Internet Law & Cybersecurity (Https://Businesslawtoday.Org/Practice-Area/Internet-Law-Cyber-Security/); International Business Law (Https://Businesslawtoday.Org/Practice-Area/International-Business-Law/)

Global Businesses Should Brace Themselves for India's New Personal Data Protection Law

14 Min Read

By: Aaron Kamath (/author/aaron-kamath/), Palak Kapoor (/author/palak-kapoor/) | Today

India's first standalone data protection legislation, the *Digital Personal Data Protection Act, 2023* ("DPDPA"),[1] is poised to soon come into force. To facilitate its implementation, the Ministry of Electronics and Information Technology recently issued draft *Digital Personal Data Protection Rules, 2025* ("Draft Rules")[2], which provide guidance on implementation of several key provisions of the DPDPA. The Draft Rules were issued for public consultation till March 5, 2025. After consideration of industry feedback, it is expected that the government may notify the Draft Rules in the coming months, bringing the DPDPA formally into force.

Because of the DPDPA's extraterritorial reach, businesses around the world need to prepare for its significant impact. Among the critical aspects of the new data protection law are provisions on cross-border data transfers and data localization, requirements for processing of children's data, personal data breach notification obligations, and heightened obligations for "significant" data fiduciaries. At a macro level, global businesses will need to assess the DPDPA's applicability to them and update their technological infrastructure and documentation to comply with the new requirements. "Consent managers," a new category of entity introduced by the law, may need to be onboarded and integrated to manage data subjects' consents, and data privacy notices will need to be revisited to ensure they provide the DPDPA's requisite disclosures. At a business level, data sharing arrangements with vendors and group companies will also need to be reconsidered in light of the DPDPA.

OVERVIEW AND EXTRATERRITORIAL APPLICATION

The DPDPA introduces several compliance requirements for collection and processing of personal data, whether collected in digital form or collected and subsequently digitized.[3] "Personal data" broadly includes "any data about an individual who is identifiable by or in relation to such data."[4] The provisions of the DPDPA do not apply to personal data processed by an individual for "any personal or domestic purpose," or to personal data that is made or caused to be made publicly available by (a) the "Data Principal" (akin to "data subjects" under other jurisdictional frameworks) to whom such personal data relates, or (b) any other person who is under a legal obligation to make personal data publicly available.[5]

The DPDPA applies not only to entities processing personal data within India but also to those outside India if such processing is in connection with any activity related to offering of goods or services to individuals (i.e., Data Principals) within India.[6] This provision is comparable to global frameworks like the European Union's *General Data Protection Regulation* ("EU GDPR"), which applies extraterritorially to non-EU businesses that offer goods or services to, or monitor the behavior of, individuals located in the EU.[7] International businesses that do not have a physical presence in India but target and serve Indian consumers, such as e-commerce websites and digital platforms, will need to comply with the DPDPA.

CONSENT AND NOTICE REQUIREMENTS

One of the core principles of the DPDPA is obtaining consent from Data Principals for processing their personal data. "Data Fiduciaries" (akin to "data controllers" under other jurisdictional frameworks) must provide clear, standalone notices in English or any official Indian language,[8] detailing the purpose of data collection, the types of data processed, and the rights of Data Principals.[9] The Draft Rules do not prescribe a rigid template or format for the notice, allowing flexibility for Data Fiduciaries to design their notices so long as other requirements are satisfied. However, the notice cannot be combined with other documentation such as an end-user license agreement, general terms of service, or other website policies.[10]

Under the DPDPA, Data Fiduciaries are required to provide similar notice to Data Principals, as soon as "reasonably practicable," regarding data for which consent for processing was obtained prior to the enforcement of the Act.[11] However, the Draft Rules do not specifically prescribe separate notice requirements for these existing datasets. In the absence of detailed guidance, it may be sufficient, in certain cases, for a public notice to be issued on the Data Fiduciary's websites or apps.

An operational aspect of concern for these notices is the language requirement. It would simplify implementation if the government were to allow notices to be accessible in the language in which the platform is supported or made available to the Data Principals, to prevent unnecessarily onerous translation requirements.

CONSENT MANAGERS

Unlike the EU GDPR, which permits data processing on some relatively broad bases such as legitimate interest, the DPDPA relies primarily on consent-based processing, with limited instances of legitimate uses such as for employment.[12] This approach imposes a greater burden on organizations to ensure

user-friendly and transparent consent mechanisms. Against this background, it is relevant to note that the DPDPA introduces the novel concept of "Consent Managers."[13] These are entities registered with the Data Protection Board of India[14] that provide Data Principals a platform to manage, review, and withdraw their consent.[15] These Consent Managers must maintain robust technical and organizational safeguards to ensure transparency and data security.[16]

While the introduction of Consent Managers may alleviate compliance burdens for Data Fiduciaries, it also creates a potential bottleneck if the regulatory framework for their operation is not adequately developed. Furthermore, it would be useful to clarify whether Consent Managers, which operate as independent entities and businesses from Data Fiduciaries, should themselves be considered Data Fiduciaries, or even Significant Data Fiduciaries.

SIGNIFICANT DATA FIDUCIARIES

The DPDPA introduces the concept of "Significant Data Fiduciaries," a subset of Data Fiduciaries that will be designated by the central government based on an assessment of "such relevant factors as it may determine," such as the volume and sensitivity of the data they process.[17] SDFs are subject to enhanced compliance obligations, including mandatory data protection impact assessments, audits, and appointment of a dedicated Data Protection Officer[18] to oversee compliance. SDFs may also be required to implement additional security measures, maintain detailed processing records, and observe strict data governance protocols. Furthermore, they may be restricted from transferring certain categories of personal data outside India (discussed below).[19] Businesses operating as SDFs must proactively assess their data processing activities and prepare to meet these heightened regulatory requirements. It is likely that big tech and large, consumer-facing health care, finance, and IT companies could potentially be notified as SDFs, though the exact criteria that the government may use to notify Data Fiduciaries as SDFs is not clear.

CROSS-BORDER DATA TRANSFERS

One of the major concerns under the DPDPA and the Draft Rules for multinational businesses is the regulation of cross-border data flows. The DPDPA permits the transfer of personal data outside India unless the government specifically restricts certain jurisdictions.[20] Unlike some stringent data localization laws, the DPDPA does not impose blanket prohibitions but retains the authority to designate restricted territories.

This regulatory approach offers some flexibility for businesses engaged in global data processing while ensuring that transfers remain subject to oversight. However, the government may prescribe additional compliance measures for transfers to certain jurisdictions,[21] such as requiring contractual clauses, data protection impact assessments, or approvals from regulatory authorities. The government may also impose additional compliance requirements on notified SDFs depending on the nature of personal data processed by the SDF and the recipient jurisdiction.[22] Organizations transferring data outside India should be prepared for these potential requirements and must stay updated on government notifications regarding restricted countries and additional conditions applicable to data transfers.

A key question is whether these restrictions will align with existing global frameworks and compliance with foreign law obligations. Companies operating across multiple jurisdictions may face conflicting compliance obligations depending on specific restrictions that may be introduced under the DPDPA. This could create operational challenges for global data-sharing frameworks, necessitating the adoption of a modular approach to data governance, which enables jurisdiction-specific adjustments while maintaining overall regulatory consistency.

DATA LOCALIZATION REQUIREMENTS

While the DPDPA generally allows data transfers, the Draft Rules introduce provisions for potential data localization requirements, particularly for SDFs. These entities may be subject to specific data storage and localization mandates.[23] A government-appointed committee will determine categories of personal data processed by SDFs that must be stored within India.[24] This could impact global enterprises, particularly those in sectors like finance, health care, and technology, where handling sensitive personal data (often across borders) is integral to operations. Apart from personal data, localization requirements may extend to traffic data pertaining to the flow of personal data,[25] which can include logs and transactional records, meaning businesses must implement robust infrastructure to ensure compliance. Companies must assess whether they are likely to fall within the SDF category and prepare for potential localization obligations by revising their data storage strategies.

These regulations could impact multinational companies that rely on global data centers and cloud services for their business operations. For companies that use global analytics and services driven by artificial intelligence, data localization can introduce significant inefficiencies. Localization mandates may result in increased costs for infrastructure deployment and operational inefficiencies due to the inability to process data across borders. Additionally, concerns have been raised regarding whether localization measures genuinely enhance data security or merely create operational and economic hurdles.

PERSONAL DATA BREACH REPORTING OBLIGATIONS

Under the DPDPA, organizations must promptly report personal data breaches.[26] The law requires that both affected individuals and the Data Protection Board of India be informed without delay upon discovering a breach.[27] Additionally, within seventy-two hours of an organization's becoming aware of the breach, a detailed report of the breach must be submitted to the Data Protection Board.[28]

This requirement aligns with international best practices, such as the EU GDPR, but lacks a materiality threshold. Every breach, regardless of its impact, must be reported. This could lead to an increased compliance burden for businesses, necessitating highly robust cybersecurity frameworks and breach detection mechanisms. The lack of a materiality threshold also raises concerns about regulatory fatigue. If organizations are required to report even minor breaches, regulators may be overwhelmed with notifications, reducing their ability to focus on critical threats. Businesses may also face reputational risks from excessive breach disclosures to multiple stakeholders, even in cases where no harm occurs.

In any case, organizations must establish internal protocols for incident detection, assessment, and reporting. Given that breach notifications may also be required under other laws, such as general[29] and sector-specific cybersecurity regulations (such as in the banking or the insurance sector), companies should harmonize their reporting obligations to avoid duplication and ensure efficiency.

ADDITIONAL CONSIDERATIONS

Data Security: Subject to a few minimal restrictions, Data Fiduciaries are allowed to implement the security standards and procedures of their choice to protect the personal data they process.[30] These safeguards are required to include making sure that the right data security measures (such as encryption, obfuscation, or mapping personal data to tokens) are implemented; access control mechanisms are in place; logs are maintained and routine monitoring is conducted to identify instances of unauthorized access; and more.[31]

Children and Persons with Disabilities: In relation to processing of personal data of children and persons with disabilities, there are additional requirements for obtaining verifiable consent from the parent or legal guardian if applicable, respectively.[32] The mode of seeking verifiable consent is left to the discretion of the Data Fiduciary.[33] Neither the DPDPA nor the Draft Rules require the Data Fiduciary to investigate the ages of its users to ascertain if they are in fact not children, or to investigate the relationship between child and purported parent. The DPDPA and Draft Rules appear to rely upon self-identification by a user as a child, or by a parent, for compliances to trigger.

Retention: According to the DPDPA, personal data must be deleted as soon as it is reasonable to believe that the specified purpose for processing the personal data is no longer being fulfilled.[34] The Draft Rules specify time frames for the processing of personal data for particular purposes by e-commerce entities, online gaming intermediaries, and social media intermediaries (that meet the prescribed user thresholds).[35] It lays out a three-year term from the enforcement of the Digital Personal Data Protection Rules, 2025, or the last time the Data Principal approached the Data Fiduciary to execute the specified purpose or exercise their rights, whichever is later.[36] There is no guidance on the manner of ascertaining when the specified purpose is no longer being served for other Data Fiduciaries. In the absence of a specific timeline, Data Fiduciaries will have varying standards to determine erasure of personal data. Further, it is unclear why a timeline has only been prescribed for the said three classes, as opposed to other Data Fiduciaries, such as those in possession of large volumes of personal data.

CONCLUSION

Feedback and comments from the industry submitted during the public consultation period are presumably under consideration by the Indian government. Based on recent media reports, it was expected that the DPDPA and the Draft Rules would be finalized for implementation by April 2025.[37] However, as of mid-May 2025, neither the DPDPA nor the Draft Rules have been brought into effect. As the rules are finalized, businesses must assess their current data protection practices based on their industry and the type of personal data they handle. Principles of purpose limitation, collection limitation, and storage limitation are enforced through the DPDPA and Draft Rules and should be enforced by businesses. Compliance will require updating technological systems, internal processes, and documentation. SDFs engaged in cross-border data sharing may face localization challenges,

necessitating adjustments to their data transfer arrangements. A critical consideration for businesses is the significant penalties prescribed under the DPDPA, which start at approximately USD 6 million and go up to approximately USD 30 million, depending on the nature of violation.While the Draft Rules offer flexibility by avoiding rigid standards, several critical aspects, such as SDF designations, data transfer restrictions, and details for obtaining verifiable consent for children's personal data, remain undefined. These details are likely to be addressed once the final rules are released or subsequently through government-issued FAQs.

---

1. Digital Personal Data Protection Act, 2023 (https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf) [hereinafter DPDPA]. ↑

2. Ministry of Electronics and Information Technology, Draft Digital Personal Data Protection Rules, 2025 (https://static.mygov.in/innovateindia/2025/01/03/mygov-999999999568142946.pdf), G.S.R. 02(E) (Issued on January 3, 2025) [hereinafter Draft Rules]. ↑

3. DPDPA § 3(a). ↑

4. DPDPA § 2(t). ↑

5. DPDPA § 3(c). ↑

6. DPDPA § 3(a)–(b). ↑

7. Article 3(2), Regulation (EU) 2016/679 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter EU GDPR]. ↑

8. DPDPA §§ 5(3), 6(3); Please note that there are twenty-two languages recognized as official under the Eighth Schedule to the Constitution of India*:* Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Maithili, Malayalam, Manipuri, Marathi, Nepali, Oriya, Punjabi, Sanskrit, Santhali, Sindhi, Tamil, Telugu, and Urdu. ↑

9. DPDPA § 5(1); Draft Rules, Rule 3; *see also* Explanatory Note to Digital Personal Data Protection Rules, 2025 (https://static.mygov.in/innovateindia/2025/01/03/mygov-999999991926765870.pdf), ¶ 3 (last visited Apr. 26, 2025). ↑

10. Draft Rules, Rule 3(a). ↑

11. DPDPA § 5(2). ↑

12. DPDPA § 7. ↑

13. DPDPA § 2(g) ("'Consent Manager' means a person registered with the [Data Protection] Board [of India], who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform."). ↑

14. DPDPA § 6(9). ↑

15. DPDPA § 6(7)–(8). ↑

16. The Draft Rules prescribe the conditions for registration of a Consent Manager under Part A of the First Schedule and enumerate the obligations applicable to the Consent Manager under Part B of the same Schedule. ↑

17. DPDPA § 10(1) ("The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including—(a) the volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order."). ↑

18. DPDPA § 10(2). ↑

19. Rule 12(4), Draft Rules. ↑

20. DPDPA § 16(1). ↑

21. Rule 14, Draft Rules. ↑

22. Rule 12(4), Draft Rules. ↑

23. DPDPA § 10(2)(c)(iii); Rule 12(4), Draft Rules. ↑

24. Rule 12(4), Draft Rules. ↑

25. Rule 12(4), Draft Rules. ↑

26. DPDPA § 2(u) ("'[P]ersonal data breach' means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data"). ↑

27. DPDPA § 8(6); Rule 7, Draft Rules. ↑

28. Rule 7(2)(b), Draft Rules. ↑

29. In particular, this refers to the obligation to report cyber-security incidents to the Indian Computer Emergency Response Team in accordance with the provisions of the Information Technology Act, 2000. ↑

30. DPDPA § 8(5). ↑

31. Rule 6, Draft Rules. ↑

32. DPDPA § 9(1). ↑

33. Rule 10, Draft Rules. ↑

34. DPDPA § 8(7)– 8(8). ↑

35. DPDPA § 8(8); Rule 8 and Third Schedule, Draft Rules. ↑

36. Third Schedule, Draft Rules. ↑

37. Surabhi Agarwal & Suraksha P, *Centre Sets April Date for DPDP Rules as MeitY Studies Feedback* (https://economictimes.indiatimes.com/tech/technology/meity-aims-to-notify-data-protection-rules-in-april-industry-bodies-raise-concerns-over-data-localisation-verifiable-parental-consent/articleshow/119432689.cms), Econ. Times (Mar. 25, 2025). ↑

By: Aaron Kamath (/author/aaron-kamath/), Palak Kapoor (/author/palak-kapoor/) | Today