TRILEGAL

The Data Protection Bill, 2021

24 December 2021

This update covers:

India does not presently have an omnibus data protection legislation. Given the rising importance of technology-based businesses, the Parliament had undertaken an exercise to formulate India's data protection regime. On 11 December 2019, the Ministry of Electronics and Information Technology (**MeitY**) introduced the draft Personal Data Protection Bill, 2019 (**PDP Bill**) before the Parliament, which was referred to a Joint Parliamentary Committee (**JPC**) for further consideration. After carrying out a series of consultations with stakeholders, on 16 December 2021, the JPC published its report along with the finalised Data Protection Bill 2021 (**DP Bill**).

On 16 December 2021, the Joint Parliamentary Committee has published its report along with the finalised Data Protection Bill, 2021. When passed into law, this has the potential to change the way in which data is used by businesses.

This update provides a brief overview of the key provisions of the DP Bill relating to the rights of data principals, obligations of data fiduciaries, grounds for which personal data can be processed, data breach reporting requirements, classification of significant data fiduciaries, and an enhanced penalty regime.

1 Applicability

The DP Bill applies to the processing of personal data that has been collected, disclosed, shared or otherwise processed in India, or to the processing of personal data by the State or State bodies, Indian corporate entities and Indian citizens. *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 for the purpose of profiling.

A separate class of data - *sensitive personal data* is also recognised in the DP Bill and is subject to enhanced thresholds. 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. The term '*financial data*' is defined narrowly in the DP Bill. Section 3(21) 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 also includes 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.

The DP 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 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. Additionally, the DP 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.

In a departure from previous drafts of this law, *non-personal data* has also been included within the scope of the DP Bill. Non-personal data has been defined to include all data ***other than*** personal data. This will potentially include anonymised data (personal data which has undergone 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**). Accordingly, until the DPA specifies the technical threshold for anonymisation, it will not be possible to categorically stipulate what constitutes anonymised data. Unlike in relation to personal data, the DP Bill does not clarify whether there are any territorial limits to the applicability of its provisions in respect of non-personal data. However, the provisions of the current draft regulate such data only to the extent of data breaches, and the Central Government's ability to issue directions to data fiduciaries and processors to provide such data for targeted delivery of services or evidence-based policy formulation.

2 Key Obligations of Data Fiduciaries

The DP Bill creates a concept of a *data fiduciary* - similar to the GDPR notion of a data controller. The entity that determines the purpose or means of processing the personal data of the data principal is referred to as the '*data fiduciary*'. Data fiduciaries can include the State, corporate entities and individuals. On the other hand, the natural person whose personal data is collected is referred to as the '*data principal*'. The DP Bill conceptualises the processing of data broadly to include most operations that are carried out on data including storage, adaptation, retrieval, dissemination, and erasure or destruction.

Similar to other privacy legislations, the DP Bill imposes several obligations on data fiduciaries with respect to the collection and processing of personal data as follows:

(a) ***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 thefollowing:

(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.

Such a notice must be clear, concise, easily comprehensible and in multiple languages to the extent necessary and practicable.

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.

(b) ***Purpose Limitation and Collection Limitation***

Every person processing personal data must do so in a fair and reasonable manner that would not exceed the reasonable expectations of the data principal. All processing is required to be carried out for one or more lawful basis for processing as contained in the DP Bill. Under the DP Bill, consent remains the primary ground under which personal data may be processed. However, similar to other privacy legislation, there are some limited non-consensual grounds for processing as well.

(i) *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 obtained after informing the data principal about the purpose of processing, which is likely to cause them any significant harm, be in clear terms such that it may be understood without referring to conduct or context and after giving them the choice to separately consent to different purposes of use for different categories of sensitive personal data. The provision of goods or services, or their quality, or the performance of a contract cannot be made conditional on consent that is not otherwise necessary or denied based on exercise of the data principal's choice.

The DP Bill introduces the concept of consent managers, who will be 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 construct 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.

(ii) *Non-consensual grounds*

The DP 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. While two indicative functions, namely the provision of a service or benefit from the State and the issuance of a certification, license or permit from the State have been specified, these are only indicative and not exhaustive. Other grounds include 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 if such processing is necessary or is reasonably expected by the data principal 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 or other corporate restructuring transactions, 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 DP Bill are required to be specified by regulations. Such regulations will take into consideration several factors including legitimate interest of data fiduciary to process for that purpose, whether it is reasonable to expect/practicable for a data fiduciary to obtain consent, public interest, degree of any adverse effect of processing on data principal rights etc.

(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.

(e) *Privacy by Design Policy*

The DP Bill requires 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 DP 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.

(f) *Transparency Measures*

The DP 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 relevant contact details for exercising them,

(iv) the existence of the right to file complaints to the DPA, and

(v) information regarding any cross-border transfers of personal data carried out by it.

The data fiduciary is also required to provide transparency about the fairness of the algorithm or method used to process personal data. There is a further obligation on a data fiduciary to periodically notify data principal of important operations with regard to the processing of their personal data.

(g) *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 considering 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.

(h) *Data Breach Reporting*

A data fiduciary must notify the DPA within 72 hours of becoming aware of any personal data breach. The term '*personal data breach*' has been defined in a broad and inclusive fashion to include any unauthorised disclosure, acquisition, sharing, use, alteration, destruction of or loss of access of personal data which compromises the confidentiality, integrity or availability of personal data to a data principal, whether intentional or accidental. This may lead to the inclusion of other potentially minor incidents being covered within the obligation to report data breaches.

The notification to DPA must include, when available, particulars of the nature of the personal data breached, the number of data principals affected, consequences of the breach, and actions being taken to remedy it. This information may also be provided in phases as and when it becomes available. The DPA may direct the data fiduciary to report such breach to the data principal after considering the severity of *harm* (explained below) to the data principal and direct them to take appropriate remedial action to mitigate such harm and to publish the details of the breach on its website. The DPA has been empowered to take steps, as may be prescribed by rules made under the DP Bill, in cases of breach of non-personal data as well.

(i) *Grievance Redressal*

Every data fiduciary is required to put in place a mechanism that allows data principals to have their grievances addressed 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 DP 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.

(j) *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. Such processing by a data processor must be done only in accordance with the instructions of the data fiduciary unless otherwise prescribed by law.

3 Rights of the Data Principal

Under the DP 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 data fiduciary should respond to confirmation and access requests in a clear and concise manner that is easily comprehensible to a reasonable individual in a similar context.

The DP 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.

The DP Bill further allows the data principal to nominate a legal heir or a representative as his nominee who can exercise the right to be forgotten on behalf of the data principal after his or her death.

(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, a data fiduciary must also take necessary and practicable 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 DP Bill grants a data principal the right to receive his or her personal data in a structured, commonly used and machine-readable format. The DP Bill has expanded the definition of '*automated means*' to equipment which is capable of operating automatically in response to instructions given or *otherwise* for processing personal data. The widening of the definition of automated is likely to extend to all situations where personal data of a data principal is processed electronically.

A data principal also has the right to have such data transferred to any other data fiduciary. Under previous versions of the law, this right was not available if the portability request would result in the disclosure of a trade secret. This exemption has been done away with and the only grounds under which a portability request can be denied is if granting the request is not technically feasible, or where the data is required to be retained for functions of the State, or in compliance with a law or an order of a court, tribunal or quasi-judicial authority.

(d) *The Right to be Forgotten*

A data principal has the right to restrict or prevent continued disclosure or processing of personal data by a data fiduciary, where such disclosure or processing

(i) has served the purpose for which it was collected or is no longer necessary for the purpose,

(ii) the consent on the basis of which such disclosure was made or such processing was being carried out has since been withdrawn, or

(iii) was made contrary to the provisions of the DP Bill or any other law.

Given that processing has been defined under the DP Bill to include even storage of such data, the DP Bill has further expanded the scope of the right to be forgotten to a right to deletion of such data from the servers of the data fiduciary.

To exercise this right, an application must be made by a data principal to an Adjudicating Officer. However, this right can only be exercised in situations where the data principal is able to show that (i) it is overridden by the right to freedom of speech and expression as well as the right to information of any other citizen, and (ii) the exercise of the right to be forgotten overrides the data fiduciary's right to retain, use or process such data, in accordance with the regulations specified by the DPA.

(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 DPA against the refusal, within such period and in such manner as may be specified. A data fiduciary need not comply with a request where compliance would harm the rights of another data principal.

4 Cross Border Transfer of Data

The DP Bill places no restrictions on the cross-border transfer and processing of personal data *per se.* This data may be transferred across borders if one of the purposes of processing are met. However, certain subcategories of personal data are subject to specific transfer restrictions:

(a) *Requirement to store a local copy of Sensitive Personal Data*

The DP Bill requires all sensitive personal data to be stored in India, even if it is transferred outside the country.

The DP 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, the term critical personal data remains undefined.

(b) *Cross Border Transfer of Sensitive Personal 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 and additionally meets any of the following conditions:

(i) if the transfer is being made subject to a contract or intra-group schemes, such schemes should have been approved by the DPA in consultation with the Central Government;

(ii) there has been an adequacy determination made by the Central Government in respect of transfers to a country or to an entity or class of entities in a country. Such an adequacy determination will have to include the finding that the data being transferred will not be shared with any foreign government or agency unless such sharing is approved by the Central Government;

(iii) if the transfer of sensitive personal data or a class of sensitive personal data is approved by the DPA in consultation with the Central Government for a specific purpose.

(c) *Prohibition on Cross Border Transfer of Critical Personal Data*

There is a general prohibition on the transfer of critical personal data outside the territory of India. The DP Bill allows exceptions to this general prohibition by permitting 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.

5 Offences and Penalties

The DP Bill envisages strict penalties for the contravention of its provisions. The exact quantum of these penalties are yet to be prescribed, however, this prescription may not exceed two pre-defined buckets (based on the nature of the contravention) under the DP Bill. The higher of these buckets extends up to INR 150 million or 4% of the total worldwide turnover of the data fiduciary for the previous financial year, and the lower of these extends up to INR 50 million or 2% of their total worldwide turnover.

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. The Bill has provisions for compensation to the data principals for harm caused to them by a data fiduciary as a result of violation of the DP Bill or rules and regulations made under it. The data principal can apply to the DPA in such cases, and such an application will be decided by the adjudicating officer appointed under the DP Bill. The Bill also provides for representative applications to be

filed if the harm has been suffered by a class of data principals. In this regard, it is relevant to note that the DP Bill has a wide definition of *'harm*' and includes bodily or mental injury, identity theft, financial loss, loss of reputation, direct or indirect restrictions on speech or movement owing to a fear of surveillance. Also included in this definition is any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal, as well as psychological manipulation which impairs an individual's autonomy. What constitutes an 'evaluative decision' or 'psychological manipulation' has not been clarified under the DP Bill. The former is likely to 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 possible that the mere act of denying a data principal certain goods, services, or benefits based on an evaluative decision could be argued to constitute a harm against the data principal.

Further, unlike the GDPR, the definition of '*harm*' under the DP Bill extends to all types of evaluative decisions regardless of whether humans are involved or not. Such a broad definition could have a chilling effect on data-based predictive decision-making. Additionally, the definition of harm can be further expanded through regulation.

The DP Bill imposes criminal liability for 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.

For offences committed by companies, the DP Bill provides that only the persons of the company that were in-charge of or responsible for that part of the company to which the offence relates can be held liable. For independent directors and executive directors, they can be held liable if it is proven that the offence took place with their knowledge or with their consent or where they had not acted diligently.

6 Significant Data Fiduciaries

The DPA may 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, the processing of data of children or provision of services to them, and any other factor that may be relevant in causing harm to any data principal as a result of such processing.

Additionally, social media platforms 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 may also be notified as significant data fiduciaries. A social media platform has been defined to be an entity that primarily or solely enable online interactions between users and allow them to exchange information between themselves. Notably, the draft envisages different user thresholds being applicable to different classes of social media platforms.

Significant data fiduciaries are required to register themselves with the DPA and are subject to greater compliance obligations. These include:

(a) *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 sensitive personal data, or undertakes any other type of processing that may pose a risk of significant harm to a data principal. It is not clear what amounts to a '*new technology*', and therefore it is unclear when the requirement to obtain a DPIA is triggered. 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.

(b) *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.

(c) *Data Protection Officer*

Every significant data fiduciary must appoint a Data Protection Officer (**DPO**) to carry out functions such as:

(i) monitoring processing activities to ensure such processing does not violate the DP Bill.

(ii) providing assistance and co-operation to the DPA in relation to the significant data fiduciary's compliance with the DP Bill.

(iii) acting as a point of contact between the DPA/data principal and the data fiduciary.

(iv) maintaining an inventory of all records.

This DPO must be based in India, and for non-state data fiduciaries must be a key managerial personnel or equivalent employee of the entity. While the intent seems to be to identify an individual who can assume the responsibility for the activities of the data fiduciary in India, the manner in which the DP Bill is phrased appears to indicate that a member of the global leadership of a significant data fiduciary would need to be

appointed as the DPO and located in India to comply with the requirement. The definition of 'key managerial personnel' can be expanded through rules issued for this purpose and clarity is awaited on whether there will be a different class of employees who may be appointed as DPOs for significant data fiduciaries that are not incorporated in India.

The DP Bill recognises that significant data fiduciaries will be regulated by other sectoral regulators, in addition to the DPA.

7 Exemptions

The DP Bill sets out various exemptions to the applicability of the Bill, discussed 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, it may direct that the provisions of the DP Bill will not apply to any agency of the government for processing personal data.

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

Specified provisions relating to obligations of data fiduciaries, grounds for processing of personal data without consent, personal data of children, rights of data principals, transparency and accountability measures (except security safeguards), and restriction on transfer of personal data outside India 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 through non-automated means by a small entity.

Of these, exemptions (v) to (viii) are particularly defined in the DP Bill to mean:

- Personal or Domestic Purposes

  The DP 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 DP 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 DP Bill will apply.

- Journalistic Purpose

  Where the processing of personal data is necessary for or relevant to a journalistic purpose and in compliance with the rules and regulations under the DP Bill as well as code of ethics issued by the Press Council of India, certain substantive data protection requirements under the DP Bill will not be applicable to such processing. Journalistic purpose has been defined under the Bill 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 statutory regulatory media organisation.

- Research, Archiving, and Statistical Purpose

  The DP 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 certain circumstances, such as when compliance with the DP 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.

- Non-Automated Processing by Small Entities

  The DP Bill exempts small entities[1] who are carrying out non-automated processing from the following requirements:

  (A) the requirement to provide notice for collection of personal data,

  (B) the obligation to ensure quality of data,

  (C) the limitations on retention of personal data,

  (D) the obligation to provide a summary of processing activities to data principals,

  (E) the requirement to facilitate a data principal's right to data portability and the right to be forgotten,

  (F) 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.

As discussed above, '*automated means*' has been defined broadly to mean any equipment capable of operating automatically or even *otherwise* for processing personal data. This should include only those kinds of processing which can take place without any equipment such as a computer. This would mean only small entities that do not rely on any such equipment for processing of data can avail the aforesaid exemption.

---

1 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.

(c) *Sandbox Provision*

The DP Bill empowers the DPA to create a sandbox to encourage innovation in artificial intelligence, machine learning or any other emerging technology in public interest. Entities included in the sandbox will be exempt from compliance with certain provisions of the DP Bill, such as the restriction on retention of personal data. Any data fiduciary whose privacy by design policy is certified by the DPA 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 DPA is required to ensure safeguards during the term of inclusion in the sandbox which is subject to a total of thirty-six months.

8 Data Protection Authority

The DP Bill establishes a DPA to serve as the regulatory and enforcement body. The DPA would comprise a chairperson and six full time members, at least one of whom would be an expert in law. The selection of the chairperson and members of the DPA would be based on the recommendations of a designated selection committee under the DP Bill. The DPA has been vested with wide ranging powers to (i) provide guidelines and directions on the applicability of several provisions of the DP Bill, (ii) ensure consistency of data protection regulations across ministries, regulators and legislations and (iii) monitor, test and certify hardware and software on computing devices to prevent malicious insertions that may cause a data breach and (iv) enforce compliance with provisions of the DP Bill 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 DP Bill itself specifies the substantive obligations that would apply to the handling of data, the specifics of some 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 transfer, 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, either on the basis of a complaint or on its own accord when it has reasonable grounds to believe that a data fiduciary or processor is either contravening its obligations under the DP 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. 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 DP 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.

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 DP Bill.

9 Personal Data of Children

Under the DP 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 and obtain parental consent in the manner specified by regulations to process the personal data of a child.

The Bill also prohibits all data fiduciaries from profiling, tracking, monitoring behaviour of, or targeting advertisements directed at children, or undertaking any other processing of personal data that can cause significant harm to children, and data fiduciaries are only permitted to process personal data of children in a manner that protects their rights.

10 Other Relevant Provisions

(a) *Bar on processing certain forms of biometric data*

The DP Bill prohibits fiduciaries from processing any biometric data which may be prescribed by the Central Government through rules as being subject to such restriction. 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 DP Bill allows the Central Government to require any data fiduciary or data processor to provide any anonymised personal data that it holds. In addition, it also allows 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

While the JPC's report on the DP Bill has already been tabled before both houses of Parliament, reports currently suggest that the DP Bill itself may not be introduced until the next session of Parliament, which typically takes place in February-March. There is a likelihood that the DP Bill may also undergo further changes based on deliberations in Parliament.

The DP Bill lists various compliances and obligations applicable to data fiduciaries and processers. However, a number of additional compliance obligations have been left to be specified by the DPA. As a result, the full impact of this legislation therefore may only be clear once the DPA has been established and issues these regulations.

UPDATES

The JPC's report has advised the government to set a timeline for compliance with the DP Bill once it has been notified, so data fiduciaries will likely await clarity in this regard once the DP Bill is enacted into law.