Technology Law Analysis

November 24, 2022

DIGITAL PERSONAL DATA PROTECTION BILL, 2022: ANALYSIS AND POTENTIAL IMPACT ON BUSINESSES

INTRODUCTION

The Ministry of Electronics and Information Technology has published the draft Digital Personal Data Protection Bill, 2022 ("**Proposed Law**") (accessible here) on November 18, 2022 for public consultation. The last date of submission of stakeholder comments is December 17, 2022.

The Indian Government has been in the process of introducing an extensive data protection law since 2018. Three drafts were issued prior to the current draft of the Proposed Law. The current draft of the Proposed Law is a significant change from its predecessor drafts and is more open – ended, leaving much to be prescribed by the Central Government. It does away with different categories of datasets (like critical or sensitive data). It also omits several onerous compliances including data localization, enhanced consent requirements for sensitive personal data, penalties on worldwide turnover, and also excludes governance of non-personal data The Data Protection Board of India ("**Board**") is proposed to be the adjudicatory body for enforcement of the Proposed Law.

Our analysis of key provisions of the Proposed Law, their impact on businesses, and our recommendations are below.

1. APPLICABILITY

The Proposed Law applies to the processing of **digital** personal data in India, where the personal data is (i) collected from the data principal online; and (ii) collected offline and subsequently digitized.[1] While the Proposed Law uses the word "and" between (i) and (ii), the intent appears to be to make these "or" conditions so that the Proposed Law applies in either of the situations.

The Proposed Law is also designed to have **extra territorial application,** i.e. it applies to the processing of personal data outside India when such processing is in connection with any profiling of, or activity of offering goods or services to data principals located within the territory of India.[2] Thus, the Proposed Law will apply to foreign entities as well, when this condition is satisfied.

"Profiling" has been defined broadly to mean any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal.[3]

The Proposed Law defines "personal data" broadly to include any data about an individual who is identifiable by or in relation to such data.[4] It is not clear what is the level of identification required e.g. is it by name or any other attribute e.g. identification of a person staying at X place.

Notably, the Proposed Law, unlike the earlier versions, does not distinguish between different types of data and all obligations and limitations (e.g. cross border transfer) under the Proposed Law apply to all "personal data" sets. However, some provisions suggest that the Central Government may make such a distinction for certain compliances.

The provisions of the Proposed Law do not apply to, inter alia, (i) non-automated processing of personal data[5], and (ii) offline personal data.[6] [7] The fact that non-automated processing is not covered is also clear from the definition of "processing" (an automated operation or set of operations performed on digital personal data). With these exclusions, several non-digital businesses (which do not convert personal data into digital form subsequently), and businesses which manually collect and process personal data are excluded from the scope of the Proposed Law.

2. DATA FIDUCIARY, PRINCIPAL AND PROCESSOR

The key definitions under the Proposed Law are as follows:

- "Data Fiduciary" is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.[8] In our view, the means of processing should not be the part of definition and only determination of the purpose should be retained in the definition. This is because the "means" may be determined by the data processor in several cases.
- "Data Principal" is the individual to whom the personal data relates and where such an individual is a child includes the parents or lawful guardian of such a child.[9] Thus, it is clear that the Proposed Law covers Data only of natural individuals.
- "Data Processor" is any person who processes personal data on behalf of a data fiduciary.[10]

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

3. NOTICE AND CONSENT

The Proposed Law imposes the obligation upon the data fiduciary to provide itemized notice[11] of the data sets sought to be collected and purpose of processing; and obtain consent[12] from the data principal on or before processing personal data. The languages of the notice should be clear and plain.[13]

The consent should be free, specific, informed and unambiguous.[14]

The Proposed Law states that "notice" can be a separate document or part of the same document through which the personal data is sought to be collected, or in such other form as may be prescribed. The Proposed Law could additionally add that the notice can be provided in the same document through which consent is being sought.[15]

Where a data principal has given consent to processing of her personal data prior to the commencement of the Proposed Law, the data fiduciary is required to provide an itemised notice in clear and plain language containing a description of the personal data collected and the purpose for which such data has been processed, as soon as it is reasonably practicable.[16] This requirement should apply only prospectively since data fiduciaries may not have maintained records of the purpose of processing of personal data in the past in the absence of a law requiring this.

The data fiduciary is required to give an option to the data principal to access the request for consent in English OR any language specified in the Eighth Schedule to the Constitution of India.[17] This requirement may be difficult for some entities, such as online platforms which only support the English language. It is advisable that platforms should be required to provide consent only in the languages supported by the platform.

Additionally, like the previous drafts, the Proposed Law recognizes the role of 'consent managers.' The consent manager has been defined as a data fiduciary which enables a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.[18] However, since content managers are merely collecting consent on behalf of the data fiduciary, they should not be termed as "data fiduciaries" since unlike consent managers, data fiduciaries determine the purpose and means of processing of personal data and are therefore subject to strict compliances.

Deemed Consent

The Proposed Law introduces the concept of 'deemed consent' where the data principal is deemed to have given consent for the processing of their personal data. under the following instances:

1. Where the data principal voluntarily provides personal data to the data fiduciary and it is reasonably expected that such personal data may be provided;[19]
2. For the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;[20]
3. For compliance with any judgment or order issued under any law;[21]
4. For responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;[22]
5. In case of taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of diseases etc.;[23]
6. For taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order;[24]
7. For purposes related to employment including prevention of corporate espionage, recruitment, termination of employment, maintenance of confidentiality, verification of attendance and assessment of performance, etc.;[25]
8. In the public interest'[26] the Proposed Law includes a broad and inclusive list of what may amount to 'public interest', including credit scoring, recovery of debt, mergers and acquisitions, and '*any fair and reasonable purpose as may be prescribed,' after* taking into account certain considerations[27].
9. For fair and reasonable purpose as may be prescribed by the Central Government, including based on legitimate interests of the data fiduciary[28], and reasonable expectation of processing of personal data.[29]

The implication of the inclusion of the concept of 'deemed consent' is that entities need not obtain consent from the data principal for the above-mentioned purposes of collection and processing. This is along the lines of the concept of alternate grounds of processing of data under the GDPR. In our view, the instances specified at 3, and 5-9 above should not be treated as consent- based grounds for processing. Treating such instances as consent-based grounds for processing would imply that consent may be withdrawn by the data principal, which cannot be the intent of the Proposed Law. To illustrate: Consent may be deemed for compliance with any judgment or order issued under any law. A data principal cannot be permitted to withdraw their consent in case of such legal obligations.

It would be more appropriate for processing on such grounds to be categorized as "other grounds of processing", or "lawful grounds for processing" which are not consent-based. Further, in some instances the exact purposes for which deemed consent is being given is not clear .

Other contemporaneous legislations such as the GDPR have multiple grounds for lawful processing of personal data apart from 'consent', which the Proposed Law appears to have clubbed under the single head of 'deemed consent.' The GDPR permits processing of personal data in case of (1) contractual necessity, (2) legitimate interests, (3) legal obligations, (4) public interest, and (5) vital interest (i.e., in matters of life or death).

The term "public interest" is used in Sections 8(9) and 30(2) other than Section 8(8) discussed in point 8 above. It

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024

needs to be clarified whether the guidance provided under Section 8(8) applies in relation to Sections 8(9) and Section 30(2) as well. .Additionally, several inclusions under Section 8(8) such as credit scoring, recovery of debt, etc. cannot be termed as "public interest".

4. DATA PRINCIPAL RIGHTS AND DUTIES

The data principals may exercise certain rights with respect to their personal data. While the Proposed Law enumerates the rights, it does not set out the procedure/manner in which such rights may be exercised:

i. Right to information about personal data: The data principal has the right to obtain (i) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; (ii) a summary of the personal data being processed or that has been processed and the processing activities; (iii) identities of all the data fiduciaries with whom the personal data has been shared along with the categories of personal data so shared and; (iv) any other information as may be prescribed by the Central Government.[30] The right to obtain a summary of the manner in which personal data has been processed in the past may be problematic as entities may not have maintained this record in the past in the absence of a law requiring them to do so. Therefore, this right should only apply prospectively.

ii. Correction and erasure of personal data: The data principal has the right to correction of their personal data "in such manner as may be prescribed". Upon receipt of a request for correction/erasure, a data fiduciary is required to (i) correct inaccurate or misleading personal data; (ii) complete any incomplete personal data and (iii) update relevant personal data. The data principal may also request for erasure of their personal data which is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.[31]

iii. Grievance redressal: Data principals have the right to register their grievances with the data fiduciary. If the response of the data fiduciary is not satisfactory or if the response is not received within seven days/such shorter period as may be prescribed, the data principal may register a complaint with the Board.[32] The government should consider defining 'grievance' similar to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Guidelines") for clarity on the types of grievances that can be registered.

iv. Complaints to the Board: If the response of the data fiduciary is not satisfactory or if the response is not received within seven days/such shorter period as may be prescribed, the data principal may register a complaint with the Board.[33] Currently it is unclear in which instances a shorter timeline may be prescribed. Time period of seven days appears very less. Rules can prescribe different timelines for different types of grievances.

v. Right to nominate: The data principal has the right to nominate any other individual to exercise the above-mentioned rights under the Proposed Law in the event of the death of the data principal.[34] Data fiduciaries should not be burdened with ascertaining the validity of nomination. Hence, in case of disputed nomination, the Board should be given power to determine the appropriate nominee.

Notably, a data principal does not appear to have any rights against the data processor. The above-mentioned rights are only applicable with respect to a data fiduciary.

There are also several duties of data principals under the Proposed Law. Data principals are prohibited from (i) registering a false or frivolous grievance or complaint with a data fiduciary and (ii) from providing false information or suppressing material information, or impersonate another person, including while applying for any document, service, proof of identity, or proof of address. It is unclear if this obligation only relates to data provided to the government or also to private bodies. The Proposed Law imposes a penalty of up to INR 10,000 for non-compliance by the data principal of its duties.[35]

Moreover, the prohibition on providing false information seems to overlap with the prohibition under the Indian Penal Code, 1100%[36] ("**IPC**") which prohibits the furnishing of false information to any public servant.

5. DATA FIDUCIARY OBLIGATIONS

The Proposed Law imposes certain obligations on the data fiduciaries to ensure security of personal data by taking reasonable security safeguards to prevent personal data breach. The Proposed Law does not prescribe or recommend the standards that should be implemented. Additionally, data fiduciaries should see to it that personal data processed by or on behalf of it is accurate and complete. A snapshot of the data fiduciary obligations are provided below:

- The data fiduciary is responsible for compliance with the Proposed Law (irrespective of whether a processing is undertaken by a processor/data fiduciary on its behalf or; if the data principal is non-compliant with their duties;[37]
- Undertake reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete if the personal data is likely to be used by the data fiduciary to make a decision that "affects" the data principal or if the personal data is likely to be disclosed another data fiduciary;[38]
- Implement appropriate technical and organizational measures;[39]
- Protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach;[40]
- In the event of a personal data breach; notify the Board and each affected data principal;[41]
- Shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer ("**DPO**"), if applicable, or a person who is able to answer on behalf of the data fiduciary, the data principal's questions about the processing of their personal data.[42]
- Share, transfer or transmit the personal data to any data fiduciary or data processor with consent of the data principal.[43]

With respect to ensuring accuracy of personal data where it affects the data principal,the scope of the word "affect" is unclear. It should be clarified that the obligation triggers when it affects the ability of the data principals to avail of some benefits (e.g. goods or services) For instance, a decision on whether to provide a loan to a data principal.

Further , the requirement to ensure accuracy at the time of disclosure to other data fiduciaries[44] should also exist only in cases where it affects the data principal. Otherwise this requirement is onerous as data fiduciaries may simply be transferring/sharing data sets to group entities that are data fiduciaries as well.

The Proposed Law does not clearly distinguish between the role of a DPO (see *Significant Data Fiduciaries* below) and grievance officer unlike the previous drafts and the Intermediary Guidelines which contain similar grievance redressal obligations. Instead, the Proposed Law requires the DPO to ensure compliance as well as redress data principal grievances. We recommend that the roles of the DPO and grievance officer be delineated for clarity and independence of grievance redressal mechanism.

The Proposed Law also does not specify the technical and organizational measures/security safeguards required to be implemented which is a welcome move. Industry specific standards can develop over time basis factors such as sensitivity of the data, risk involved, nature of the industry etc. These standards can be adhered to by entities in the industry.

6. DATA PROCESSOR OBLIGATIONS

- Data processors who process personal data on behalf of other entities have certain independent statutory obligations under the Proposed Law: Protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach;[45]
- In the event of a personal data breach; notify the Board and each affected data principal;[46]
- Undertake sub-contracting of processing activities if permitted under the contract with the data fiduciary.[47]

The Proposed Law does not prohibit contractual arrangements between the data fiduciary and the data processor in respect of inter-se liability for obligations.

7. SIGNIFICANT DATA FIDUCIARIES

The Central Government may classify a Data Fiduciary or a class of Data Fiduciary as a Significant Data Fiduciary ("**SDF**") based on the volume and sensitivity of the data processed by them, the risk of harm to the data principal, potential impact on the sovereignty and integrity of India and other such factors.[48] A SDF would have certain additional obligations such as having to appoint a DPO in India[49] and an independent Data Auditor[50], along with undertaking certain additional measures such as data protection impact assessments.[51] In this Section, "such other measures" is open ended. Guidance should be provided in the Act itself as to what type of measures could be imposed on SDFs.

8. EXEMPTIONS

The Proposed Law exempts certain compliances including data fiduciary obligations, notice and consent requirements for certain specified circumstances including processing of personal data is necessary for enforcing any legal right or claim; performance of any judicial or quasi-judicial function; personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; and where the personal data of data principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India.[52]

Additionally, Proposed Law also enables the Central Government to exempt the applicability of the Proposed Law by way of notification under the following circumstances:

- Exempt an instrumentality of the State (which could include entities that are financially, functionally and administratively dominated by or under the control of the Central Government) from compliance with this law in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these. This exemption should ideally be subject to procedural safeguards of necessity, proportionality, and legality.[53]
- Exempt applicability of the Proposed Law to the processing of personal data necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards which may be notified by the Board.[54]

Additionally, the Proposed Law states that the Central Government, by notification, notify certain data fiduciaries or class of data fiduciaries to whom the provisions of Section 6, Section 9(2), Section 9(6) and Sections 10, 11 and 12 of the Proposed Law will not apply. The reason for selection of these specific provisions is not clear in the Proposed Law. Additionally, it is unclear currently what types of data fiduciaries may be excluded by way of this provision.

It should also be clarified that the exemption for processing of personal data by courts/tribunals also applies to judicial bodies outside India. Litigation proceedings involving Indian multinational companies may take place globally. Disputes involving Indian parties are also increasingly referred to foreign institutional arbitrations.

The Proposed Law contemplates an exemption to outsourcing activities[55] i.e. where personal data of individuals outside India is processed in India basis a contract. However, the cross-border transfer restriction continues to apply in respect of such data as well.[56] The continuance of applicability of the cross-border transfer restrictions to personal data of data principals outside India is inefficient and contradictory to the intent behind providing the exemption for outsourcing activities. Further, we also note that the State and its instrumentalities have been absolved from the requirement to erase data at the end of processing and when the purpose of collection of the personal data has been fulfilled[57] (see *Data Retention* below). This may lead to arbitrary retention of data for extended periods of time without reasonable justification.

9. RETENTION OF PERSONAL DATA

Personal data should not be retained if the (i) retention is no longer necessary for legal or business purposes[58] and (ii) the purpose for which such personal data was collected is no longer being served by its retention.[59]

The term "business purpose" is not defined. Thus, data fiduciaries may have flexibility in defining business purpose at the time of taking consent. The retention period can be determined basis factors relevant to a specific industry since retention of data for longer periods of time may be significant for some industries. For instance, longer retention periods of medical records is an industry practice in certain jurisdictions since it is beneficial to the data principal.

10. TRANSFER AND CROSS-BORDER TRANSFERS OF DATA

Data may be transferred between data fiduciaries, or data fiduciary and data processor only upon the data principal consenting to such transfer.[60]

Personal data can be transferred to only those countries which are notified by the Central Government in accordance with terms and conditions as may be prescribed.[61] At present, there is no sight on the countries likely to be notified, nor factors basis which countries may be notified. It is possible that this determination by the Central Government will be based on political considerations and geo-political issues, in the absence of the Proposed Law identifying the basis on which countries will be white-listed.

Further, since "personal data" is broadly defined, this Section will apply to all types of data, irrespective of whether it is sensitive or not. A better approach may be an adequacy test, i.e., transfers permitted to countries having an adequate level of data protection.

11. CHILDREN'S DATA

Under the Proposed Law, 'child' is an individual below eighteen years.[62] However, the Proposed Law (unlike its predecessor drafts) does not require data fiduciaries to undertake KYC to determine if a user is in fact a child. Accordingly, it is unclear whether the obligations in relation to processing of personal data of children apply only upon users disclosing they are children.

Data fiduciaries processing personal data of children have to comply with additional obligations:

- Obtain verifiable parental / guardian's consent prior to processing the child's personal data, in a form as may be prescribed;[63]
- Data fiduciaries are prohibited from undertaking processing of personal data of children which is likely to cause harm to a child, as may be prescribed by the Central Government.[64]
- Data fiduciaries are prohibited from, tracking and behaviorally monitoring children, and directing targeted advertising at them;[65]

Further, there appears to be a drafting error in the wording of the prohibition on tracking and targeted advertising, which is not linked to processing of personal data of a child, unlike the previous sub-section.

In any case, the Guidelines for the Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 ("**Misleading Ads Guidelines**") issued by the Central Consumer Protection Authority, already contain exhaustive provisions regulating advertisements that address or target children. The Misleading Ads Guidelines apply to all forms, format, or mediums of advertisements. The provisions under the Misleading Ad Guidelines, being a special law dealing with such advertisements, should be the sole regulations for such advertisements, and the prohibition under the Proposed Law should be deleted.

12. DATA PROTECTION BOARD OF INDIA

An adjudicatory body - the Board is proposed to be established under the Proposed Law . The Board will function digitally, and will be digital by design in terms of receipt of complaints, hearings, pronouncement of decisions, and other functions.[66]

The functions of the Board appear to be mainly adjudicatory in nature, and would include determination of non-compliance; and adoption of urgent remedial measures in cases of personal data breaches.

a. Independence of the Board

   While it is stated to be an 'independent body,' the composition of the Board, process of selection, removal, terms and conditions of appointment and services, are left to be prescribed by the Central Government.

   In addition, it may be noted that the chief executive appointed to manage the affairs of the Board, will be appointed by the Central Government, and the Central Government will determine the terms and conditions of service. Accordingly, the scope of the Board's independence in view of these provisions is unclear.

b. Qualifications of the Board Members

   Typically, legislations creating statutory bodies specify the composition and qualifications of the members of the body as opposed to including it in the rules and regulations. However, the Proposed Law does not set out the qualifications of the Board members. Since the Board is proposed to perform an adjudicatory function it is recommended that the Board should comprise of at least one judicial person and also one technical member for every determination.

c. Orders of the Board

   There is no specific guidance as to the nature of orders the Board may pass. While one of the factors to be taken into account at the time of levy of penalty by the Board is whether mitigation measures were undertaken by the individual, there is no clarity on what types of mitigation measures may be taken. In some legislations, the regulatory and adjudicatory bodies are authorized to issue improvement notices and orders for compliance

before issuing final orders for levy of penalty. The Proposed Law should also enlist the types of orders that may be passed by the Board.

d. Appeals from Board Orders

Board orders will be deemed to be decrees made by a civil court and may be appealed to the High Courts.

Resultantly, once the Board passes an order, an execution petition can be filed seeking compliance with the order. If the relevant person does not comply with the provisions, consequences under the Code of Civil Procedure, 1908 will follow. The Proposed Law does not clarify which High Court will have jurisdiction to hear appeals. Ideally, the High Court of the State where the data principal is resident should be explicitly vested with jurisdiction to hear appeals arising from orders of the Board.

13. VOLUNTARY UNDERTAKING

The Proposed Law also introduces the concept of 'voluntary undertaking.'[67] The Board may accept a voluntary undertaking in respect of any matter related to compliance with provisions of Proposed Law from any person at any stage.[68] Such voluntary undertaking may be publicized,[69] However, the language of the provision is unclear on the aspect of whether every instance of voluntary undertaking has to be publicized or whether the Board may require specific instances of voluntary undertaking to be published.

14. PERSONAL DATA BREACHES

"Personal Data Breach" has been defined 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**.[70]

The Proposed Law obligates the data fiduciary or the data processor to notify the Board and the affected data principals in the event of a personal data breach.[71] The obligation to notify data principals does not exist under Indian law currently. It is unclear why both the Board as well as the data principal must be informed in the first instance. Ideally, the obligation should be limited to informing the Board, and upon the Board requiring notification to the data principal depending on the severity of the issue or the likely impact upon the data principal, they may be informed. Even if data principals are to be informed at the first instance, this should be limited to situations where certain action is required on part of the data principal for security, such as changing of password.

It appears from the wording of the provision that the data fiduciary and data processor can contractually determine which of the two will be responsible for breach notification.

Currently, reporting obligations in case of "cyber security incidents" exists under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**2013 Rules**") and the recently introduced direction relating to "information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet" issued by the Indian Computer Emergency Response Team ("**CERT-In**"). Under the Information Technology Act, 2000 ("IT Act"), CERT-In, which is a statutory body empowered to deal with cyber security issues, has the powers to issue guidelines, directions, etc. to entities in response to cyber security incidents. On a similar note, the Proposed Law also empowers the Board to direct data fiduciaries to adopt urgent measures to remedy personal data breaches or mitigate harm caused to data principals. Therefore, in cases of incidents reportable under both laws, an entity may need to not only report the breach to two statutory bodies but may also need to comply with directions issued by two separate bodies. Additionally, the question arises if the Board will have the expertise to understand the complexity of data breaches to be able to issue measures that will help remedy a breach or mitigate harm.

15. PENALTIES

Upon the conduct of an inquiry, if the Board finds non-compliance by an individual to be significant, it may impose a financial penalty for up to INR 500 crore.[72] The Proposed Law also prescribes specific penalties of INR 50 crore – INR 250 crore for failure to take reasonable security safeguards to prevent personal data breach; failure to notify the Board and affected data principals of data breaches; non-compliance with additional obligations for SDFs.[73] The most significant penalties under the Proposed Law are for failure to comply with the data-breach obligations under the Proposed Law.

Unlike the previous drafts, the Proposed Law does not enable affected data principals to seek compensation for breaches by data fiduciaries. This may disincentivize individuals from pursuing costly adjudication before the Board.

The Act should provide that the Board should publish a guidance for determination of the quantum of penalties (to bring in transparency). Additionally, the decisions of the Board should be made publicly available.

16. DELEGATED LEGISLATION

In total, at 18 places, the Proposed Law contains the term "as may be prescribed" meaning that the scope of obligations and restrictions remains open ended for now . These aspects include form and manner of personal data breach notifications; registration and functions of consent manager; parental consent for processing of personal data of children; composition of the Board; conduct of data protection impact assessments and audits etc. It is recommended that appropriate legislative guidance be provided for each rule making power. .

17. TIMELINES FOR COMPLIANCE AND OTHER EXISTING LAWS

Unlike its predecessor drafts, there are no specific timelines for compliance prescribed for the implementation of the Proposed Law. This should be clearly indicated, so that businesses can plan their compliances accordingly. It should also be clarified that the Proposed Law will only apply prospectively.

The Proposed Law states that in the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict. There are sectoral laws where there may be provisions contrary to the Proposed Law. E.g. RBI has mandated payments data

localization but under Section 17 of the Proposed Law cross border data transfer may be permissible. This may create confusion in terms of compliance. Hence, clarity is required in this regard.

Once the Proposed Law is enacted, Section 43A of the IT Act (this provision provides for the compensation for failure to protect data and specifically, the SPDI Rules has been enacted for this purpose) will be omitted.[74] The Proposed Law does not explicitly repeal Section 72A of the IT Act, which prescribes a penalty (including imprisonment and fines) for service providers disclosing personal information about a person without their consent, or in breach of contract, with intent to cause, or knowledge that such breach is likely to cause wrongful loss to the person, or wrongful gain to the service provider. The Government may consider repealing this provision as well, and consolidating all prohibitions under the Proposed Law.

The Proposed Law seeks to amend the Right to Information Act, 2005 to bar the disclosure of personal data if its disclosure has no relationship to any public activity or interest or if it would cause unwarranted invasion of the privacy of the individual. However, a Public Information Officer can direct the disclosure of such personal information if the authority is satisfied that "the larger public interest."[75]

– Varsha Rajesh, Tanisha Khanna, Aparna Gaur & Gowree Gokhale

You can direct your queries or comments to the authors

---

[1] Section 4(1), Proposed Law.

[2] Section 4(2), Proposed Law.

[3] Section 4(2), Proposed Law.

[4] Section 2(13), Proposed Law.

[5] Section 4(3)(a), Proposed Law.

[6] Section 4(3)(b), Proposed Law.

[7] Additionally the Proposed Law also provides an exemption for (i) personal data processed by an individual for any personal or domestic purpose; and (ii) personal data about an individual that is contained in a record that has been in existence for at least 100 years.

[8] Section 2(5), Proposed Law.

[9] Section 2(6), Proposed Law.

[10] Section 2(7), Proposed Law.

[11] Section 6, Proposed Law.

[12] Section 7, Proposed Law.

[13] Section 6(1), Proposed Law.

[14] Section 7(1), Proposed Law.

[15] Explanation (a) to Section 6(2), Proposed Law.

[16] Section 6(2), Proposed Law.

[17] Section 6(3), Proposed Law.

[18] Section 7(6), Proposed Law.

[19] Section 8(1), Proposed Law.

[20] Section 8(2), Proposed Law.

[21] Section 8(3), Proposed Law.

[22] Section 8(4), Proposed Law.

[23] Section 8(5), Proposed Law.

[24] Section 8(6), Proposed Law.

[25] Section 8(7), Proposed Law.

[26] Section 8(8), Proposed Law.

[27] As per Section 8(8) of the Proposed Law, 'public interest' includes *"(a) prevention and detection of fraud; (b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws; (c) network and information security; (d) credit scoring; (e) operation of search engines for processing of publicly available personal data; (f) processing of publicly available personal data; and (g) recovery of debt.*"

[28] Section 8(9)(a), Proposed Law.

[29] Section 8(9)(c), Proposed Law.

[30] Section 12, Proposed Law.

[31] Section 13, Proposed Law.

[32] Section 14, Proposed Law.

[33] Section 14, Proposed Law.

[34] Section 15, Proposed Law.

[35] Section 16, Proposed Law.

[36] Section 177, IPC.

[37] Section 9(1), Proposed Law.

[38] Section 9(2), Proposed Law.

[39] Section 9(3), Proposed Law.

[40] Section 9(4), Proposed Law.

[41] Section 9(5), Proposed Law.

[42] Section 9(7), Proposed Law.

[43] Section 9(9), Proposed Law.

[44] Section 9(2)(a), Proposed Law.

[45] Section 9(4), Proposed Law.

[46] Section 9(5), Proposed Law.

[47] Section 9(9), Proposed Law.

[48] Section 11(1), Proposed Law.

[49] Section 11(2)(a), Proposed Law.

[50] Section 11(2)(b), Proposed Law.

[51] Section 11(2)(c), Proposed Law.

[52] Section 18(1), Proposed Law.

[53] Section 18 2(a), Proposed Law.

[54] Section 18 2(b), Proposed Law.

[55] Section 18(1)(d), Proposed Law.

[56] Section 17, Proposed Law.

[57] Section 9(6), Proposed Law.

[58] Section 9(6)(b), Proposed Law.

[59] Section 9(6)(a), Proposed Law.

[60] Section 9(9), Proposed Law.

[61] Section 17, Proposed Law.

[62] Section 2(3), Proposed Law.

[63] Section 10(1), Proposed Law.

[64] Section 10(2), Proposed Law.

[65] Section 10(3), Proposed Law.

[66] Section 19, Proposed Law.

[67] Section 24, Proposed Law.

[68] Section 24(1), Proposed Law.

[69] Section 24(2), Proposed Law.

[70] Section 2(14), Proposed Law.

[71] Section 9(5), Proposed Law.

[72] Section 25(1), Proposed Law.

[73] Schedule 1, Proposed Law.

[74] Section 30(1)(a), Proposed Law.

[75] Section 30(2)(a), Proposed Law.