Analysis

The Personal Data Protection Bill, 2019

12 December 2019

The Personal Data Protection Bill, 2019 aims to protect the privacy of individuals with respect to their personal data and governs the relationship between individuals and entities processing their personal data. It simultaneously strives to create a robust digital economy by ensuring innovation through digital governance.

1. Introduction

The Personal Data Protection Bill, 2019 (PDP Bill) was introduced in Parliament on December 11, 2019.

The PDP Bill is based on the draft legislation submitted to the Ministry of Electronics and Information Technology (MeitY) by a nine-member committee of experts headed by Justice B.N. Srikrishna (Committee) in July 2018. The draft legislation submitted by the Committee recommended significant changes in the way data is processed in India, and included requirements such as localisation of personal data, restrictive conditions for transfer of personal data, penalties for reckless de-identification of data, and the creation of a Data Protection Awareness Fund. The PDP Bill substantially modifies the draft of the Committee and also introduces new constructs such as consent managers and social media intermediaries and confers greater powers on the Data Protection Authority and the Central Government.

In a significant departure from the Committee draft, the mechanism for the phased implementation of the provisions of the PDP Bill has been done away with, and the various provisions the law will come into force on the dates on which they are notified.

This update provides a brief overview of the provisions of the PDP Bill.

2. Definitions

Section 3 of the Draft Bill lays down several important definitions.

(a) Personal data and Sensitive personal data

The PDP Bill treats both personal data and sensitive personal data separately and specifies different obligations in
Personal data is defined as data about or relating to a natural person who is directly or indirectly identifiable, having regard to a feature of identity or a combination of such features (whether virtual or physical) and also includes inferences drawn from such data that for the purpose of profiling.

Sensitive personal data is personal data that reveals, is related to, or constitutes financial data, health data, official identifiers, sex life and sexual orientation, biometric data, genetic data, transgender status, intersex status, and caste or tribe, religious, political belief or affiliation, and any other category as may be notified. In a departure from the construct under the previous version of this Bill, passwords are no longer classified as sensitive personal data, similar to the position under the European Union's General Data Protection Regulation, 2016 (GDPR).

The natural person whose personal data is collected is referred to as the 'data principal' and the entity that determines the purpose or means of processing this data is referred to as the 'data fiduciary'. Data fiduciaries can include the State, corporate entities and individuals.

Processing is defined broadly, to encompass most operations on data including storage, adaptation, retrieval, dissemination, and erasure or destruction.

(b) Financial Data

The term 'financial data' is defined narrowly in the PDP Bill. Section 3(19) defines financial data as any number or other personal data that is used to identify (i) an account opened by a data fiduciary, or (ii) a card or payment instrument issued by a financial institution. It is also defined to include personal data regarding the relationship between a financial institution and a data principal including financial status and credit status.

Other types of data like account statements, data relating to other financial products and investment information are not included within the definition of financial data.

(c) Anonymisation

Anonymisation is defined as an irreversible process of transforming or converting personal data to a form in which the data principal cannot be identified as per the standards of irreversibility laid down by the Data Protection Authority (DPA). This provision provides a greater degree of certainty than the Committee draft, since the data will be considered to be anonymised as long as they comply with the standards laid down by the DPA.

(d) Harm

Under the PDP Bill, 'harm' is defined to inter alia include any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal. What constitutes an 'evaluative decision' has not been clarified under the PDP Bill; however, it would likely include predictive decisions based on data-processing that determine whether a data subject should be provided with certain entitlements such as credit, employment etc. The definition of 'harm' does not make a distinction between evaluative decisions that are prejudicial to or discriminatory against the data principal and evaluative decisions that are otherwise justifiable. Hence, it is conceivable that the mere act of denying a data principal certain goods, services, or benefits based on an evaluative decision could constitute a harm against the data principal.

While data principals can only claim compensation for a harm suffered as a result of any violation of any provision under the PDP Bill, and not for a harm per se, this may have certain unintended consequences. For instance, if the data fiduciary is unable to provide the data principal with a summary of the processing undertaken to make the evaluative decision, thereby violating the data principal's right to confirmation and access provided in Section 17, then the data principal could claim compensation, even though the denial of service may be entirely justified.

Further, unlike the GDPR, the definition of 'harm' under the PDP Bill extends to all types of evaluative decisions.
regardless of whether humans are involved or not. Such a broad definition may have a chilling effect on data-based predictive decision-making.

3. Applicability

The PDP Bill, applies to the processing of personal data that has been collected disclosed, shared or otherwise processed in India, or to the processing by the State or State bodies, Indian corporate entities and Indian citizens. The PDP Bill also applies to the processing of any personal data by entities located outside India if the personal data is processed with respect to any business or activity that involves offering goods or services to individuals located in India or the profiling[1] of data principals within India. However, any such activity must specifically target Indian citizens and the provision of goods or services must not be incidental.

The PDP Bill does not apply to the processing of anonymised data.

Additionally, the PDP Bill gives powers to the Central Government to exempt from the application of the Bill, the processing of personal data of data principals not within the territory of India, pursuant to a contract entered with any person/company incorporated outside India, by any data processor incorporated under Indian law.

4. Obligations of Data Fiduciaries

Similar to other privacy legislations, the PDP Bill imposes several obligations on data fiduciaries with respect to collection and processing of personal data as set out below:

(a) Purpose Limitation and Collection Limitation

The PDP Bill prohibits the processing of personal data by any person, except for a specific, clear and lawful purpose. Every person processing personal data is mandated to process personal data in a fair and reasonable manner such that it does not go beyond the reasonable expectations of the data principal. This obligation extends to data processors with whom the data fiduciary may have shared the personal data for fulfilment of the purpose.

(b) Notice

The data fiduciary is obliged to provide notice to the data principal at the time of collection of personal data of the data principal, even if such personal data is not being collected from the data principal directly. This notice must contain inter alia (i) the various purposes for which personal data is to be processed; (ii) the nature and categories of personal data being collected; (iii) the identity and contact details of the data fiduciary (including its data trust score, if applicable) and Data Protection Officer (DPO); (iv) the rights of the data principal; (v) information pertaining to sharing, cross-border transfer and retention of personal data; (vi) the procedure for grievance redressal; and (vii) any other information as specified by the regulations.

Data fiduciaries will not be required to provide notice in specific instances where the provision of notice substantially prejudices the purpose of processing of personal data, such as processing personal data for performance of certain functions of the State, for compliance with any order of a court, or to respond to medical emergencies, disaster relief, or public order situations.

(c) Data Quality

The key requirements of data quality are that data should be accurate, complete and up-to-date. The data fiduciary is required to take necessary steps to ensure that the personal data being used is relevant to the purpose for which it is to be used and is not misleading. The data fiduciary is also responsible for ensuring accuracy and in case any data is inaccurate, it must correct, complete or update the data on request by the data principal.
(d) Data storage limitation

The data fiduciary is not permitted to store personal data beyond the period reasonably necessary to satisfy the purpose for which it was initially collected or is being processed. Data fiduciaries must delete the personal data once the purpose for which the personal data is collected and processed is achieved. However, personal data may be retained for a longer period provided the data principal has explicitly consented to such retention or if such prolonged retention is necessary to comply with any obligation under applicable law.

5. Grounds for Processing personal data

Under the Draft Bill, consent remains the primary ground under which personal data may be processed. However, similar to other privacy legislations there are some limited non-consensual grounds for processing as well.

(a) Consent

Consent needs to be obtained no later than at the commencement of the processing. It must be free, informed, specific, clear and capable of being withdrawn as easily as it is given. If consent is withdrawn without a valid reason, the data principal will have to bear any legal consequence for the effects of such withdrawal. For the processing of sensitive personal data, consent must additionally be informed, clear and specific.

The PDP Bill introduces the construct of consent managers, who are data fiduciaries registered with the DPA that provide interoperable platforms that aggregate consent from a data principal. Data principals may provide their consent to these consent managers for the purpose of sharing their information to various data fiduciaries and may even withdraw their consent through these consent managers. This is a unique construct and appears to have been introduced to support the Data Empowerment and Protection Architecture (DEPA) for financial and telecom data that currently powers the Account Aggregators licensed by the RBI.

(b) Non-consensual grounds

The PDP Bill allows both personal data and sensitive personal data to be processed in the absence of consent under certain grounds, such as for the performance of certain State functions, for compliance with law or any order of a court, and for prompt action such as responding to medical emergencies, providing assistance during a disaster or breakdown of public order.

In addition, personal data which is not sensitive personal data may be processed by an employer for purposes such as recruitment, termination or assessment of employees, where processing based on consent may not be appropriate.

Processing may also be carried out for other reasonable purposes which could be fraud, whistle blowing, mergers and acquisitions, network and information security, credit scoring recovery of debt, processing of publicly available personal data and the operation of search engines. Unlike the GDPR, these grounds for reasonable processing though illustrated in the PDP Bill are required to be specified by regulations. Until such regulations are framed it is unlikely that this ground can be availed of.

6. Personal data and Sensitive personal data of Children

Under the PDP Bill a ‘child’ is defined as a data principal under 18 years of age, which is a higher age limit than most other jurisdictions. All data fiduciaries are required to verify the age of a child in the manner specified by regulations and obtain parental consent to process the personal data of a child.

In line with other global privacy legislations, the PDP Bill places additional obligations on certain data fiduciaries who operate commercial websites or online services directed at children or process large volumes of children's personal data, which are classified under regulations as 'guardian data fiduciaries'. Guardian data fiduciaries are prohibited from profiling,
7. Rights of the Data Principal

Under the PDP Bill, a data principal has the following rights with respect to a data fiduciary:

(a) The Right to Confirmation and Access

A data principal has the right to request a data fiduciary to confirm if it is processing or has processed his personal data. The data principal can also request the data fiduciary for the personal data being processed or that has been processed, or a brief summary of such personal data, as well as a summary of processing activities undertaken with respect to the personal data.

The PDP Bill grants data principals the right to access in a consolidated place, the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary, along with the categories of personal data shared. The place and method of such access are to be determined by regulations.

(b) The Right to Correction and Erasure

The data principal also has the right to compel a data fiduciary processing his personal data to - (i) correct inaccurate or misleading personal data; (ii) complete any incomplete personal data; (iii) update personal data that is out of date; and (iv) to erase personal data that is no longer required for the purpose for which it was processed.

If the data fiduciary does not agree with such a request by the data principal, it is required to provide a justification for rejecting the request. When making a change, it must also take reasonable steps to notify the change to all relevant entities or individuals to whom the personal data has been disclosed, particularly where such change would have an impact on the rights and interests of the data principal or on decisions made regarding data principal.

(c) The Right to Data Portability

When the processing is carried out by automated means, the Draft Bill grants a data principal the right to receive his personal data in a structured, commonly used and machine-readable format. A data principal also has the right to have such data transferred to any other data fiduciary. This right is however not available where compliance with such request would reveal a trade secret of the transferor data fiduciary or would not be technically feasible, or where processing is required for functions of the State, or in compliance with a law or an order of a court.

(d) The Right to be Forgotten

A data principal has the right to restrict or prevent continued disclosure of personal data by a data fiduciary, where such disclosure (i) has served the purpose for which it was collected or is no longer necessary for the purpose, (ii) was made on the basis of consent and such consent has since been withdrawn, or (iii) was made contrary to the provisions of this Draft Bill or any other law made by Parliament or any State Legislature. To exercise this right, an application must be made by a data principal to an Adjudicating Officer.

(e) Exercise of rights

Other than the right to be forgotten, the above-mentioned rights may only be exercised upon a request made in writing to the data fiduciary, either directly or through a consent manager. If a data fiduciary refuses any such request, the data fiduciary must provide the data principal with the reasons for such refusal and inform the data principal that he has the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified. However, a data fiduciary need not comply with a request where compliance would harm the rights of another data
8. Transparency and Accountability Measures

(a) Privacy by Design Policy

The PDP Bill introduces a requirement for every data fiduciary to create a ‘privacy by design policy’ detailing the various elements in its policies that implement the principle. While the concept of privacy by design has been included in most global privacy legislations, the PDP Bill requires all data fiduciaries to frame it into a policy and offers an option to have the policy certified by the DPA. Once approved, the policy must be published on the data fiduciary’s website.

(b) Transparency Measures

The PDP Bill details the level of transparency that a data fiduciary will have to maintain regarding its practices for processing personal data. A data fiduciary must make available, in an easily accessible form, information such as, (i) the categories of personal data collected, (ii) the purpose and manner of such collection, (iii) the existence and procedure for exercise of the rights of a data principal and the contact details for the same, (iv) the existence of the right to file complaints to the DPA, and (v) information regarding cross-border transfers of personal data. There is a further obligation on a data fiduciary to notify a data principal of important operations in the processing of personal data periodically.

(c) Security Safeguards

Every data fiduciary as well as data processor is required to implement security safeguards, including: (i) the use of de-identification and encryption; (ii) steps necessary to protect the integrity of personal data; and (iii) measures to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data. These safeguards must be implemented taking into account the nature and scope of processing, the risks associated, and the likelihood of harm that may be caused to the data principal and must be reviewed periodically.

(d) Personal data Breach Reporting

A data fiduciary must notify the DPA (as soon as possible and no later than the period specified by the DPA under regulations) of any personal data breach that is likely to cause harm to any data principal. Such notification must include particulars of the nature of the personal data breached, the number of data principals affected, consequences of the breach and measures being taken to remedy it. This information may also be provided in phases as and when it becomes available.

The DPA will determine as to whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of harm to the data principal and whether some action is required from the data principal to mitigate such harm. The DPA may also direct the data fiduciary to take remedial action and to publish the details of the breach on its website, and additionally may also post such details on its own website. However, there is no restriction on the data fiduciaries choosing to inform affected data principals or publishing details of such a breach even in the absence of such direction from the DPA.

(e) Third party processing of personal data

A data fiduciary may engage a data processor to process personal data on its behalf only through a valid contract. Further, the processing may not be sub-contracted by a data processor without the authorization of the data fiduciary, contractually or otherwise. Further, such processing must be done only in accordance with the instructions of the data fiduciary unless otherwise prescribed by law.

(f) Significant data fiduciaries
The DPA is required to notify certain data fiduciaries (or classes of data fiduciaries) as 'significant data fiduciaries', based on factors such as the volume of personal data processed, sensitivity of such data, annual turnover of the data fiduciary, the risk of harm from any processing undertaken by the data fiduciary, use of new technologies, and any other factor that may be relevant in causing harm to any data principal as a result of such processing. These significant data fiduciaries are required to register themselves with the DPA.

Under the PDP Bill, significant data fiduciaries will be subject to increased compliance standards. These are:

(i) **Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is mandatory before a significant data fiduciary undertakes any data processing involving new technologies or large-scale profiling, or use of sensitive personal data, or any other processing that may pose a risk of significant harm to a data principal. Owing to the ambiguity of what amounts to a ‘new technology’, it is currently uncertain as to when the requirement to obtain a DPIA is triggered for a significant data fiduciary. For entities that operate in high technology fields, this will potentially apply to most forms of processing that they undertake.

The DPIA is required to contain: (i) a detailed description of the proposed processing including the purpose and nature of the data processed; (ii) assessment of potential harm to data principals; and (iii) measures for managing and mitigating such risk of harm. Upon completion of the DPIA, the DPO appointed by the significant data fiduciary is required to review the DPIA and submit the same to the DPA. The DPA may then (if it believes that the processing may cause harm to data principals) direct the data fiduciary to cease such processing or may prescribe conditions to such processing.

(ii) **Record Keeping and Audits**

A data fiduciary is required to maintain records (in the form and manner specified by regulations) of: (i) important operations in the data life cycle, (ii) periodic review of security safeguards; (iii) DPIAs; and (iv) any other aspect as specified by the DPA.

A significant data fiduciary is required to have its policies and processing audited by an independent data auditor. The auditor may assign a rating in the form of a data trust score, the criteria for which will be provided by the DPA. The DPA may also in its discretion order an audit to be conducted, when it is of a view that an act of processing may cause harm to a data principal by an auditor appointed by it in this regard.

(iii) **Data Protection Officer**

Every significant data fiduciary must appoint a DPO to carry out functions such as:

- monitoring processing activities to ensure such processing does not violate the act.
- providing advice on compliance with the Draft Bill, including DPIAs and Privacy by Design.
- acting as a point of contact between the DPA/data principal and the data fiduciary.
- maintaining an inventory of all records.

This DPO must be based in India and the intent seems to be to identify an individual that can assume the responsibility for the activities of the data fiduciary in India, much like the resident director requirement in India.

(iv) **Social Media Intermediaries**

The PDP Bill introduces the construct of social media intermediaries, which are entities that primarily or solely enable online interactions between users and allow them to exchange information between themselves. The Central Government can notify those social media intermediaries that have a specified number of users, and whose actions are likely to have a significant impact on electoral democracy, security of state, public order, or the sovereignty of India, as significant data fiduciaries. However, entities that primarily enable commercial or business-oriented transactions, provide access to the
internet or are in the nature of search engines, email services or online storage services are however not included within this definition.

All social media intermediaries that are significant data fiduciaries are required to provide their users the ability to voluntarily verify their accounts and all such verified accounts are required to be provided with a mark of verification which is publicly visible. There is, at this stage, no clarity on what documents will be accepted for the purpose of verification and what consequences (if any) will follow from this verification.

(g) Grievance Redressal

Every data fiduciary is required to put in place a mechanism that allows data principals to have their grievances addressed in quickly and efficiently. Data principals may file a complaint to the DPO (in case it is a significant data fiduciary, or the officer authorised by the data fiduciary (for other data fiduciaries) for any contravention of the PDP Bill that is likely to cause them harm. These complaints are to be resolved within 30 days. In case this timeline is not met, or if the data principal is not satisfied with the resolution of their complaint, they may file a complaint regarding the same with the DPA.

9. Cross Border Transfers of Data

The PDP Bill places no restrictions on the cross-border transfer and processing of personal data. This is a significant dilution of the data localisation required under the Committee draft of the PDP Bill, which required a copy of all personal data to be stored in India.

Instead, the PDP Bill requires the localisation of sensitive personal data and has imposed conditions on the cross-border transfer of sensitive personal data and critical personal data.

(a) Localisation Requirement for sensitive personal data

The PDP Bill requires all sensitive personal data to be stored in India, irrespective of whether it is transferred outside the country. The provision may therefore be interpreted as a requirement to store a copy of all sensitive personal data in India.

The PDP Bill also empowers the Central Government to notify certain categories of personal data as critical personal data that shall only be processed in India. At present, there is no indication as to what data may be notified as critical personal data.

(b) Cross Border Transfers of Data

Where sensitive personal data is required to be transferred outside the country, a data fiduciary may only transfer such data if it obtains the explicit consent of the data principal. In addition to obtaining explicit consent, the data fiduciary must additionally meet any of the following conditions:

(i) if the transfer is made subject to a contract or intra-group schemes that have been approved by the DPA. In order to obtain approval, contracts and inter-group schemes under this provision are required to ensure protection of the rights of the data principal as well as liability of the data fiduciary for harm caused due to any non-compliance. This is a deviation from the earlier version of the Draft Bill, which permitted transfers based on standard contractual clauses, in line with global frameworks such as the GDPR. The new construct of a contract is unclear as to whether the requirement of approval applies to each individual contract, and this may have wide implications for entities who rely on contractual obligations for cross-border transfers.

(ii) subject to an adequacy determination by the Central Government
The PDP Bill also permits critical personal data to be transferred outside the country for certain limited purposes such as:

(i) for prompt action including transfers to persons or entities engaged in health or emergency services

(ii) to a country, an entity or a class of entity in a country or, an international organisation under the adequacy determination discussed above. In addition, the Central Government must also be satisfied that such a transfer would not prejudicially affect the security and strategic interest of the nation.

10. Exemptions

The PDP Bill sets out various exemptions to the applicability of the Bill. These exemptions are elaborated below:

(a) Exemption to any agency of the Government

If the Central Government, by a written order, is satisfied that it is necessary in the interest of or for preventing incitement to the commission of a cognisable offence relating to the (i) sovereignty and integrity of India, (ii) security of the State, (iii) friendly relations with foreign states, (iv) public order, direct that the provisions of the Act will not apply to any agency of the government for processing personal data. The term cognisable offense is as defined in the Code of Criminal Procedure, 1973. Processing of personal data for the purpose of this provision includes sharing by or sharing with such agency of the government by any data fiduciary, data principal or data processor.

(b) Exemptions for certain types of processing of personal data

Certain specified provisions will not apply where personal data is (i) processed in the interest of prevention, detection, investigation and prosecution of any offence or any other contravention of law, (ii) disclosed for *inter alia* enforcing a legal right, (iii) processed by any court or tribunal, (iv) exempted by the Central Government where processing of personal data of data principals not within the territory of India, (v) processed by a natural person for any personal or domestic purpose, (vi) processed for a journalistic purpose, (vii) processed for research, archiving or statistical purposes, (viii) processed manually by a small entity. Exemptions (v) to (viii) are explained below:

(c) Personal or Domestic purposes

The PDP Bill provides that a natural person processing personal data for purely personal or domestic purposes, will not be subject to certain substantive data protection requirements under the PDP Bill. However, if the processing involves disclosure to the public or is undertaken in connection with any professional or commercial activity, then the provisions of the PDP Bill will apply.

(d) Journalistic purpose

Where the processing of personal data is necessary for or relevant to a journalistic purpose, certain substantive data protection requirements under the PDP Bill will not be applicable to such processing.

Journalistic purpose has been defined to mean any activity intended towards the dissemination of factual reports, analysis, opinions, views or documentaries regarding news, recent or current events, or any other information which the data fiduciary believes to have public interest. Further, the exemption will be available only if it can be demonstrated that the processing complies with the code of ethics issued by the Press Council of India or any self-regulatory media organisation.

(e) Research, Archiving, Statistical Purpose
The PDP Bill allows the DPA to specify different categories of research, archiving or statistical purposes and exclude the applicability of certain provisions of the Bill to such categories. The exemption is available only under circumstances, such as when compliance with the PDP Bill will disproportionately divert resources from the purpose of processing, where the purpose cannot be achieved if the personal data is anonymised, or where such processing would not give rise to a risk of significant harm to the data principal, amongst others.

(f) Manual Processing

The PDP Bill exempts small entities who are carrying out manual processing from the following requirements: (i) the requirement to provide notice for collection of personal data, (ii) the obligation to ensure quality of data, (iii) the limitations on storage of personal data, (iv) the obligation to provide a summary of processing activities to data principals, (v) the requirement to facilitate a data principal's right to data portability and the right to be forgotten, (vi) the obligations regarding privacy by design, transparency, security safeguards, personal data breach notification, data protection impact assessment, maintenance of records, data audits, data protection officer and grievance redressal.

(g) Sandbox provision

The PDP Bill empowers the DPA to create a sandbox to encourage innovation in artificial intelligence, machine learning or any other emerging technology in public interest. This provision has been introduced in order to ensure that the new privacy regime offers opportunities for data fiduciaries to innovate and utilise emerging technologies.

Entities included in the sandbox will be exempt from to compliance with requirements such as specifying the purpose of data processing, limitations on collection of personal data, obligations directly depended on the obligations to specify purpose and limitation on collection of personal data and restrictions on retention of personal data. Any data fiduciary whose privacy by design policy is certified by the Authority will be eligible to apply for inclusion in the sandbox. While applying for inclusion in the sandbox, the data fiduciary must provide details including (i) the term (not exceeding 12 months) for inclusion in the sandbox, (ii) the innovative use of technology and its beneficial uses, (iii) the data principals participating under the proposed processing. The Authority is required to ensure safeguards during the term of inclusion in the sandbox which is subject to a total of thirty-six months.

11. Data Protection Authority

The PDP Bill establishes a DPA to serve as the regulatory and enforcement body. The DPA has been vested with wide ranging powers to, (i) provide guidelines and directions on the applicability of several provisions of the Act, (ii) ensure consistency of data protection regulations across ministries, regulators and legislations and monitor, and (iii) enforce compliance with provisions of the Act by various stakeholders. In performing these functions, the DPA or such Inquiry Officer, as appointed by the DPA, would have the powers of a civil court with respect to discovery, summons and inspection. A few notable functions of the DPA are:

(a) Codes of Practice

While the PDP Bill itself specifies the substantive obligations that would apply to the handling of data, the specifics of these obligations are to be detailed under what is termed in the bill as 'Codes of Practice', which will be issued by the DPA. These Codes of Practice would relate to compliances such as form of notices, retention periods, grounds for processing, method for exercise of rights by data principals, specific measures or standards for security and safeguards for personal data, cross border data transfers, personal data breaches, data protection impact assessments, processing of de-identified data for research, archiving or statistical purposes etc. Codes of Practice would be applicable either generally or to a particular industry or sector. The DPA is required to issue Codes of Practice in consultation with the relevant stakeholders including the regulators, the industry and the public, and would also be authorised to approve Codes of Practice submitted by an industry or trade association.

(b) Inquiry and Investigation
The DPA can conduct an inquiry on a complaint or on its own, when it has reasonable grounds to believe that a data fiduciary or processor is either contravening its obligations under the PDP Bill or carrying out activities detrimental to the interest of data principals. For this purpose, the DPA may appoint one of its officers as an Inquiry Officer. Inquiry Officers have broad powers to investigate and examine the records and personnel of any data fiduciary or processor under the PDP Bill and is required to submit a report to the DPA on all inquiries made.

Further, if the Inquiry Officer has reasonable grounds to believe that a data fiduciary or processor may tamper or not produce records that it has been directed to produce or may contravene any provisions of the PDP Bill, it may make an application to a designated court for an order to exercise search and seizure powers. The search and seizure powers of an Inquiry Officer, after getting authorised by the respective court are very broad and allow the officer to access and seize all property of the person being inspected and examine any person who is in possession or control of any material. An Inquiry Officer may also enlist the assistance of police officers or officers of the central government for this purpose.

Upon the conclusion of an inquiry, the DPA may issue directions requiring the data fiduciary or processor to modify its business, cease and desist some activities, or close down an aspect of their business. If a data fiduciary or processor is aggrieved by an order of the DPA, they may appeal before the Appellate Tribunal set up under the PDP Bill.

12. Offences and Penalties

The PDP Bill specifies strict penalties for the contravention of its provisions. These penalties are prescribed in two brackets, the higher of which extends up to INR 150 million or 4% of the total worldwide turnover of the data fiduciary for the previous financial year, depending on the nature of the offence. Notably, significant data fiduciaries may be subject to a penalty up to INR 50 million or 2% of their total worldwide turnover, whichever is higher, for not complying with the obligations that are specifically applicable to them. The penalties may only be imposed after an inquiry has been conducted by an Adjudicating Officer of the DPA and the data fiduciary has been provided with a reasonable opportunity of being heard. An inquiry can only be initiated upon a complaint made by the DPA.

As a positive step compared to the previous version of this Bill, the PDP Bill only criminalises the re-identification, and reidentification and processing of data. The consequences for this offence may be imprisonment up to a term of three years or a fine which may extend to INR 200,000. These offences are cognisable and non-bailable - a clear indication that they are treated with a high degree of severity. Courts may take cognizance of this offence only on a complaint made by the DPA.

13. Compensation

Additionally, compensation may be awarded to data principals who have suffered harm due to violations by a data fiduciary or data processor. Compensation is also decided by an Adjudicating Officer and may be sought by the data principal by making an application to the Adjudicating Officer. The orders of the Adjudicating Officer are appealable before the Appellate Tribunal.

A data processor will only be held liable to pay compensation if it is found to have acted in a negligent manner or if it has violated any provisions of the PDP Bill.

Other Relevant Provisions

(a) Bar on processing certain forms of biometric data

The PDP Bill prohibits fiduciaries from processing any biometric data which has been notified by the Central Government as being subject to such restriction. However, such processing may be carried out if the data fiduciary is specifically permitted by law.

While it is presently unclear as to what kind of biometric data will be notified under this section, it seems likely that entities
may face some restrictions on use of specific forms of biometric data, such as fingerprints, iris scans, facial recognition, etc. This has the potential to affect a wide variety of activities from biometric verification systems for employees to device access.

(b) Governmental Access to Non-Personal and Anonymised Data

The PDP Bill allows the Central Government to require any data fiduciary or data processor to provide any anonymised personal data that it holds and provide this to the Government. In addition, it also allows for the Central Government to call for non-personal data from fiduciaries and processors. This data is to be used by the Central Government to enable better targeting of delivery of services or formulation of evidence-based policies.

Moving Ahead

The PDP Bill was introduced in Parliament and has been referred to the Joint Select Committee, which is required to submit its report to Parliament by the next session scheduled for February 2020.

While the PDP Bill provides some more clarity on the compliances and obligations applicable to data fiduciaries and processors, a large number of compliances remain subject to the determination of the DPA, and the full impact of this legislation therefore may only be measured once these regulations are released.

[1] The Draft Bill defines profiling to mean any form of processing that analyses or predicts the behaviour, attributes or interests of a data principal located in India
[2] Small entities are defined as data fiduciaries as may be classified, by regulations, having regard to: (i) the turnover of the data fiduciary in the preceding financial year, (ii) purpose of collection of personal data for disclosure to other persons, and (iii) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve months.

If you require any further information about the material contained in this newsletter, please get in touch with your Trilegal relationship partner or send an email to alerts@trilegal.com. The contents of this newsletter are intended for informational purposes only and are not in the nature of a legal opinion. Readers are encouraged to seek legal counsel prior to acting upon any of the information provided herein.