jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection

Digital Personal Data Protection Act

Edition 14

February 2025

Beyond global compliance: Navigating additional obligations under the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("**DPDPA**"), along with the Draft Digital Personal Data Protection Rules, 2025[1] ("**Draft Rules**"), introduce certain compliance requirements that are different from other global data protection laws. Although entities located outside India, may already be compliant with their geography's laws, they will now have to go a step further to ensure alignment with the DPDPA's specific obligations, particularly around consent, cross-border data transfers, grievance redressal, and accountability. In this edition of the Prism, we explore key compliance requirements to be taken into consideration by these entities.

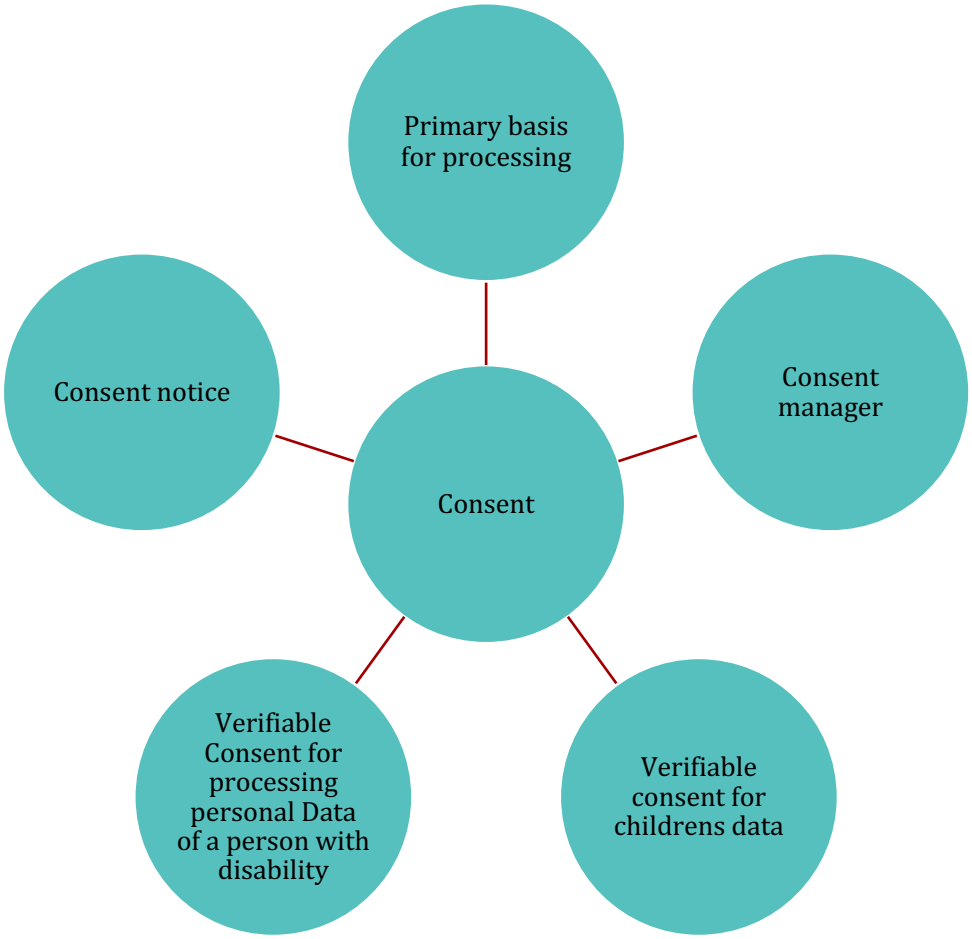
Applicability

The DPDPA applies to entities outside India when they process data in India or when they process data of residents in India in connection with offering goods or services. This means that entities, that handle the digital personal data of Indian data principals must comply with DPDPA requirements.

[1] The draft rules are open for public consideration until February 18, 2025.

Key considerations for entities operating outside India

Consent



1. **Consent as the primary basis of processing personal data**:

   The primary basis for processing personal data under the DPDPA is consent. This is different from other global data protection laws like the General Data Protection Regulation ("**GDPR**"), under which consent is one of the bases for processing personal data and there are several other grounds for processing personal data like the performance of a contract, legitimate interests, etc, or the California Consumer Privacy Act ("**CCPA**") which primarily relies on an opt-out model rather than requiring explicit consent for most data processing activities.

   Entities that rely on any ground for processing personal data other than consent, under the other data protection laws, may now need to revisit their grounds for processing personal data to be compliant with their obligations under the DPDPA. These entities need to rely on consent for processing personal data unless their processing activity falls under any of the legitimate uses specified under the DPDPA such as voluntary submission of personal data or processing for government benefits, medical emergencies, processing for State functions, legal compliance, or for core employment functions.

2. **Privacy notice to be published in english and the languages listed in the Eighth Schedule of the Indian Constitution**:

   When processing is based on consent, the data fiduciaries including such entities operating outside India, are required to provide a privacy notice that is independent, clear, and in plain language with an itemised description of the personal data processed for an itemised purpose and description of goods/services. Under the DPDPA the data fiduciaries are required to publish the privacy notice not only in English but also in the languages listed in the Eighth Schedule of the Indian Constitution. This might mean developing localised, legally compliant notices in multiple Indian languages, which requires additional resources and legal vetting for linguistic accuracy.

3. **Verifiable consent for processing personal Data of children**:

   DPDPA mandates that the data fiduciaries ensure verifiable parental consent before processing any children's data. Unlike the CCPA or the U.S. Children's Online Privacy Protection Act ("**COPPA**"), which imposes parental consent for children aged between 13 (thirteen) and 16 (sixteen), the requirement of verifiable parental consent under the DPDPA applies to all children under the age of 18 (eighteen). The draft Rules also prescribe the means to obtain verifiable consent of the parents. The requirement of verifiable consent under the DPDPA is similar to the requirement under COPPA, however, the requirement under COPPA applies to only such entities providing services directed at children. The DPDPA adds an additional layer of complexity, even for entities providing services that are not directed at children, as they must still adhere to these requirements when handling any children's data.

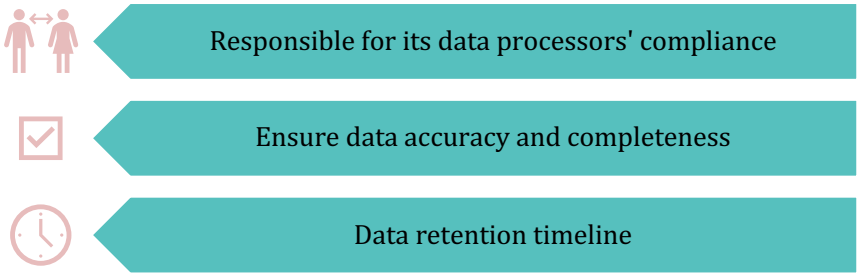
4. **Verifiable consent for processing personal data of a person with disability**:

   The DPDPA has extended the requirement of verifiable consent to processing personal data of a person with a disability as well. The data fiduciary would need verifiable consent from a lawful guardian before processing personal data of a person with disability. The Draft Rules require the data fiduciary to also verify that such guardian is duly appointed under applicable laws. This would mean the data fiduciaries may need to have separate consent workflow mechanisms while processing the personal data of a person with disability.

5. **Consent managers**:

   The concept of consent managers is very new in the global data protection regime. The option of providing, managing, and withdrawing consent via a third party is a novel concept provided for in the DPDPA. The DPDPA provides the option for the data principals to give, manage, and review their consent through a consent manager. The consent manager is an unrelated third party with an interoperable platform, that helps to manage the consent flow between the data principal and the data fiduciary. Even entities operating outside India could explore the possibility of integrating with consent managers while processing such data principals' data who have decided to manage their consent through consent managers.

Data fiduciary obligations



1. **No separate data processor obligation; data fiduciary to be solely responsible for its data processors' compliance**:

   Unlike GDPR or Health Insurance Portability and Accountability Act (HIPAA) which places independent legal obligations on the processors or business associates respectively, the DPDPA does not impose any obligation directly on the data processors. This imposes additional obligations on the data fiduciaries to flow down all the required obligations contractually to the data processors to ensure data processors' compliance with the DPDPA. The DPDPA also requires the data fiduciaries to implement reasonable security safeguards to protect the personal data both in its possession or under its control, including the personal data processed by a data processor. To ensure this it is important that data fiduciaries undertake extensive due diligence on the data processors including

diligence on the security safeguards implemented by these processors before engaging them, negotiate appropriate contracts and audit their vendors periodically.

2. **Ensure data accuracy and completeness**:

Additionally, the DPDPA mandates that data fiduciaries ensure data accuracy and completeness before making decisions affecting individuals or sharing data with other fiduciaries.

3. **Data Retention**:

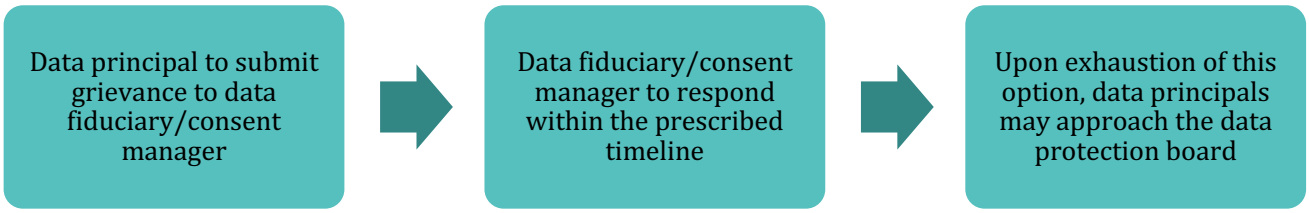
The Draft Rules have prescribed a definitive data retention period for certain classes of data fiduciaries, such as e-commerce entities, online gaming intermediaries, and social media platforms. This is not the case under other global data protection laws. GDPR or CCPA does not prescribe a specific retention period but rather mandates the entities to only retain the personal data as long as it is necessary for the collected purpose. The entities that fall under any of the classes of data fiduciaries specified under the Third Schedule of the Draft Rules, may now be required to re-evaluate their existing data retention policies to align with the requirements under the DPDPA.

Data principal rights

1. **Right to nominate**:

Most of the rights that data principals have under the DPDPA align with other global laws like the GDPR. Additionally, the DPDPA provides the data principals with the right to nominate, which is not present under the GDPR or the CCPA. This right enables the data principals to designate one or more individuals to exercise their data principal rights on their behalf in the event of their death or incapacity. The data fiduciaries including those entities that comply with GDPR or CCPA may need to update their technical and organisational measures to accommodate this nomination process, ensuring both the data principal and their nominee can be properly identified, and the right is exercised appropriately.

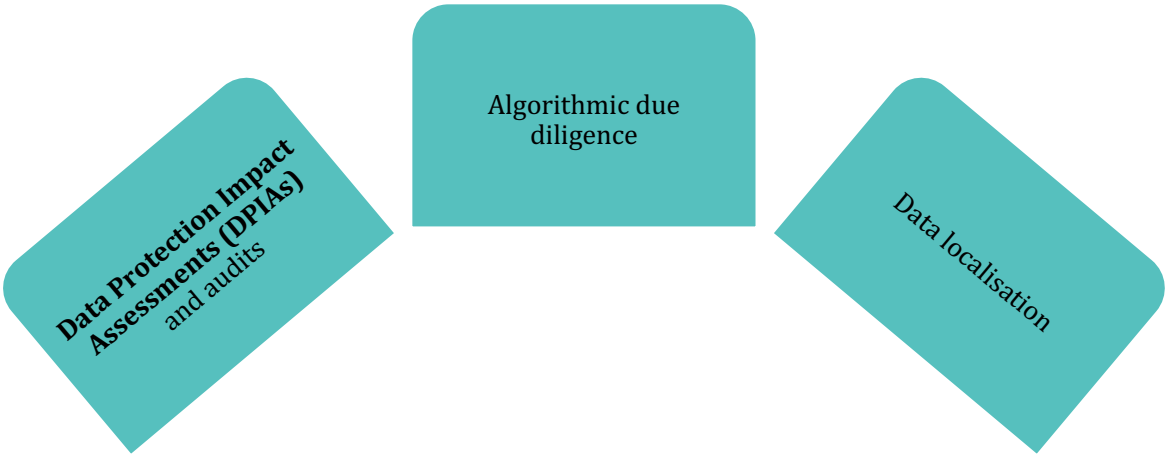
2. **Grievance redressal**:



The DPDPA mandates the data fiduciaries and consent managers to provide the data principals with the right to grievance redressal to address any act or omission of such data fiduciary or consent manager. While GDPR requires the entities to be transparent about how data principals can make requests exercise their rights and have processes in place to address data subject requests efficiently, the right to grievance redressal is not an explicit right under GDPR. CCPA is also similar to GDPR in this regard. The data fiduciaries to be compliant with DPDPA in addition to having processes to enable the data principals to exercise their rights like the right to access or erasure, now need to implement grievance redressal mechanisms.

New categories of data fiduciaries: Significant Data Fiduciaries

The DPDPA has introduced a new class of data fiduciaries i.e., the Significant Data Fiduciaries ("**SDFs**"). An entity might be classified as an SDF based on the volume and sensitivity of personal data processed, risk to the rights of the data principals, etc. While the GDPR and CCPA impose additional obligations based on the sensitivity of the data processed by an entity, the DPDPA categorises entities themselves into different classes. The DPDPA and the Draft Rules impose these additional obligations on the SDF:



1. **Data Protection Impact Assessments ("DPIAs") and audits**:

   The DPDPA mandates that SDFs conduct DPIAs and independent data audits annually. These reports must be submitted to the Data Protection Board of India ("**Board**"). While the GDPR mandates periodic DPIAs only when processing activities pose a high risk to the data subjects, the DPDPA requires all SDFs to conduct a DPIA annually. The independent data audit is mandated in addition to DPIAs, which differs from other laws like the GDPR or CCPA. For entities who are compliant with other global data protection laws, complying with DPDPA may mean additional compliance requirements.

2. **Algorithmic due diligence**:

   Under the draft Rules, SDFs must do due diligence to ensure that any algorithmic software used for data processing does not pose risks to data principals' rights. GDPR includes protections against automated decision-making, allowing individuals to opt out of decisions made solely by automated processing. However, GDPR does not mandate proactive due diligence of all algorithmic models before deployment, which the DPDPA requires. CCPA, while focused on data privacy, does not impose direct obligations on artificial intelligence or automated decision-making. This due diligence requirement under the DPDPA may involve additional compliance checks, periodic internal reviews, and implementation of transparency mechanisms for the SDFs using algorithmic software.

3. **Data localisation**:

   The Draft Rules give the power to the Central Government to mandate personal data processed by SDFs to be processed and stored exclusively in India. This provision differs from GDPR, which does not mandate data localisation for any category of data and permits cross-border transfer to a country recognised by the adequacy decision or to a third country if adequate additional safeguards are in place. Similarly, while CCPA imposes restrictions on data sharing and data selling, does not require data localisation. SDFs that might process those categories of data identified by the Central Government, may need to explore the possibilities of having local data centres in India or restructuring data flows to comply with the new restrictions under the DPDPA.

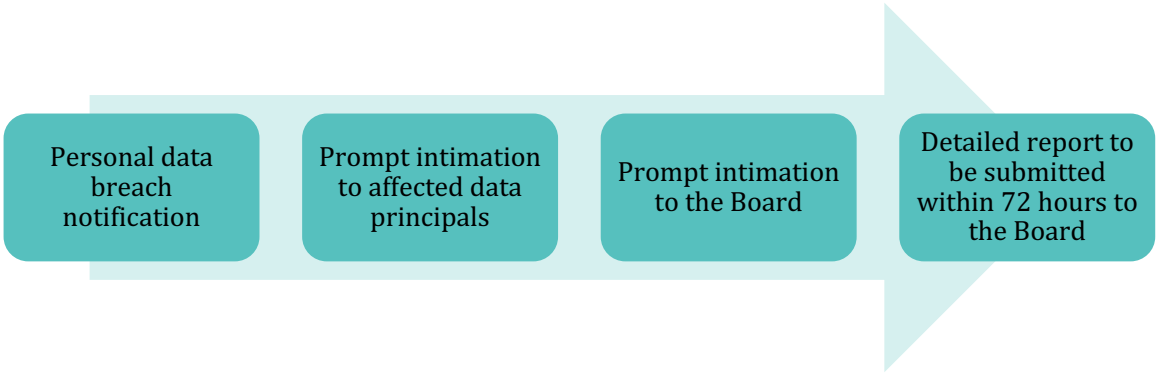
4. **Appointment of a Data Protection Officer ("DPO") in India**:

   Under the DPDPA, SDFs are required to appoint a DPO in India. This would mean SDFs operating outside India who have a DPO outside India may need to evaluate appointing a DPO in India to be compliant with the DPDPA.

Cross-border data transfer

GDPR allows cross-border data transfer based on adequacy decisions, contractual safeguards, or Binding Corporate Rules (BCRs). The DPDPA takes a different approach by which the Central Government can restrict the transfer of personal data to specific countries or territories. Under the Draft Rules, the Central Government may also add other restrictions on transfer of personal data outside India. The data fiduciaries to be compliant with the cross-border transfer restrictions should reassess their data storage and processing strategies.

Prompt personal data breach notification to data principals and the Board



Under the DPDPA, a personal data breach must be reported both to the Board and to each affected data principal. The notification to data principals must be concise, clear, and in plain language, delivered without delay via their registered communication channels. Following the prompt initial notification to the data principal and the Board, the data fiduciaries must send a follow-up notice to the Board, providing a description of the breach and a detailed report, within 72 (seventy-two) hours, covering causes, impact, responsible parties, and remediation efforts. There may be a difference in the notification requirement under the DPDPA and other global data protection laws. GDPR for instance, requires the entities to notify the supervisory authority within 72 (seventy-two) hours, and such affected individuals only if the breach poses a high risk to their rights and freedoms and CCPA requires notification of breach involving unencrypted personal information. The DPDPA, however, mandates notification in all cases, regardless of a harm or risk threshold.

Entities to be compliant with DPDPA may now need to re-evaluate their incident management and response plans to ensure faster detection, response, and notification mechanisms.

Central Government directions

Under the DPDPA, the Central Government has the authority to request information from data fiduciaries in the interest of India's sovereignty, integrity, or security, or to fulfil its legal obligations or perform specific functions. The DPDPA extends this power of the Central Government to all data fiduciaries, including entities that operate outside India but offer goods or services within India.

Non-monetary penalties

While the focus of the global data protection laws is primarily on imposing monetary compensation on the entities violating their data protection obligations, under the DPDPA, the Board apart from having the power to impose monetary penalties, also has the power to recommend to the Central Government to block access to information or services provided by such data fiduciary in the public interest.

This introduces an operational risk that goes beyond mere financial penalties. If the Central Government decides to block access to their services in India, entities could face disruptions in business operations including their ability to process transactions and provide services, or information within India.

Infotech Practice (Privacy and Data Protection)

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:

Akshaya Suresh
Partner

Drishya Kamath
Associate

Tharusha Selvanambi
Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice

---

3 Band 1 Practices

---

4 Band 1 Lawyers,1 Eminent Practitioner

12 Practices and
50 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

Ranked Among Top 5 Law Firms in India for ESG Practice

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

jsa
advocates & solicitors

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