January 2025

Ministry of Electronics and Information Technology releases draft Digital Personal Data Protection Rules, 2025

On January 3, 2025, the Ministry of Electronics and Information Technology issued a draft of the Digital Personal Data Protection Rules, 2025 ("**Draft Rules**") for public consultation, with public feedback submissions due by February 18, 2025. The Draft Rules provide clarifications on the implementation of the Digital Personal Data Protection Act, 2023 ("**DPDPA**"). Most notably, the Data Protection Board of India ("**DPB**"), which is the oversight agency under the DPDPA, will be constituted after the final rules are notified, following the conclusion of public consultation. Other provisions of the DPDPA will come into effect at a later stage, on such dates that will be specified in the final rules.

Key takeaways

1. **Detailed notice**: Data fiduciaries have an obligation to publish a notice, providing a detailed account of the information necessary to enable data principals to provide an informed consent to the processing of their personal data. Some notable notice requirements introduced in the Draft Rules are:
   a) the notice must be 'understandable independently' of any other information provided by the data fiduciary;
   b) the notice must contain a full and transparent account containing all information necessary to enable the data principal to provide specific and informed consent;
   c) the notice must mandatorily include the following details:
      i) an itemised description of the personal data;
      ii) the specified purposes of processing, with an itemised description of the goods/services to be provided or the functions to be enabled by such processing;
      iii) a communication link to access the data fiduciary's app, website or both; and
      iv) a description of other means through which the data principal can withdraw his/her consent, exercise his/her rights under the DPDPA and make a complaint to the DPB. Notably, the Draft Rules reiterate that the ease of withdrawal of consent must be comparable to that with which consent was first given.
2. **Consent managers**:
   a) the Draft Rules prescribe detailed requirements for registration of a consent manager with the DPB, and obligations applicable to a registered consent manager. One of the key requirements applicable to a consent manager is an obligation to ensure that there is no conflict of interest (directly or indirectly) with any of the data fiduciaries onboarded by it;

b) consent managers must be an Indian incorporated company, which means that foreign companies cannot register themselves as consent managers in India. There is also a minimum net worth requirement of INR 2,00,00,000 (Indian Rupees two crore) (approx. USD 250,000 (US Dollars two hundred and fifty thousand)); and

c) some notable obligations of consent manager include:

i) maintaining an interoperable platform on a website, app or both, for data principals to provide their consent directly to the data fiduciary or through a data fiduciary onboarded onto such platform, who maintains such personal data with the consent of the data principal;

ii) ensuring personal data shared by the data principal is not readable by the consent manager;

iii) adopting reasonable security measures to prevent data breach;

iv) avoiding conflict of interest with data fiduciaries (directly and through its promoters, key managerial personnel, senior management), and making required disclosures on its platforms to confirm that there is no conflict of interest; and

v) adopting audit mechanisms to ensure compliance with its obligations.

3. **Standards for processing by State for legitimate use under Section 7 (b) of the DPDPA**: The Draft Rules prescribe standards for the State and its instrumentalities to process personal data under the legitimate use exemption set out in Section 7 (b) of the DPDPA[1]. These standards are detailed in the Second Schedule of the Draft Rules. The standards encapsulate key privacy principles such as lawfulness, purpose limitation, ensuring accuracy of the personal data and accountability.

4. **Reasonable security safeguards**: The Draft Rules specify the reasonable security safeguards that a data fiduciary must implement, such as ensuring encryption/masking to secure data, control access to the computer resources used by the data fiduciary or its data processor(s), maintenance of logs, detection of unauthorised access and ensuring continuity by storing data backups. Notably, no certification or standards such as ISO 27001 have been prescribed. Interestingly, the security safeguards as specified in the Draft Rules remain 'baseline' in nature, meaning that data fiduciaries may have to implement additional appropriate security safeguards based on the nature and volume of personal data processed by them.

5. **Retention period**: The DPDPA requires data fiduciaries to erase personal data when it is reasonable to assume that the 'specified purpose' for which the data was being processed is no longer being served. For certain categories of data fiduciaries (listed below), the maximum retention period is 3 (three) years from data principal's last request to the data fiduciary. These categories are:

a) e-commerce entities having not less than 2,00,00,000 (two crores) (20,000,000 (twenty million)) registered users in India;

b) online gaming intermediaries having not less than 50,00,000 (fifty lakh) (5,000,000 (five million)) registered users in India; and

c) social media intermediaries having not less than 2,00,00,000 (two crores) (20,000,000 (twenty million)) registered users in India.

[1] According to Section 7(b) of the DPDPA, the State or any of its instrumentalities may process personal data of data principals, without seeking express consent of the data principal, to provide or issue to the data principal a subsidy, benefit, service, certificate, licence, or permit, provided that: (a) the data principal has previously consented to the processing of her personal data for such purposes, or (b) the personal data is available in digital form, or in non-digital form and subsequently digitised, from any database, register, book, or document maintained by the State.

Data fiduciaries must inform the data principal at least 48 (forty-eight) hours before deleting their personal data, unless the data principal (i) logs into her user account; or (ii) otherwise contacts the data fiduciary for performance of the specified purpose, or (ii) exercises her rights in relation to the processing of her personal data.

6. **Breach reporting**: The Draft Rules specify the manner in which a data fiduciary must report a personal data breach to affected data principals and the DPB. An initial report with certain specific details needs to be provided by the data fiduciary to the affected data principals and the DPB 'without delay', upon becoming aware of the breach. Thereafter, a detailed report must be shared with the DPB within 72 (seventy-two) hours; however, the Draft Rules allow data fiduciaries to apply to the DPB for an extension to submit this detailed report.

7. **Verifiable parental consent:** The Draft Rules clarify that if a user is a minor, the data fiduciary must obtain the consent of the parent and verify that such parent is an identifiable adult. The data fiduciary may rely on the parent's details already available in its records (if any) or use Identification ("**ID**") proof and age proof voluntarily provided by the parent, or use a virtual token issued by a government agency that is mapped to the ID and age proof. However, there are no prescribed mechanisms for a data fiduciary to establish the relationship between the child and the parent. It is unclear whether a data fiduciary will need to establish such a relationship before processing data. At present, confirmation of the parent's age and identity will likely qualify as 'verifiable consent' under Draft Rules. For a person with a disability, 'verifiable consent' of his/her lawful guardian may be obtained by verifying if the individual identifying themselves as a lawful guardian has been appointed by a court, designated authority or 'local level committee' under applicable laws. This may be challenging as data fiduciaries may be unable to accurately verify the authenticity of such documents.

8. **Additional obligations of Significant Data Fiduciaries:** The following obligations are specifically applicable to data fiduciaries that have been notified as Significant Data Fiduciaries ("**SDF**")[2] by the Central Government:

   a) Appointment of Data Protection Officer ("**DPO**"): SDFs are required to appoint a DPO based in India, who will be accountable to the governing body of the SDF, serve as a point of contact for grievance redressal, and represent the SDF under the DPDPA.

   b) Appointment of Independent Data Auditor ("**IDA**"): SDFs must appoint an IDA to conduct annual audits and take additional compliance measures to evaluate their compliance with the DPDPA:

      i) Data Protection Impact Assessment ("**DPIA**"): SDFs are required to perform annual DPIAs, which assess data principals' rights, processing purposes, and risk mitigation strategies;

      ii) Periodic audits: The SDF must conduct audits as prescribed by the Central Government and report the results, including compliance with data protection requirements, to the DPB.

   c) Due diligence on algorithmic software: The Draft Rules mandate SDFs to verify that their algorithmic software (used in managing personal data) does not compromise the rights of data principals.

   d) Compliance with data processing restrictions: If the Central Government imposes restrictions on offshore processing of personal data, including data localisation or related traffic, SDFs must comply with these requirements. Clearly, the Draft Rules empower the Government to restrict an SDF from transferring certain personal data and "traffic data pertaining to its flow" (a term that has not been defined) to territories outside India.

9. **Mandatory disclosures on website/app:** Each data fiduciary (and consent manager) must mandatorily publish on its website: (a) business contact information of its DPO or contact person; (b) grievance redressal details and manner in which a data principal may exercise her rights; and (c) information regarding the username or any other identifier of the data principal that may be utilised to recognise her under the terms of service.

[2] The Central Government will notify a data fiduciary or a class of data fiduciaries as SDF on the basis of an assessment of certain relevant factors like (i) the volume and sensitivity of personal data processed, (ii) risk to the rights of 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.

10. **Data transfers:** In addition to the ability to notify 'blacklisted' territories to which personal data cannot be transferred, Indian Government is empowered to pass orders to restrict data fiduciaries from transferring any personal data governed by the DPDPA and the Draft Rules to foreign governments or quasi-governmental authorities. Such transfer restrictions may be imposed on personal data processed (a) within India; or (b) outside India in relation to goods/services offered to data principals in India. This means that even if personal data is processed entirely outside India, the Indian Government can regulate or restrict the transfer of such data if it falls within the scope of the DPDPA and Draft Rules.
11. **Clarification on research exemption:** The Draft Rules prescribe standards for processing personal data where it is necessary for 'research, archiving or statistical purposes'. Processing for such purposes is exempted from the requirements under the DPDPA and Draft Rules. The prescribed standards include data minimisation, limitation of processing to the specified purpose, reasonable time period for retention, implementing reasonable security measures, among others.
12. **Government's ability to call for information:** The Draft Rules empower the Central Government, through designated/authorised personnel, to require data fiduciaries to furnish personal data of data principals in the interest of national security, sovereignty, or security. Interestingly, the Draft Rules also restrict the disclosure of such personal data, upon consent of authorised personnel, where such disclosure could jeopardise India's sovereignty, integrity, or security.

Conclusion

Once the Draft Rules are published in final form, it will facilitate the effective implementation of India's new data protection regime. The public consultation window is an important opportunity for stakeholders to provide input, helping to identify and address any potential issues prior to the full enactment of the law.

Infotech Practice

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Probir Roy Chowdhury
Partner

Yajas Setlur
Partner

Shivani Bhatnagar
Senior Associate

Pranavi Pera
Senior Associate

Chambers TOP RANKED Asia-Pacific 2025 JSA

18 Practices and
41 Ranked Lawyers

Chambers TOP RANKED Global 2024

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice

---

3 Band 1 Practices

---

4 Band 1 Lawyers,1 Eminent Practitioner

IFLR1000 TOP TIER FIRM 2024

12 Practices and
50 Ranked Lawyers

The LEGAL 500

14 Practices and
38 Ranked Lawyers

asialaw OUTSTANDING FIRM 2024

20 Practices and
22 Ranked Lawyers

The LEGAL 500

Ranked Among Top 5 Law Firms in India for ESG Practice

GCR 100 2025 The guide to the world's leading competition practices

Recognised in World's 100 best competition practices of 2025

Among Top 7 Best Overall Law Firms in India and 11 Ranked Practices

---

11 winning Deals in IBLJ Deals of the Year

---

11 A List Lawyers in IBLJ A-List - 2024

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services Law Firm of the Year 2022

Ranked #1
The Vahura Best Law Firms to Work Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and 3 Ranked Lawyers

For more details, please contact km@jsalaw.com

www.jsalaw.com

advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi