COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2024

Chetan Lunkar (clunkar@gmail.com) is a Counsel and Chartered Accountant based in Bangalore, India.

Deciphering India's new data protection law

By Chetan Lunkar

India's Parliament passed the Digital Personal Data Protection Act in August 2023. It is India's first comprehensive and cross-sector data privacy law. The act will be effective upon notification in the *Gazette of India*.[1] Provisions may be brought into effect on different dates, implying a phased approach toward implementation.

The act is a principles-based legislation incorporating concepts such as lawfulness, fairness, data minimization, purpose limitation, integrity, and confidentiality of personal data. It governs data fiduciaries (data controllers), data principals (data subjects), and data processors. While the act is comparable to the EU's General Data Protection Regulation (GDPR), it differs in crucial areas, such as the limited powers granted to the supervisory authority and expansive exemptions afforded to public entities. Key provisions of the act would be characterized and defined through subsequent rules to be issued by the central government, and the manner in which the act would be operationalized and enforced would determine whether the act adheres to or takes a different path from GDPR.

Key provisions of the act

Personal data

While the definition of "personal data"under the act is conceptually similar to GDPR's personally identifiable information (PII),[2] the act applies to processing of PII in digital form only—either collected in digital form or subsequently digitized.[3] However, since digitized data processing is ubiquitous, excluding nondigitized PII may be inconsequential. Processing of PII for personal or domestic purposes,[4] or where the PII is made publicly available,[5] is outside the purview of the act. Unlike the GDPR, the act applies uniformly to all types of PII, and differential provisions based on the sensitivity or categorization of PII have not been stipulated in the act.

Territorial scope

The act has extraterritorial reach as it applies to processing within India, regardless of the nationality or residency status of the data principal.[6] While this would include data principals outside India, processing in such cases if under a contract, is broadly exempted.[7] The act also applies to the processing outside India in relation to goods or services offered to data principals within India.[8] As such, the act will apply to organizations even if they operate entirely—or are domiciled—outside India.

Data principals

When juxtaposed with GDPR, data principals have fewer rights. Rights include access to information,[9] erasure,[10] and correction.[11] Notably, these rights can be exercised only if consent or voluntary disclosure is given as the grounds for processing. Uniquely, data principals have certain duties under the act, including a duty not to impersonate or suppress material information while providing PII or to raise false or frivolous grievances.[12] With respect to children (younger than 18 years old), safeguards include parental consent for processing, prohibiting processing that may impact the well-being of children, and use of techniques like tracking or monitoring, which are typically leveraged for behavioral analytics.[13] The latter restrictions would predominantly affect sectors—such as gaming or social media platforms—that rely on algorithms to position or differentiate their services.

Data fiduciaries and data processors

Unlike the GDPR, data processors have minimal statutory obligations, and obligations under the act solely rest with the data fiduciary—even in relation to acts or violations committed by the data processor. So, it's imperative for data fiduciaries to define precise terms in contracts with data processors so that contractual claims can be invoked against the data processor. Obligations for data fiduciaries include (i) maintaining safeguards to protect PII;[14] (ii) ensuring completeness, accuracy, and consistency of PII;[15] (iii) breach intimation;[16] (iv) erasure of data upon withdrawal of consent or on cessation of the purpose specified for processing;[17] (v) and instituting grievance redressal mechanisms.[18]

A data processor can only be engaged under a contract and only in connection with any activity relating to the offering of goods or services.[19] It remains to be seen whether activities that are unrelated—or indirectly ancillary or incidental—to offering goods or services can be delegated to a data processor.

Significant data fiduciaries

A data fiduciary or a class of data fiduciaries can be designated as a significant data fiduciary (SDF) based on factors (thresholds are currently unquantified and undefined) such as volume and sensitivity of PII, risks to data principals or risks to the sovereignty or security of India. Compared to other data principals, SDFs have elevated responsibilities and obligations, such as appointing a data protection officer, audits by an independent auditor, periodic audits, and data protection impact assessments.

Processing

The definition of processing is similar to the definition in GDPR and includes an entire gamut of operations ranging from collection to deletion.[20] However, as nondigital PII is outside the act's purview, the scope is restricted to automated or partly automated operations. At the same time, even manual operations may amount to processing if the manual operations are considered a subset of the more extensive set of operations. Data fiduciaries should consider this subtle nuance while designing or evaluating compliance processes.

Grounds for processing

Data fiduciaries may process PII for a lawful purpose only under two grounds:[21] consent and specific "legitimate uses."[22] The act provides for nine cases or scenarios of legitimate use, and relevant scenarios for a typical commercial organization are:

- Where the data principal has voluntarily disclosed PII for a specific purpose.[23]
- For purposes of employmentor those relating to safeguarding the employer from loss or liability, such as preventing corporate espionage and maintaining the confidentiality of information assets such as intellectual property, trade secrets, and classified information.[24]

The concept of "voluntary" disclosure of PII is singular and is bound to raise questions without sufficient contextual clarity. It also appears that the "employment" legitimate use does not give carte blanche to employers to process PII for all types of loss prevention or mitigation activities, as the scope appears to be restricted to matters relating to information assets.

The grounds used for processing would be of significance, as it appears that the rights of data principals, such as notice, access information, correction, or erasure, can be exercised if PII was processed on the grounds of consent or voluntary disclosure. Notably, the act does not provide for contractual necessity or legitimate interests as grounds for processing, making it imperative for data fiduciaries to obtain consent in almost all circumstances.

Consent and notice

Consent requirements under the act are rigid. Consent should be free, specific, informed, unconditional, and unambiguous with clear affirmative action.[25] As such, consent for unspecified purposes must be separately obtained, and grounds like bundled or implied consent may be infeasible. Consent may be withdrawn, and the ease of withdrawal of consent should be comparable with the ease with which consent was given. As such, data fiduciaries cannot institute deterrents or obstacles to discourage the withdrawal of consent.

Notice

Compared to the GDPR, the act requires less information to be laid out in the notice for consent. The notice should list the (i) PII and the purpose of processing; (ii) how consent may be withdrawn and grievances can be raised; and (iii) how complaints may be made to the Data Protection Board.[26] Furthermore, the data principal should have the option to view the notice in 23 languages—including English, a requirement that may be difficult to implement.[27]

Consent managers

Another notable feature is that the act permits a data principal to manage consent through a "consent manager" accountable to the data principal and registered with the board.[28] While details of how this would be actualized have to be articulated, the underlying framework is expected to be built upon an open-source digital stack, enabling interoperability, ease of access, and accountability.

Data protection board

The board appears to have limited dominion as a rule-making power. The power to define regulations and clarify modalities while implementing or interpreting the act has been solely vested with the central government.[29] The board can receive and investigate complaints by data principals against data fiduciaries and consent managers, levy penalties, and issue directions to remediate or mitigate data breaches. Significantly, data principals must exhaust remedies available under the grievance redressal mechanisms of the data fiduciary before approaching the board.[30]

Cross-border transfers

Transfer of PII to other countries is permitted to all countries unless specifically restricted by the central government; this approach diverges from other countries.[31] However, sector-specific regulations that provide for a higher degree of protection generally or in connection to the transfer of PII outside India would also be applicable and coexist with the act. As such, localization mandates prescribed by regulators (such as the Reserve Bank of India) for the financial sector would still be relevant.

PII breaches

Data fiduciaries are mandated to report PII breaches to the Data Protection Board and the data principal regardless of the materiality or impact, unlike the GDPR, which requires reporting based on risk thresholds.[32] This contrasting approach may lead to operational complexities in implementation and incremental costs to data fiduciaries, and the underlying benefits are unclear.

Penalties

Varying penalties (up to INR 2.5 billion/USD 30 million) for PII breaches and other noncompliance with the act may be levied by the board, and factors such as materiality, duration, and nature of the violations and mitigation measures are to be considered by the board while determining the penalty.[33] Notably, affected data principals are not eligible for compensation.

Exemptions

The act provides exemptions from substantially all provisions of the act for processing for the prevention, detection, investigation, or prosecution of offenses, among other processing purposes.[34] From the context of a private organization, almost all types of misconduct may be interpreted to constitute offenses under the law, and this exemption may be leveraged to justify superfluous and extensive processing. This approach would diverge from the act's spirit. An alternate view is that this exemption would be limited to offenses where a specific duty or obligation has been cast upon a data fiduciary under law, thereby limiting the usage of this exemption. It is anticipated that subsequent directions or rules from the central government will clarify the nuances of this exemption. The central government can also exempt—based on the volume and nature of PII processed—data fiduciaries from certain obligations such as notice requirements or erasure of PII, and it is anticipated that start-ups and small businesses would fall under this exemption.

Notified government entities are completely exempted if the processing is connected with security and public order. This exemption has been critiqued to an extent as it places such government entities on a different pedestal altogether; in the absence of checks and balances, privacy rights may be diminished. The act will also not apply for processing in connection with research, archiving, or statistical purposes if the PII is not used to make any decision specific to a data principal. Notably, this exemption will permit the training of AI models on personal data.