TRACE LAW PARTNERS

DPDP Act Compliance for Alternative Investment Funds (AIFs): Key Considerations and Next Steps

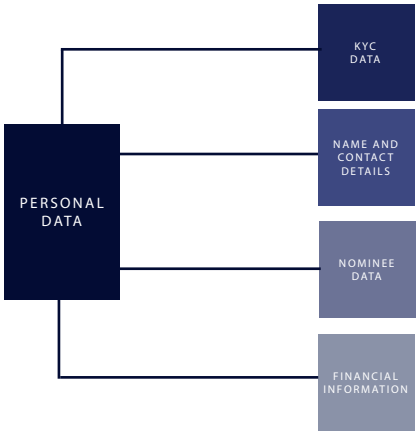
The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") brings in a new data protection regime in India. Businesses now have an approximately 16-month window now to comply with all substantive obligations. These FAQs are intended to help AIFs understand how the DPDP Act impacts their fund operations, investor interactions, and service provider relationships.

1. Does the DPDP Act apply to the AIF ecosystem?

The DPDP Act applies to any processing of digital personal data in India or outside India if in relation to provision of goods and services in India. If AIFs/entities such as the investment manager ("**IM**") on behalf of AIFs in India are processing any "personal data" belonging to any individual, the DPDP Act applies. The DPDP Act also applies to foreign entities in the AIF ecosystem if they process personal data (including feeder entities as they process their own investors' data) in connection with any activity related to offering goods or services to Data Principals (as defined under Q. 3 below) within the territory of India.

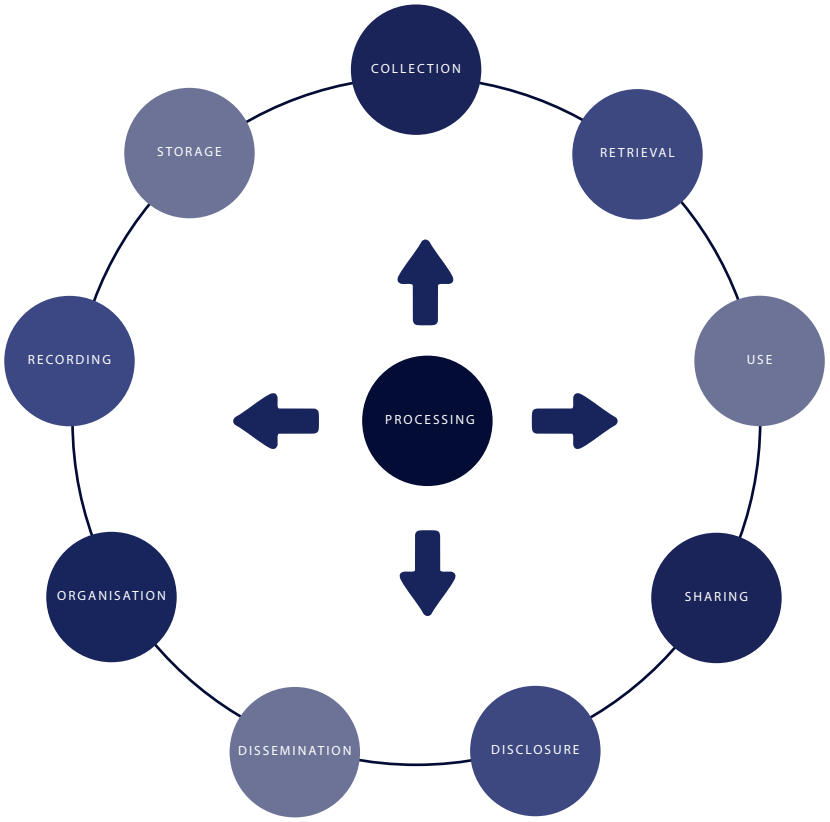
2. What is "personal data" and "processing"?

"Personal data" is defined under the DPDP Act as "any data about an individual who is identifiable by or in relation to such data". The definition of "personal data" is broad and goes beyond obvious identifiers like names or contact details. KYC data collected from investors and directors/partners/individual trustees of investor entities will fall within the definition of "personal data". Even indirect identifiers such as IP addresses may be considered as personal data if they can be used to identify an individual.



"Processing" is defined broadly under the DPDPA and includes the operations depicted below. Processes requiring use of investor data including day to day decision making, opening of accounts and internal

analytics are likely to qualify as "processing" if they involve use of personal data of investors.



3. Who is the "Data Principal" in an AIF context?

Data principal is any individual whose personal data is processed.

- Investors / LPs
- Directors/Partners/Individual Trustees of investor entities
- If the investor is a minor or a person with disabilities, then the investor as well as their parent/legal guardian
- Employees

4. Who is a data fiduciary and data processor?

The Data Fiduciary is the entity that decides the purpose and means of processing. All compliances under the DPDP Act are applicable to the data fiduciary. The data fiduciary is the entity that decides the purpose (why) and means (how) of processing. The data processor is any person who processes personal data on behalf of the data fiduciary.

It is important to determine if an entity is a data fiduciary or a data processor as the obligations under the law and the consequences of non-compliance fall solely upon the data fiduciary. Data fiduciaries are required to enter into contracts with data processors and pass down certain obligations.

Determination of whether an entity acts as a data fiduciary or processor is a factual analysis, based on the role of each party.

For fund structures:

- AIFs are typically "trusts". Since a trust is a non-juridical person, the DPDP Act technically would not apply to the AIF itself. If the AIF is a company or an LLP which is a rare scenario, the applicability of the DPDP Act will depend on which entity acts as the "data fiduciary" in relation to personal data of investors, employees, etc.

- In fund structures, the IM acts on behalf of the AIF, however, it must be seen that from a data protection perspective, which entity controls the decision making with respect to the purpose and means of processing, i.e., why the personal data is used and how it is used. In this context, trustees of AIFs which are set up as trusts could also fall within this ambit, or at least within the ambit of data processors.

- In practice, the IM usually drives investor onboarding, KYC workflows, vendor selection and makes investment decisions. Therefore, it is possible that the IM will be treated as the Data Fiduciary for day-to-day processing if the IM decides "why" personal data is processed and "how" such data is processed.

- Therefore, it is important to consider the roles and responsibilities of the parties involved to deter mine which entity will be considered the data fiduciary.

5. Do AIFs need consent for all processing of personal data?

Processing can be on the basis of consent or under the specific legitimate uses identified under Section 7 of the DPDP Act. In the context of AIFs, most processing of investor personal data is likely to be consent-based, except in limited scenarios where processing can be clearly aligned with a specific legitimate use under Section 7, as outlined below.

Some relevant legitimate uses include:

- Processing data voluntarily provided by the Data Principal for a specified purpose for which the data has been shared (e.g., an investor providing contact details for sending drawdown notices);

- Processing to fulfil a legal obligation to disclose information to the State or its instrumentalities (e.g., reporting to SEBI, FIU-IND, or tax authorities).

The DPDP Act also recognises certain categories of processing of employee personal data as a "legitimate use" that does not require consent. Processing for the purposes of employment or to safeguard the employer from loss/liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by an

employee. The term "purposes of employment" is not defined in the law. This may include various day-to-day employee related activities.

Additionally, certain types of processing activities such as processing of personal data made publicly available by the Data Principal, processing for the purpose of research (in accordance with prescribed standards under the DPDP Act) are exempted from the application of the DPDP Act.

6. How is data collected prior to the commencement of the DPDP Act treated?

If consent was collected before the commencement of the DPDP Act (through terms and conditions or otherwise), a fresh notice must be issued to inform Data Principals, as soon as reasonably practicable, about the personal data and the purpose of its processing, the manner in which the Data Principals can exercise their rights and the manner in which they can make a complaint to the Data Protection Board of India. The Data Principal will have the choice to opt out, in which case the processing will have to discontinue (unless covered by other provisions of the DPDP Act). All other compliances applicable under the DPDP Act will remain applicable.

If no consent has been obtained earlier, consent will need to be obtained in accordance with the DPDP Act and all other compliances will be applicable.

7. What are some important considerations relating to consent and provision of notice?

The specific requirements in relation to consent and notice are provided in the DPDP Act. Importantly, consent given by the Data Principal must be free, specific, informed, unconditional and unambiguous with a clear affirmative action. Further, the notice for consent must provide certain details to the Data Principal. This includes providing an itemised description of personal data being processed and the specified purpose for processing, along with an itemised description of the goods, services, or uses that the processing will enable.

Therefore, consents should be structured in a granular manner, clearly listing out the different purposes of processing (e.g., onboarding and KYC, regulatory reporting, investor communications, marketing updates, data sharing with service providers). While AIFs typically collect investor personal data at the KYC stage, the same data is often subsequently used for multiple downstream purposes such as assessing accreditation status, appointing depositories or custodians, regulatory filings, and ongoing fund administration. Broad consent language and bundled consent will not work under the DPDP Act.

8. If an investor is a child or a person with disabilities, what special provisions apply?

For processing of personal data of children and persons with disabilities, verifiable consent from parents/ the legal guardians is required. The manner in which verifiable parental consent must be obtained is set out in the DPDP Act and rules.

9. What happens if an investor withdraws consent?

If an investor withdraws consent, the AIF is required to cease processing the personal data in respect of which consent has been withdrawn. However, withdrawal of consent does not automatically require deletion of all investor data. The AIF may continue to process the personal data to the extent such processing is permitted under applicable law.

The DPDP Act expressly recognises that the data principal must bear the consequences of withdrawal of consent. To the extent certain processing activities are dependent on consent, withdrawal may impact the AIF's ability to continue providing services, perform fund-related operations, or comply with contractual arrangements linked to such processing.

From a practical perspective, AIFs should assess the impact of consent withdrawal on the investor relationship, clearly identify processing activities that can continue on a non-consent basis, and communicate upfront that withdrawal of consent may limit the AIF's ability to provide certain services or perform fund-related activities.

10. What obligations should be passed down to data processors?

When a data fiduciary appoints a data processor, they must:

- Contractually pass down obligations under the DPDP Act to the data processor depending upon the activity undertaken by such data processor. For instance, for any processing activity, data processors must be obligated to notify the data fiduciary in case of breach, and comply with prescribed security standards. If the data processor is consumer-facing, it must comply with notice and consent require ments at the time of collection of data.

- Carry out diligence to ensure the data processor has technical and organisational capacity to comply with such obligations.

- Require prior approval from the data fiduciary in case of appointment of sub-processors.

- Ensure appropriate oversight mechanisms, such as audits, reports, compliance mechanisms.

11. Does the DPDP Act introduce additional reporting obligations in relation to data breaches?

Yes, "personal data breaches" have to be reported to the Data Protection Board and all the affected Data Principals in the manner set out in the law. "Personal data breach" means 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 such personal data.

This obligation is in addition to reporting to CERT-In and sectoral regulators (if applicable).

12. Are there cross-border transfer restrictions under the DPDP Act?

DPDP Act does not impose blanket localisation but adopts a "blacklist" approach (transfers allowed unless restricted). Currently, no blacklist has been issued by the government.

13. What are the applicable penalties under the DPDP Act?

If the Data Protection Board determines on conclusion of an inquiry that a significant breach of the provisions of the DPDP Act has occurred, it may impose penalties up to INR 250 crores.

14. What should AIFs prioritise in the run-up to full DPDP Act enforcement?

AIFs should follow a structured two-phase approach of discovery and implementation to achieve DPDP Act readiness within the 18-month compliance window.