#taghash

Digital Personal Data Protection Act, 2023 & Rules, 2025

A Primer for Alternative Investment Funds

OVERVIEW

Executive Summary

- The Digital Personal Data Protection Act, 2023 (the “Act”) and the DPDP Rules, 2025 (the “Rules”) establish a rights-based, consent-driven and security-focused approach to the processing of personal data.
- In most fund structures, the Investment Manager will be the Data Fiduciary. A trust-form AIF is unlikely to qualify, as it is not a “person” under Section 2(s).
- Contractual necessity is not a recognised ground of processing. Managers should therefore obtain specific consent from investors unless a legitimate use under Section 7 applies.
- Retention obligations under the PMLA and tax laws qualify, but do not displace, the duty to erase personal data once its purpose has been served.
- The regime overlaps materially with SEBI's Cybersecurity and Cyber Resilience Framework, and a consolidated approach to security, incident reporting and data governance is advisable.

13 May 2027

All remaining provisions take effect

₹250 crore

Amount up to which statutory penalties may extend (Section 33(2))

90 days

Maximum period for responding to a grievance under Rule 14(3)

REGULATORY BACKGROUND

Background and Phased Commencement

Before the Act, personal data was regulated principally by the SPD Rules, 2011, framed under Section 43A of the Information Technology Act, 2000, which distinguished between personal information and sensitive personal data. The Rules take effect in three phases: some provisions on publication, and others after twelve or eighteen months.

1

13 November 2025

ON PUBLICATION

The Rules were notified by the Ministry of Electronics and Information Technology, and certain provisions took effect immediately.

2

After 12 months

SECOND PHASE

Further provisions take effect one year after the date of notification.

3

After 18 months

FINAL PHASE

The remaining provisions take effect eighteen months after the date of notification.

Many funds already operate to GDPR standards. That experience is useful but not determinative: the Act departs from the GDPR in important respects, notably on the grounds on which personal data may be processed.

SCOPE

Application to Investment Funds

Fund structures

- AIFs may be constituted as trusts, limited liability partnerships or companies. Most Indian AIFs are trusts, with a professional trustee that delegates management to an Investment Manager under an investment management agreement.
- SEBI registers the AIF, whereas in the IFSC it is the fund management entity that is registered with the IFSCA. The impact of the regime is broadly uniform across the SEBI and IFSCA categories.

Territorial reach and personal data

- The Act applies to digital personal data processed in India, and to processing outside India in connection with offering goods or services to Data Principals in India.
- A foreign entity, such as the administrator of an offshore feeder fund, may therefore be within scope where its processing relates to investment management services offered in India.
- “Personal data” is defined broadly; a name or mobile number suffices. Obligations therefore arise from first contact with a prospective investor, before any contribution agreement is signed.

Data typically held: contact details, PAN (for TDS), bank details (for payment of redemption proceeds), KYC and AML records of investors and vendors, and employee data.

Identifying the Data Fiduciary

Party	Characterisation	Analysis
Investors	**Data Principals**	Individuals to whom the personal data relates (Section 2(j)).
Investment Manager	**Data Fiduciary**	Determines the purpose and means of processing (Section 2(i)). This will be readily demonstrable for practically every AIF.
Trustee	**Possibly a Data Fiduciary**	Only where it determines the purpose and means of processing jointly with the Investment Manager, which may be difficult to establish for many trustees.
AIF constituted as a trust	**Unlikely to be a Data Fiduciary**	A trust is not a “person” under Section 2(s). The Investment Manager acts as its agent.
AIF constituted as an LLP or company	**May be a Data Fiduciary**	The Section 2(s) objection does not apply, so such an AIF could itself be treated as a Data Fiduciary.
RTAs, KRAs, custodians and fund administrators	**Data Processors**	Process personal data on behalf of, and under contract with, the Data Fiduciary.

The characterisation matters. Were the AIF itself a Data Fiduciary, penalties for non-compliance could fall directly on investors' capital.

Grounds for Processing Personal Data

Consent (Sections 4 and 6)

- Consent must be free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the data necessary for the specified purpose.
- The notice must describe the data and purposes, the manner of exercising rights and withdrawing consent, and a contact for queries and grievances.
- The Data Fiduciary bears the burden of proving that valid consent was given (Section 6(10)).

Legitimate uses (Section 7)

Processing without consent is permitted only for the uses enumerated in Section 7. These include:

- data voluntarily provided for a specified purpose;
- functions of the State;
- compliance with a judgment or order;
- medical emergencies, epidemics and disasters; and
- employment purposes.

Contractual necessity is not a legitimate use. Unlike Article 6(1)(b) of the GDPR, the Act does not permit processing merely because it is necessary to perform a contract. Investment Managers should therefore obtain explicit consent, and a conservative approach is to record that consent before any pre-onboarding data is collected.

Separate Consent Form or Contribution Agreement?

Separate consent form

ADVANTAGES

- Evidences a distinct and specific choice, assisting in discharging the burden of proof.
- Permits consent to be taken before the contribution agreement, covering pre-onboarding data.
- May be updated without amending the contribution agreement, and avoids bundled consent.

DISADVANTAGES

- Adds documentation and may slow onboarding; an unsigned form creates compliance risk.

Contribution agreement

ADVANTAGES

- Reduces the risk that consent is not obtained at all.
- Allows the consequences of withdrawal, including exit, to be addressed contractually.

DISADVANTAGES

- Consent embedded in a commercial agreement is more open to challenge as conditional or insufficiently specific.

Assessment: there are arguments for either route. Where a separate form is used, the onboarding risk may be mitigated by digital consent and a workflow that prevents subscription until consent has been recorded.

CONSENT MECHANICS

Withdrawal of Consent by an Investor

A Data Principal may withdraw consent at any time, and the right cannot be excluded by contract. Because an AIF cannot meet its regulatory obligations without processing an investor's personal data, a withdrawal of consent is, in substance, incompatible with continued investment.

OPTION 1 — OPEN-ENDED CAT III

Treat withdrawal as a redemption request

The fund documents may provide that a withdrawal of consent operates as a request for redemption. This would work for an open-ended Category III AIF. Where a lock-in applies, the PPM may prescribe a charge for premature redemption.

OPTION 2 — HAS PITFALLS

Continue processing on another ground

The Manager may seek to continue processing in reliance on its other legal obligations. This carries material risk: compliance with law is not, as such, an enumerated legitimate use, and Section 7(d) is directed at disclosures to the State.

The contribution agreement may state expressly that withdrawal of consent will require cessation of processing.

STORAGE LIMITATION

Retention and Erasure of Personal Data

Section 8(7) requires a Data Fiduciary to erase personal data, and to cause its Data Processors to erase it, once the specified purpose is no longer being served, unless retention is required by law. The Data Fiduciary remains responsible for its Processors notwithstanding any agreement to the contrary.

PMLA

Records must be maintained for at least five years after the business relationship ends. Personal data may be retained for that period and should be erased thereafter, absent another legal requirement.

Income Tax Act, 1961

Reassessment is generally available for three years after the relevant assessment year, extending to ten years where income of ₹50 lakh or more, represented in an asset, may have escaped assessment.

Clawback provisions

Clawback provisions in the fund documents may justify retaining data after an investor exits. The appropriate period is not settled and should be assessed case by case.

Managers should review their data holdings periodically, erase data no longer required, and maintain a correction mechanism synchronised with KRAs, RTAs, custodians and administrators.

SECTION 8(2)

Contracts with Data Processors

A Data Fiduciary may engage a Data Processor only under a valid contract. Agreements with RTAs, KRAs, custodians and administrators should, at a minimum, provide for the following.

1 Erasure

Erasure of personal data on instruction, and on termination of the services.

2 Correction

Implementation of correction and update requests received from Data Principals.

3 Audit trail

Audit logs evidencing each deletion and update carried out.

4 Audit rights

A right for the Data Fiduciary to audit the Processor's procedures.

5 Indemnity

An indemnity for penalties caused by the Processor's default, without displacing the Fiduciary's primary liability.

6 Notice of constraints

Immediate notice where the Processor cannot erase data for legal, technical or operational reasons.

Rule 6 additionally requires Processor contracts to mandate equivalent security safeguards and immediate notice of any breach.

SECTION 8(5) AND RULE 6

Reasonable Security Safeguards

A Data Fiduciary must take reasonable security safeguards to prevent personal data breaches, including in respect of processing by its Processors. Rule 6 requires, at a minimum, the following measures.

- Encryption or tokenisation of personal data in storage and in transmission.
- Strict, role-based access controls.
- Monitoring and review of all access to personal data.
- The ability to detect and investigate unauthorised access promptly.
- Backups to ensure business continuity.
- Retention of relevant logs for at least one year to support breach detection and remediation.
- Processor contracts requiring equivalent safeguards and immediate notice of any breach.

₹250 crore

Amount up to which statutory penalties may extend (Section 33(2))

1 year

Minimum period for which relevant logs must be retained

The Board determines the penalty having regard to the nature, gravity and duration of the breach, the type of data affected, repetition and mitigation.

Personal Data Breaches: Parallel Reporting Obligations

A single incident affecting investor data may trigger several reporting obligations, each on a different timeline.

Data Protection Board DPDP regime	Data Principals DPDP regime	CERT-In CERT-In reporting	SEBI CSCRF
Notification of the breach to the Board within the specified timelines.	Notification of the breach to each affected Data Principal.	Reporting of cyber incidents within six hours.	Quarterly reporting of cyber incidents by regulated entities.

Practical point: these obligations may result in dual reporting on inconsistent timelines, and should be coordinated within a single incident-response process.

REGULATORY OVERLAP

Interaction with SEBI's CSCRF

SEBI's Cybersecurity and Cyber Resilience Framework (circular dated 20 August 2024) addresses the cyber resilience of regulated entities, whereas the Act addresses the privacy rights of individuals. The two regimes overlap in three areas.

1

Security safeguards

Both require encryption, access controls and vulnerability management. The Rules add a requirement to retain logs for at least one year.

2

Incident reporting

CSCRF reporting to SEBI, breach intimation under the Rules and the six-hour CERT-In window can result in dual reporting on inconsistent timelines.

3

Consent and erasure

Statutory KYC and record-keeping duties may limit an investor's ability to withdraw consent or obtain erasure. Under Section 8(7), retention required by law prevails.

Outside the Act: corporate data, such as a company's financial information, is not personal data, even where the company's shareholders are individuals.

Contact Person, Policies and Grievance Redressal

1

Data protection contact

Each Data Fiduciary, including the Investment Manager, must designate a person to answer questions about the processing of personal data. The contact details must be published prominently, included in every consent notice, and used consistently in rights and grievance correspondence.

2

Privacy notice and policies

The Act does not prescribe a “privacy policy” as such. Read with the Rules, however, it requires detailed notices and written internal policies on security, retention and erasure, breach response, processor management and rights handling. Existing policies should be redrafted accordingly.

3

Grievance redressal

Rule 14(3) requires the Fiduciary to publish the period within which it will respond to grievances, which must not exceed 90 days. The mechanism should also handle access, correction and erasure requests, with acknowledgement, identity verification and records of outcomes.

Significant Data Fiduciary Status

The Central Government may designate a Data Fiduciary as a Significant Data Fiduciary, which attracts enhanced obligations. The designation turns on the factors set out alongside.

ASSESSMENT

Given the limited volume of data they process, AIFs, their Investment Managers and trustees are unlikely to be notified as Significant Data Fiduciaries. A large mutual fund, by contrast, may be. It remains to be seen whether any AIF, Investment Manager or trustee will be so classified.

Factors the Government may consider

- Volume and sensitivity of the personal data processed.
- Risk to the rights of Data Principals.
- National sovereignty.
- Electoral democracy.
- Security of the State.
- Public order.

RECOMMENDATIONS

Action Points for Investment Managers

1. Map personal data flows across the Manager, the trustee and each Processor, and identify the ground relied upon for each processing activity.
2. Decide whether consent will be taken by a separate form or in the contribution agreement, and ensure it is recorded before pre-onboarding data is collected.
3. Address the consequences of withdrawal, including whether it is to be treated as a redemption request, in the fund documents.
4. Adopt a retention schedule reflecting PMLA, income-tax and SEBI requirements, with erasure automated where practicable.
5. Amend Processor agreements to provide for erasure, correction, audit logs, audit rights, indemnity and notice of constraints.
6. Implement the Rule 6 safeguards, including log retention of at least one year, and align them with existing CSCRF controls.
7. Designate and publish a data protection contact, and establish a grievance mechanism with a published response period not exceeding 90 days.
8. Redraft the privacy notice and internal policies, and adopt a single incident-response protocol covering the Rules, the CSCRF and CERT-In.

Given the overlap with SEBI and operational requirements, a consolidated approach and an early review of current practices are advisable.

#taghash

do@taghash.io