from the PDP Bill. While the PDP Bill is a significant attempt to solve issues of data security in India, much remains dependent on how the law resulting from the PDP Bill will finally be passed in the Parliament.

This is an update for general information purposes only and does not constitute legal advice. Please contact us if you require further clarifications on this subject.

Mr. Rohan K George
Partner, Chennai
rohan@samvadpartners.com

Ms. Sanjana Srivastava
Associate, Chennai
sanjana@samvadpartners.com