TRILEGAL

Draft Digital Personal Data Protection Bill, 2022

24 November 2022

Partners: *Rahul Matthan, Nikhil Narendran and Jyotsna Jayaram,* ***Senior Associates****: Thomas J. Vallianeth and Karishma Sundara,* ***Associates****: Krati Hashwani, Akanksha Singh, Vishal V, Sanjeev Jothi, Madhav Tampi, Sindhu A, Prabal De, Padmavathi Prasad and Sidharth Ray*

This update covers:

1 Introduction

The much-awaited draft of the Digital Personal Data Protection Bill, 2022 was released for public consultation on 18 November 2022. The draft (which is substantially pared down, when compared with prior iterations) primarily seeks to establish a framework to govern the processing of digital personal data by data fiduciaries, while creating duties and rights for data principals and streamlining the obligations of data fiduciaries.

On 18 November 2022, the Ministry of Electronics and Information Technology released a draft of the Digital Personal Data Protection Bill, 2022 (**DPDP Bill**) for public consultation.[1] This comes just a few months after the Government withdrew the previous bill, *i.e.*, the Personal Data Protection Bill, 2019 (**PDP 2019**) and by extension, the draft Data Protection Bill, 2021 (**2021 Bill**) from Parliament, citing the need for a fresh and comprehensive draft. The Government has indicated that the DPDP Bill is considerably different from its predecessors in the manner and form of the obligations it imposes and in its treatment of non-compliance and enforcement.

Broadly, the DPDP Bill: (i) alters/omits definitions that were key in prior iterations; (ii) refrains from prescribing prescriptive notice requirements; (iii) does not categorise personal data based on sensitivity into sensitive personal data or critical personal data; (iv) alters the legal bases for non-consensual processing of personal data; (v) prescribes certain general obligations for data fiduciaries and limited additional obligations for significant data fiduciaries; (vi) provides for certain data principals' rights and imposes (for the first time) duties on them; (vii) permits the cross-border transfer of personal data to notified countries subject to certain conditions; (viii) positions the Data Protection Board more as an enforcement authority, as opposed to a regulator; and (ix) focuses on tempered penalties in place of the earlier trifecta of compensation, penalties and criminal liability.

The DPDP Bill is open for public consultation until 17 December 2022. As far as implementation is concerned, the DPDP Bill contemplates a phased roll-out once it is notified. Some of the key provisions of the DPDP Bill and their implications are discussed below, and parallels to the 2021 Bill have been drawn where required to demonstrate the evolution of these concepts.

2 Scope of Applicability and Key Definitions

2.1 Context

As per the explanatory statement accompanying the draft, the DPDP Bill is based on seven broad principles: (i) lawful, fair and transparent use of personal data; (ii) purpose limitation; (iii) data minimisation; (iv) reasonable efforts towards accuracy of personal data; (v) storage limitation; (vi) reasonable safeguards to avoid unauthorised collection or processing and prevent data breaches; and (vii) accountability for the person deciding the purposes and means of processing. These defining principles are, however, present to different extents in the actual text of the DPDP Bill, as discussed below.

[1] See here: https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

2.2 Applicability

The DPDP Bill applies to (i) the processing of personal data *within* the territory of India where it is collected from data principals online, or collected offline and then digitised; and (ii) the processing of digital personal data *outside* India in connection with any profiling of or activity of offering goods or services to data principals within the territory of India. Notably, therefore, the DPDP Bill does not apply to the processing of personal data of persons residing outside India by data fiduciaries in India. Where an Indian data fiduciary does so, its only obligation is to take reasonable security measures. This is a departure from the 2021 Bill, which did not make this distinction, indicating that an Indian data fiduciary would have to comply with the full gamut of obligations when processing personal data of non-residents.

The DPDP Bill does not apply to personal data that is (i) processed through non-automated means; (ii) offline in nature; (iii) processed by an individual for any personal or domestic purpose; or (iv) is about an individual and contained in a record that is at least 100 years old. It is likely that non-personal data will be governed under a separate framework.

The DPDP Bill broadly also exempts the applicability of its provisions to processing conducted by the State and its instrumentalities; for research, archival, or statistical purposes; and for the outsourcing industry.

3 Definitions – Key Exclusions, Inclusions, and Additions

3.1 Data Principal

The DPDP Bill adopts an expansive definition of a 'data principal' (*i.e.*, the individual to whom the personal data relates), including a child (*i.e.*, a person under 18 years) as well as the parent or lawful guardian of the child concerned. As a result, there may be two data principals wherever a child's personal data is processed. Consequently, the data fiduciary's obligations to the data principal (*e.g.*, providing notice of processing, or personal data breaches) and the rights accruing to this child as a data principal, could equally apply to the parent or guardian of the child. Practically, this would mean that the data fiduciary would (i) have to issue dual privacy notices to *both* the child and the parent; (ii) require the parent's consent for the child to meaningfully exercise her rights of correction and erasure. For instance, where a child signs up for an online streaming service and provides her name and phone number (i) this personal data cannot be processed without a notice of such processing being provided to the child *and* the parent/lawful guardian; and (ii) if the child wishes to have her personal data subsequently erased, such a request can only be made *via* and with the parent/lawful guardian's consent as a minor's personal data cannot be processed without verifiable parental consent (*related practical hurdles are discussed below in Section 10*).

3.2 Personal data

'Personal data' is defined in the DPDP Bill as '*any data about an individual who is identifiable by or in relation to such data*'. While this is a simpler definition than what was provided in the 2021 Bill, a plain reading and the use of '*such data*' suggests that non-identifiable data may not be considered personal data, even if the same is capable of being combined with other data to create personally identifiable data. Such a reading would be a departure from the 2021 Bill that specifically included within the scope of personal data *any* data that could, in combination with other features, result in personally identifiable data.

Further, while the definition does not include other elements contained in the 2021 Bill, such as data relating to any *characteristic, traits, attributes or any other features*, whether *online or offline*, or any '*inference drawn*

from such data for the purpose of profiling', the broad language used would likely ensure that such categories are nonetheless covered. The DPDP Bill does not classify personal data based on sensitivity, thereby omitting the concepts of 'sensitive' or 'critical' personal data, and the more onerous obligations that accrued to these categories.

The net effect is the creation of a streamlined data classification obligation, where data is simply classified as either personal data or non-personal data, with the provisions of the DPDP Bill applying to all personal data.

3.3 Harm

The DPDP Bill defines 'harm' exhaustively, limiting it to actual bodily harm, distortion or theft of identity, harassment, or the prevention of lawful gain or causation of significant loss. 'Loss' and 'gain', defined for the first time in the DPDP Bill, cover only a small set of largely financial losses and gains, thereby accounting only for a segment of the wider definition of 'harm' contemplated under the 2021 Bill.

This scaled-down list of what constitutes 'harm' necessarily has implications wherever the term 'harm' plays a deciding role (*e.g.*, in determining the risk of harm posed by a data fiduciary's activities, which in turn could determine its classification as a significant data fiduciary). Factors that were relevant under the 2021 Bill (*i.e., 'discriminatory treatment', 'denial or withdrawal service'*, and '*psychological manipulation which impairs the autonomy of an individual*') do not qualify under the DPDP Bill's heading of 'harm', and do not, accordingly, impact such determinations. For instance, earlier, an online platform connecting homeowners with prospective tenants could have been considered a significant data fiduciary because the platform may process personal data likely to result in discriminatory treatment. However, under the DPDP Bill, the platform's processing activities would now need to carry a risk of one of the more limited categories of harm, or qualify on some other basis (*e.g.*, volume of personal data processed) for the provider to be considered a significant data fiduciary.

Further, while 'harm' was earlier the trigger for a claim for compensation under the 2021 Bill, the DPDP Bill no longer provides for a compensation model, reducing the significance of the term. 'Harm' was previously also a determining factor in imposing/quantifying penalties for non-compliance but is no longer a consideration under the DPDP Bill.

3.4 Personal data breach

The DPDP Bill defines 'personal data breach' widely as *any* unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. The DPDP Bill prescribes penalties for personal data breaches, with penalties of INR 250 crore (USD 30 million) for a failure to take reasonable security safeguards. It also requires personal data breaches to be reported to every affected data principal, with non-compliance triggering a penalty of INR 200 crore (USD 25 million).

The wide definition has implications not only for the kind of instances that are reported as personal data breaches, but also for parallel penalties that may apply to the same processing activities. For instance, given that personal data breach includes *unauthorised processing of personal data*, even unintended excessive processing (*e.g.*, if it compromises the confidentiality of the personal data) would fall within its scope. Consequently, a data fiduciary may be simultaneously liable for penalties for (i) failing to undertake reasonable security practices; (ii) failing to report a breach (if applicable); as well as (iii) violating other obligations under the DPDP Bill.

3.5 Public Interest

The DPDP Bill has also introduced a definition of 'public interest', as being '*in the interest of any of the following: (a) sovereignty and integrity of India; (b) security of the State; (c) friendly relations with foreign States; (d) maintenance of public order; (e) preventing incitement to the commission of any cognisable offence relating to the preceding sub-clauses*'. In addition to this, the DPDP Bill includes '*(f) preventing dissemination of false statements of fact*' within the meaning of public interest. This definition is particularly significant in the context of processing personal data based on *deemed consent* (discussed below in Section 5.2). Processing data in 'public interest' is now permissible where the consent of the data principal is *deemed* to have been given *provided* it meets certain additional conditions specified under the deemed consent provision, *e.g.*, credit scoring; recovery of debt; prevention and detection of fraud. This, consequently, allows data fiduciaries to potentially undertake an entirely new genre of processing '*in public interest*', *e.g.*, to curb misinformation/disinformation. The extent to which processing is permissible under this ground is, however, still unclear.

3.6 Exclusions

The DPDP Bill excludes several definitions, such as (i) 'sensitive personal data' and its various sub-categories like 'genetic data', 'health data', 'biometric data', 'official identifier'; (ii) 'systematic activity'; (iii) 'social media platform'; (iv) 'State'; (v) 'regulations'; (vi) 'journalistic purposes'; (vii) 'in writing'; (viii) 'intra group schemes'; (ix) 'de-identification'; (x) 'data auditor'; (xi) 'anonymised data'; and (xii) 'anonymisation', that were present in the earlier drafts. The corresponding provisions (some of which imposed onerous obligations, such as mirroring a copy of sensitive personal data in India) have also been dropped.

4 Notice

The DPDP Bill requires data fiduciaries to provide data principals with a notice stating: (i) the personal data to be collected; and (ii) the purposes for which such personal data will be processed. Such notice is required to be provided *on or before requesting the data principal's consent* for processing. Every such notice must also be presented in clear and plain language (including the option to access such notice in English or in one of the 22 regional languages identified in the Eighth Schedule to the Constitution of India, *e.g.*, Hindi, Punjabi, Sanskrit, and Tamil), along with the contact details of the relevant data protection officer or person made responsible for responding to data principals' requests to exercise their rights under the DPDP Bill. These requirements must be met for all personal data processed once the DPDP Bill is notified and as soon as reasonably practicable thereafter for instances where processing has commenced before the DPDP Bill comes into force.

However, for instances where the personal data is not being collected directly from data principals (*e.g.*, where a person provides another person's name and address while placing an order to have medicines delivered to them), the DPDP Bill does not enable data fiduciaries to deliver such notice to data principals within a reasonably practicable time *after* collection (as was permitted under the 2021 Bill). Given this, data fiduciaries will be required to reassess their notice practices to ensure that they are able to, nonetheless, serve notices (in line with the timing prescribed for such notice) to data principals where data is not directly collected from them.

5 Consent

The DPDP Bill provides two broad bases for the processing of personal data – express consent and deemed consent.

5.1 Express Consent

The DPDP Bill allows for data fiduciaries to process personal data based on the consent obtained from individuals. Such consent must be free, specific, informed and unambiguous (although these factors have been left undefined) and must be provided through affirmative action for a *specified purpose* (as stated in the corresponding notice).

A data principal's right to withdraw her consent has also been recognised, following which the data fiduciaries must cease processing the personal data within reasonable time, unless such processing is required or authorised under applicable law. This would potentially push data fiduciaries to either delete the personal data they hold or to ensure that such data is no longer in the nature of 'personal data' (*e.g.*, by anonymising it). The DPDP Bill also clarifies that (i) data fiduciaries' performance of contracts that are concluded with data principals cannot be made conditional on consent to the processing of any personal data that is not necessary to perform the contract; and (ii) if the Data Protection Board questions the basis of processing, the data fiduciary bears the onus of proving that it has complied with the notice and consent requirements under the DPDP Bill.

Data principals can manage processing to which they have already consented, *via* a 'consent manager'. This framework (retained from the 2021 Bill) requires consent managers to register themselves with the Data Protection Board in the manner and subject to conditions (such as technical or financial conditions) as may be prescribed through delegated legislation. Similar frameworks already exist under Indian sectoral regulations, such as under the NBFC – Account Aggregator framework whose design was largely inspired by the NITI Aayog's Data Empowerment and Protection Architecture. It is plausible that consent managers under the DPDP Bill will also model themselves on these existing designs.

5.2 Deemed Consent

The DPDP Bill also permits the processing of personal data based on 'deemed consent'. Styled by the DPDP Bill as a bundle of other bases of processing, this includes some of the standard grounds typically recognised across other jurisdictions *e.g.*, for compliance with a judgement or order; medical emergencies; and employment-related purposes. It, however, also includes a scenario (i) where the data principal *voluntarily* provides her personal data and is reasonably expected to provide her personal data (Expectation Ground); and (ii) where processing may be required in public interest (PI Ground).

Data fiduciaries seeking to rely on the Expectation Ground must meet the reasonable expectation threshold, *i.e.*, the data principal must ***reasonably expect*** that such personal data must be provided in that particular circumstance. By implication, such data fiduciaries would have to demonstrate a *direct connection* or *nexus* between the processing of personal data and the purpose for its collection. For example, data fiduciaries operating retail stores may rely on the Expectation Ground to process payment information to process a sale transaction without having to seek express consent for doing so. However, where the processing activity *does not* have a reasonable nexus to the purpose for its collection, data fiduciaries cannot arguably rely on deemed consent for such processing. For example, the retail data fiduciary arguably cannot process date of birth information or anniversary dates of customers to process a sale transaction as it is likely that the data principal did not reasonably expect to have to provide such information in this circumstance.

Accordingly, this particular deemed consent scenario presents two primary obstacles: (i) data fiduciaries likely cannot rely on this ground to process personal data that may not be necessarily required to provide the concerned services (*e.g.*, in the second example above). In such circumstances, while the DPDP Bill does not require data fiduciaries to issue a notice to data principals in order to rely on the deemed consent basis, providing such a notice may nevertheless help/strengthen data fiduciaries' ability to rely on this ground by demonstrating that such processing was reasonably expected; and (ii) demonstrating that the personal data was voluntarily provided may be difficult in certain circumstances (*e.g.*, where a data principal is subject to CCTV surveillance but is not made aware of the same).

Further, data fiduciaries may not be able to effectively rely on certain other non-consensual grounds of processing because of how narrowly they have been drawn. For example, while mergers and acquisitions, prevention and detection of fraud, credit scoring, and debt recovery (among others) have been recognised under the DPDP Bill as grounds for the non-consensual processing of personal data, data fiduciaries must also demonstrate that such processing is being undertaken in the public interest (which itself is narrowly drawn to include situations such as the security of state and maintenance of public order). Given this, it is unlikely that this particular ground for non-consensual processing of personal data, for instance, will apply to the processing of personal data in connection with a potential merger between two *private* entities.

Further, the DPDP Bill also allows the Central Government to notify additional non-consensual grounds of processing based on factors such as processing in legitimate interests of the data fiduciary. However, even these additional grounds are subject to the processing being carried out in the public interest. Accordingly, this would also be applicable only in very limited circumstances.

Data fiduciaries must, accordingly, keep these principles and concerns in mind while determining *which* basis of processing to rely upon when handling personal data in a particular context.

6 Key Additional Considerations for Data Fiduciaries

While the obligations of data fiduciaries under the 2021 Bill and the DPDP Bill are largely similar, the DPDP Bill pares down the list. Specifically, data fiduciaries are required to do the following:

a. *Data Quality and Retention Requirements*

Data fiduciaries are now required to take *reasonable* efforts to only ensure personal data processed by them or on their behalf is accurate and complete (omitting '*not misleading and updated*', which was present under the 2021 Bill) where the data is (i) likely to be used by the data fiduciary to make a decision that affects the data principal, or (ii) is likely to be disclosed by the data fiduciary to another data fiduciary. This streamlines a data fiduciary's obligations in this regard and places the onus for correcting such information/keeping it updated upon the data principal, who may do so by exercising her rights under the DPDP Bill. For instance, matrimonial and dating sites could now potentially demonstrate incorporation of reasonable efforts without spending excessive time and resources to curb proliferation of fake profiles on their apps/sites (that would have otherwise been necessary under the 2021 Bill), to ensure processing of accurate data. Such reasonable efforts could include requiring customers to corroborate their details with relevant identification proof rather than verifying each customer's identity through publicly available records. Further, companies operating such sites can also now rely on their customer's (*i.e.*, the data principal's) obligation to provide accurate data (*as discussed in Section 9 of this update*).

Separately, under the DPDP Bill, the data fiduciary must cease to retain or remove the means by which personal data can be associated with a data principal, as soon as it is reasonable to assume that (i) the

purpose for which such personal data was collected is no longer being served; or (ii) retention is no longer necessary for legal or business purposes, although it is unclear what will fall within the realm of 'business purposes'.

b. *Breach Prevention and Reporting*

The DPDP Bill requires every data fiduciary to implement reasonable security safeguards to prevent personal data breaches and to protect the personal data in its possession or control. The specific standards for such safeguards, however, have not been prescribed.

When a personal data breach (which also includes unauthorised processing *as discussed in Section 3.4 of this update*) occurs, the data fiduciary is required to notify the Data Protection Board and each affected data principal in the manner and form subsequently prescribed in every instance. Given that the DPDP Bill does not build in a materiality threshold for reportability, this is a significant deviation from the 2021 Bill as well as global privacy regulations, where a data principal is only notified after considering the severity of harm caused by such breach. Practically, this means that if a company unintentionally shares data with its group entities, even if the level of harm caused by such accidental disclosure is low, the company would now be required to notify the Data Protection Board and *all* affected data principals. This significantly increases the compliance burden associated with such reporting. While the 72-hour reporting timeline prescribed under the 2021 Bill is absent here, the current draft suggests that the reporting timeline kicks in immediately.

c. *Exclusion of Privacy by Design and Fairness of Algorithms*

The DPDP Bill, unlike the 2021 Bill, does not require data fiduciaries to implement a privacy by design policy or to disclose the fairness of its algorithms. A data fiduciary is, however, required to implement appropriate technical and organisational measures to ensure effective adherence with the DPDP Bill's provisions. The DPDP Bill does not, however, prescribe *what* such '*appropriate technical and organisational measures*' will include, making this requirement (and compliance with it) subjective.

7 Significant Data Fiduciaries

The DPDP Bill creates a class of data fiduciaries referred to as significant data fiduciaries (**SDFs**) that may be notified separately by the Central Government. The Central Government can notify such SDFs based on factors such as (i) the volume and sensitivity of personal data processed; (ii) risk of harm to the data principal; (iii) potential impact on the sovereignty and integrity of India; (iv) risk to electoral democracy; (v) security of the State; and (vi) public order, and can even take into account such other factors that it considers necessary. For instance, payment applications processing a high volume of payments or telecom service providers may be classified as SDFs on the basis of a combination of such factors (*e.g.*, volume and sensitivity of personal data processed and risk of harm), or based on a single, standalone factor (simply, the volume of the personal data involved here).

Entities classified as SDFs will have the following additional obligations.

a. *Appointing a Data Protection Officer*

An SDF is required to appoint a Data Protection Office (**DPO**) based in India to act as its point of contact with respect to grievance redressal, as required under the DPDP Bill. Unlike the 2021 Bill, the DPO need not be a senior-level officer or key managerial personnel, making this (by comparison) a less onerous obligation.

b. *Appointing an Independent Data Auditor*

Under the DPDP Bill, an SDF will also have to appoint an Independent Data Auditor (IDA) to evaluate the SDF's compliance with the DPDP Bill. The 2021 Bill required SDFs to conduct *annual* audits to assess such compliance. The DPDP Bill does not, however, specify a timeline or periodicity for conducting such audits.

c. *Other Measures*

SDFs can also be required to undertake other measures as may be prescribed by the Central Government, such as a data protection impact assessment and periodic audit. This is a marked shift from the 2021 Bill, which mandatorily required SDFs to undertake data protection impact assessments before commencing any processing involving large-scale profiling.

8 Rights of Data Principals

Data principals have been provided specific rights under the DPDP Bill, *i.e.*, (i) the right to confirmation and access to information about personal data; (ii) the right to correction and erasure of personal data; and (iii) the right to nominate another person in the event of their death or incapacity, in addition to the right to grievance redressal. The right to data portability and the right to be forgotten are, however, conspicuously absent, markedly reducing the associated compliance burden.

In the context of the right to access, while the data principal can obtain information regarding all data fiduciaries that have access to their data, data fiduciaries are no longer required to also specify the identities of third-party data processors that have access to the same data. Under the DPDP Bill, data fiduciaries are not expressly empowered to reject requests from data principals in relation to the exercise of their rights. This suggests that data fiduciaries must mandatorily comply with all requests from data principals seeking to exercise their rights under the DPDP Bill. That said, the exercise of the right to erasure itself, while not subject to an express right of refusal, is circumscribed by two factors: the personal data no longer being necessary for (i) the purpose for which it was processed or (ii) for a legal purpose, indicating some room for interpretation here. The right of erasure and correction as contained in this draft also helps improve the quality of data available with data fiduciaries, by requiring verifiably authentic information for the exercise of a data principal's right to correction or erasure. However, the utility of this may be limited as given that most data is not verifiable, this would presumably be limited to: (i) information that *can be verified*, such as a residential address; and (ii) providing reasonably valid documents, such as *Aadhaar number*.

The right to grievance redressal requires the data fiduciary, (i) to establish a mechanism to register complaints; and (ii) respond to complaints received within seven days (even though a shorter response timeline can be prescribed). However, there is notably no express compulsion on data fiduciaries *to resolve* the complaint within the same timeline.

9 Duties of Data Principals

Data principals are now subject to certain duties under the DPDP Bill, specifically (i) compliance with laws while exercising their rights; (ii) prohibition on registering false or frivolous grievances, furnishing false particulars, suppressing material information, or impersonating another person; and (iii) duty to furnish verifiably authentic information when exercising their rights on correction or erasure. The breach of these duties, once determined by the Board as being significant, can be penalised with a fine of up to INR 10,000 (USD 122).

The imposition of these duties will likely deter trivial complaints leading to reduced compliance costs for companies and better data quality. For instance, as data principals may be penalised for furnishing false particulars or impersonating other persons, platform providers would arguably encounter fewer fake profiles/accounts. That being said, the risk to data principals is minimal, given that the Board will likely only impose a penalty if the non-compliance is significant.

10 Processing Children's Data

The DPDP Bill defines a 'child' as an individual under 18 years of age. It mandates verifiable parental consent (in a manner to be prescribed) to be obtained before processing a child's personal data. The DPDP Bill does not, however, provide any guidance on what may constitute '*verifiable parental consent*', which may vary depending on the risks and likelihood of harm involved in processing. For instance, while email verification might suffice for activation of a social media account, more stringent measures like KYC checks may be required for obtaining financial or medical services involving processing a child's personal data. Further, verifiable parental consent will likely pose *practical obstacles*, including where information has been collected offline but is otherwise digitally processed. For instance, any store that a teenager may shop at would necessarily require the consent of the parent in order to collect any details about the child (such as a phone number) - consent that likely cannot be obtained where the parent does not accompany the child. In an online context, an online gaming platform may be required to obtain verifiable parental consent on multiple occasions for additional processing activities not covered under the original notice/consent moment (e.g., where an online gaming platform also introduces a messaging functionality and must process additional personal data to enable the child to use such a functionality).

The DPDP Bill, unlike the 2021 Bill, does not expressly mandate verification of the child's age. However, as data fiduciaries are obliged to obtain verifiable parental consent prior to processing a child's data, data fiduciaries will have to ascertain if the data principals providing personal data to them are minors. This requirement may compound privacy concerns, as data fiduciaries may be required to collect *more* personal data in order to ensure compliance.

Data fiduciaries are barred from tracking, monitoring the behaviour of, or targeting advertisements directed at children, irrespective of whether these activities are likely to cause 'significant harm' to the child. The Government can exempt any data fiduciary from (i) the requirement of obtaining parental consent; and (ii) the bar on tracking, behavioural monitoring, and targeted advertising of/to children for certain purposes of processing to be prescribed by the Government.

Separately, given the level of protection afforded to children's data, it is unclear how (if at all) *deemed consent*, especially the Expectation Ground, may be relied upon by data fiduciaries to process children's data under the various deemed consent grounds (see Section 5.2). The DPDP Bill does not appear to expressly restrict the ability of data fiduciaries to process children's data on such bases.

11 International Transfer and Data Localisation

Unlike the 2021 Bill, the DPDP Bill does not impose a hard localisation requirement *i.e.*, to process and store critical personal data only in India. It also does not require data fiduciaries to store a mirror copy of sensitive personal data in India. As discussed above, the DPDP Bill no longer sub-categorises personal data into sensitive personal data and critical personal data and all personal data may be transferred outside India to countries or territories that are notified by the Central Government (based on factors it considers necessary) in accordance

with the terms and conditions that it may specify. Such terms are not expected to prescribe an adequacy determination or impose other conditions such as intra-group schemes or standard contractual clauses that were required under the 2021 Bill for cross-border transfers. This is a welcome step for the industry, which had pushed back on the hard localisation and mirror copy requirements. However, this will still be subject to the list of countries notified by the Government for international transfers (and the allied terms, if any).

The DPDP Bill, however, clarifies that its provisions are in addition to (and not in derogation of) existing laws, and only in cases of a conflict will the provisions of the DPDP Bill prevail. Given this, any localisation requirements under existing laws (such as those applicable to payments data that also qualifies as personal data) will continue to apply even after the DPDP Bill (if notified in its present form) comes into force.

12 Enforcement of the DPDP Bill

12.1 Establishing the Data Protection Board

The Data Protection Board is the enforcement authority under the DPDP Bill. The DPDP Bill is silent on the strength and composition of the Data Protection Board, the process of appointment and service of officers, their conditions of service, and removal of its chairperson, which will be prescribed by the Central Government.

The Data Protection Board is entrusted with the following functions: (i) determining non-compliance with the provisions of the DPDP Bill by a person and imposing financial penalties where the non-compliance is significant; (ii) registering consent managers; (iii) prescribing standards for processing of personal data necessary for research, archiving or statistical purposes; (iv) receiving notifications from data fiduciaries or data processors regarding personal data breach and directing them to adopt urgent measures; (v) issuing necessary directions from time to time to discharge its functions. The DPDP Bill does not specify any guiding factors that the Data Protection Board may take into account before issuing such directions. The breadth of this provision may even permit the Data Protection Board to impose non-monetary penalties (specifically called out under the 2021 Bill), issue interim orders and take other similar measures, in excess of the financial penalties specified.

The DPDP Bill also reiterates the bar on jurisdiction of civil courts to entertain suits or take any action, including the granting of an injunction, under the provisions of the DPDP Bill. However, this does not foreclose remedies such as enforcement of writ jurisdiction.

In contrast to the 2021 Bill, the Data Protection Board has limited powers to initiate *suo motu* inquiries against data fiduciaries/data processors. It can only act on complaints from affected persons, references from governments, directions from courts, or on its own motion against data principals acting in violation of their duties. While this is a welcome move shielding data fiduciaries and processors from activist adjudication on the part of an independent regulator, it does not preclude data principals and government from bringing complaints before the Data Protection Board with regard to large public-facing entities. Further, it does not have the power to seize documents or information, prevent access to premises, take custody of equipment or call for information from a data fiduciary or data processor, except as part of any inquiry.

12.2 Appeal

The DPDP Bill does not provide for an appellate authority before whom appeals against the decisions of Data Protection Board will lie. Instead, the Data Protection Board may form a group specifically for a review hearing (either on its own or through a representation made before it) to modify, withdraw, suspend, or cancel an

order issued by the Data Protection Board. The DPDP Bill also permits an affected party to prefer an appeal before the relevant High Court within 60 days of the issuance of the impugned order of the Data Protection Board.

13 Penalties

13.1 Omitting Criminal Offences and Compensation

The DPDP Bill has entirely omitted (i) criminal penalties imposed for the re-identification of de-identified data, and processing of re-identified data without consent; and (ii) a scheme that enabled individuals who suffered harm caused by data fiduciaries to receive compensation. This has simplified the regime for adjudication, avoiding onerous penalties in addition to specific, uncapped compensation. Moreover, the derecognition of criminal offences altogether grants data fiduciaries the latitude to implement and experiment with de-identification and anonymisation of personal data.

13.2 Liabilities for Non-compliances

The DPDP Bill prescribes the following penalties:

	Description of Non-Compliance	Penalty Prescribed
1.	Failure of data processor or fiduciary to take reasonable security safeguards to prevent personal data breach	Up to INR 250 crore (USD 30 million)
2.	Failure of data fiduciary to notify the Data Protection Board and affected data principals of a personal data breach	Up to INR 200 crore (USD 25 million)
3.	Non-fulfilment of obligations in relation to children's personal data	Up to INR 200 crore (USD 25 million)
4.	SDF's non-fulfilment of additional obligations	Up to INR 150 crore (USD 18 million)
5.	Any other non-compliance with other provisions of the DPDP Bill	Up to INR 50 crore (USD 6 million)

The 2021 Bill prescribed a number of penalties for contravention of its provisions, with the two most notable categories of violations requiring data fiduciaries to pay sums of INR 5 crore (USD 600,000) or 2% of its total worldwide turnover in the preceding financial year (whichever was higher) for certain violations on the one hand, and INR 15 crore (USD 2 million), or 4% of their worldwide turnover (whichever was higher) in other cases. The DPDP Bill, on the other hand, specifies that the financial penalties that the Data Protection Board may impose cannot exceed INR 500 crore (USD 61 million) *per instance*. There is no indication of what may be considered a single instance, but it is likely that the Data Protection Board will club multiple contraventions forming part of a single cause of action as one instance.

13.3 Voluntary Undertakings

The DPDP Bill has introduced a novel provision (not contemplated under any of the previous iterations of the draft law), allowing a person, at any stage of the proceedings against such person in relation to non-compliance with the DPDP Bill, to submit voluntary undertakings to remedy such non-compliance. These voluntary undertakings may include undertakings to take specified actions within a particular time or to refrain from

doing so; or to make the undertaking public. The DPDP Bill also imposes a bar on proceedings that can be initiated in relation to the contents of the voluntary undertaking once the Data Protection Board has accepted it.

A parallel may be drawn with the concept of 'compounding' schemes under other laws, such as under foreign exchange laws. Much like the Singaporean data protection law, this measure is likely to allow the Data Protection Board to refocus proceedings from reprimand to remediation. This is a welcome move for all stakeholders since this permits proactive and practical measures to be implemented with sufficient accountability.