INDIA'S NEW DATA PRIVACY REGIME – A PRIMER FOR INVESTMENT FUNDS

INTRODUCTION & BACKGROUND

- The Digital Personal Data Protection Rules, 2025 (**"DPDP Rules**") were notified by the Ministry of Electronics and Information Technology ("**MeitY**") on November 13, 2025. The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and the DPDP Rules take effect in stages, some immediately upon publication, the rest either after one year or eighteen months from the date the DPDP Rules were notified by MeitY.
- Data privacy laws are not new to the Investment Funds industry or to India. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPD 2011**"), issued under Section 43A of the Information Technology Act, 2000, has applied to all *"body corporates"* (companies, firms, sole proprietorships, etc) engaged in commercial/ professional activities. The SPD 2011 classified personal data into two categories: personal information and sensitive personal data or information ("**SPDI**"). SPDI was afforded various protections whereas other personal information was given limited protection. Many Indian funds and their managers, particularly those raising monies from non-residents, also complied with GDPR[1] and other international data privacy frameworks.
- Nevertheless, the DPDP Act and the recently notified DPDP Rules ("**New DP Regime**") are a gamechanger for India; it establishes a rights-based, consent-driven, security-focused approach to the processing of personal data, one that aligns India more closely with global privacy norms. The New DP Regime means that Indian funds will have to move fast to ensure that they adopt a compliance architecture which is in line with the new regime within the prescribed deadlines. In this note, we have analysed some of the key provisions of the New DP Regime that are particularly relevant to the Indian investment funds ecosystem.

STRUCTURE OF AN ALTERNATIVE INVESTMENT FUND (AIF)

- Under the SEBI (Alternative Investment Funds) Regulations, 2012 ("**SEBI AIF Regulations**"), an alternative investment fund ("**AIF**") may be set up in the form of a trust or an LLP or a company. The AIF is required to have a sponsor and investment manager. The sponsor is required to make a minimum capital commitment in the AIF to demonstrate skin-in-the-game. The sponsor and the investment manager may be the same entity. SEBI licences the AIF and not the investment manager, as is the norm in many parts of the world.
- Under the International Financial Services Centres Authority (Fund Management) Regulations, 2022 ("**IFSCA FM Regulations**"), the International Financial Services Centres Authority ("**IFSCA**") licenses fund management entities ("**FME**") to carry out fund management activity. The FME may establish one or more AIFs structured as a trust, a

[1] GDPR stands for General Data Protection Regulation. It is a comprehensive European Union (EU) law on data protection and privacy, officially known as Regulation (EU) 2016/679.

limited liability partnership ("**LLP**"), or a company. The FME is expected to make a minimum capital commitment in each scheme to demonstrate skin-in-the-game. IFSCA licenses and regulates the FME rather than the fund itself, which is broadly in line with international practice.

- In India, most AIFs (under the SEBI AIF Regulations and the IFSCA FM Regulations) are set up in the form of a trust which has a professional trustee. Under Indian law, a trust is not a legal entity and all actions by the trust are carried out by the trustee. The trust pools money from investors and the trustee delegates its powers to the investment manager or FME ("**IM**") under an investment management agreement, pursuant to which the IM deploys the monies pooled from investors and manages the AIF. The IM is usually a private limited company or an LLP.
- The SEBI AIF Regulations provide for three categories of AIFs and SEBI regulations vary across categories, especially on aspects such as investment restrictions, sponsor commitment and fees payable to SEBI. However, there is no difference in the type of structure permitted for funds and fund managers by SEBI and hence, the impact of the New DP Regime is likely to be uniform across the three categories of AIFs regulated by SEBI. In the same manner, though the IFSCA FM Regulations provide for various categories of FMEs and AIFs, the New DP Regime is likely to have the same impact across categories in GIFT-IFSC.

IMPACT OF THE NEW DP REGIME ON AIFS AND THEIR MANAGERS

- The DPDP Act and DPDP Rules regulate the processing of digital personal data in India. They also apply to the processing of digital personal data outside India, if such processing is in relation to the provision of goods and services in India.
- Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Thus, even names and mobile numbers would be personal data and investment managers and trustees of AIFs will start collecting personal data from investors much before a formal contribution agreement is signed.
- AIFs gather personal data primarily for the following reasons:
  - Investors' contact details for future communications.
  - Investors' PAN numbers for deducting tax at source.
  - Investors' bank account details for payment of redemption proceeds.
  - To comply with AML and KYC regulations with respect to their investors and vendors.
  - Employee's data in the ordinary course of business as an employer.
- The New DP Regime will also apply to any foreign entity, such as the administrator of a feeder fund, even if such entity processes personal data of any person outside India, provided that such processing is in relation to the offering of investment management services in India.

DATA FIDUCIARIES AND DATA PRINCIPALS UNDER THE NEW DP REGIME?

- Section 2(i) of the DPDP Act defines a *"Data Fiduciary"* as:

  "Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."
- Section 2(j) of the DPDP Act defines a *"Data Principal"* as:

  "The individual to whom the personal data relates and where such individual is—
  - *child, includes the parents or lawful guardian of such a child.*
  - *a person with disability, including her lawful guardian, acting on her behalf."*
- The DPDP Act defines *"processing"* broadly to include any automated or partly automated operation performed on digital personal data such as collection, recording, organization, storage, use, sharing, disclosure, restriction or erasure.

- It is clear from the definitions of *"Data Fiduciary", "Data Principal" and "processing"* that the investors of an AIF would be data principals, while the IM and/ or the trustee of every fund (if the fund is set up as a trust) would be data fiduciaries under the DPDP Act, if it is demonstrated that the trustee in conjunction with the IM determines the purpose and means of processing of personal data. For practically every AIF in existence, it would be very easy to demonstrate that the IM determines the purpose and means of processing of personal data. It may not be possible to do so for many trustees.
- Equally, there is also the possibility that, an AIF itself could be treated as a data fiduciary. This is because the IM of an AIF is in effect an agent of the AIF, appointed by the AIF's trustee through the investment management agreement. So, when the investment manager collects, stores and processes personal data, it is doing so on behalf of the AIF itself. However, if the AIF is set up in the form of a trust (and not as an LLP or a company), the AIF would not fall within the definition of 'person' given in Section 2(s) of the DPDP Act and hence such an AIF would not be treated as a data fiduciary.
- The DPDP Act imposes extensive duties and responsibilities on all data fiduciaries, such as the obligations to obtain valid consent, ensure data accuracy, implement reasonable security safeguards, notify data breaches, honour data principal rights, manage data retention and deletion, and conduct due diligence on data processors. If the AIF itself is treated as a data fiduciary, any breach of the obligations could lead to penalties being imposed on the AIF, putting the investors' monies at direct risk.

OBTAINING CONSENT FROM POTENTIAL INVESTORS

- Under the New DP Regime, digital personal data can be processed based either on consent from a data principal or for an identified legitimate use.
- As regards consent-based processing, Section 4 of the DPDP Act requires every data fiduciary to process personal data only with the valid consent of the data principal or for certain legitimate purposes.
- Section 6 of the DPDP Act, in turn, provides that *"consent"* must be *free, specific, informed, unconditional, and unambiguous*, and it must be expressed through a *clear affirmative action* and shall signify an agreement to the processing of the personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Accordingly, a conservative interpretation of Section 6 would call for the IM to obtain the consent of every potential investor in writing, or any other recorded format such as an email, before collecting, storing and otherwise processing their personal data such as names, mobile numbers and addresses. The consent form signed by the potential investor should describe the categories of personal data that will be collected, the purposes for which each category will be used, and provide for certain other information including the manner in which the potential investor may exercise certain rights. Specifically, the notice must also provide the investor with a straightforward method to contact the IM or its designated data-protection representative in case of queries or grievances.
- The potential investor must also be informed of his/ her right to withdraw the consent.

LEGITIMATE USE OF PERSONAL DATA

- As stated above, digital personal data can also be processed without consent provided such processing is for a legitimate use. Section 7 of the DPDP Act identifies specific *"legitimate uses"* where personal data can be processed without obtaining explicit consent from individuals. These legitimate uses include:
  - ***Voluntary sharing:*** When individuals voluntarily provide their data for a specific purpose and do not object to its use (such as sharing a phone number to receive a purchase receipt).
  - ***Government Services:*** Processing by the State or its agencies to provide subsidies, benefits, licenses, certificates, or other services, and to perform functions related to national security, sovereignty, or public administration.
  - ***State Sovereignty & security:*** Processing by State (or its instrumentalities) for purposes in the interest of sovereignty and integrity, or security of the State.

- ***State functions (providing services/benefits):*** The State (or its instrumentalities) to provide or issue a subsidy, benefit, service, certificate, licence, or permit, where the data principal has either previously consented or their personal data is available in a notified government database.
- ***Legal Compliance:*** Processing required to fulfil legal obligations or comply with court orders, judgments, or decrees from Indian or foreign tribunals.
- ***Medical emergency situations:*** Processing for responding to a medical emergency that involves a threat to life or immediate threat to the health of the data principal or any other individual.
- ***Public health/disaster:*** Processing necessary during medical emergencies, epidemics, public health threats, natural disasters, or public order breakdowns.
- ***Compliance with judgement/order:*** Processing for complying with any judgment, decree, or order issued under any existing Indian law, or any judgment or order relating to claims of a contractual or civil nature under any law in force outside India.
- ***Employment purposes:*** Processing for employment-related matters or to protect employers from losses, including safeguarding trade secrets, intellectual property, and confidential business information.

- These provisions recognize that while consent is the primary basis for data processing, certain essential activities whether for governance, legal compliance, emergency response, or legitimate business operations require practical flexibility to function effectively without compromising the overall privacy framework.
- ***"Contractual necessity" is not a legitimate use under the New DP Regime***

  It is interesting to note that *"contractual necessity"* is not expressly provided for in the list of legitimate use of personal data under Section 7 of the DPDP Act. This is in studied contrast with Article 6(1)(b) of the GDPR which permits the processing of personal data without consent if the processing is *"necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."* Therefore, AIFs cannot rely on contractual necessity as a ground for processing personal data and rather processing must be based on explicit consent unless one or more of the legitimate uses can be identified as a ground for processing.

OBTAINING CONSENT FROM INVESTORS

- All investors in an AIF execute a contribution agreement. Would it suffice if the investors consent for the processing of their personal data is recorded in the contribution agreement or should such consent be obtained in a separate consent form? There are arguments for either option.
- **Pros of having a separate consent form:**
  - A separate consent form isolates the act of giving consent, making it clear that the investor had a distinct choice and that the consent was specific and unambiguous. Since the onus to prove that valid consent was provided lies with the data fiduciary under Section 6(10) of the DPDP Act, it is easier for the AIF and the IM to defend themselves in case of a conflict. Moreover, it creates a cleaner audit trail for regulators and can be easily presented.
  - It allows the IM to lawfully collect and store investor personal data at the pre-onboarding stage even before the contribution agreement is executed.
  - It is operationally flexible because the IM can update the consent notice without amending the contribution agreement.
  - It simplifies handling investor rights requests such as erasure, correction and withdrawal, since the standalone form can clearly set out processes and timelines.
  - It reduces the risk of the contribution agreement being viewed as *"bundled consent"* or insufficiently specific. When consent is tied to execution of the contribution agreement, regulators may consider it coercive or not

"freely given," which can weaken enforceability. A separate consent form avoids this risk by decoupling data-processing consent from contractual obligations. Additionally, Section 6(1) of the DPDP Act requires consent to be *"unconditional,"* and embedding consent within a contract that the investor must sign to invest could be challenged as conditional consent.

- As mentioned earlier, collection of personal data by the AIF's IM usually starts much before a formal contribution agreement is signed. If a separate consent form is used, it can be obtained prior to the collection of any personal data.

- **Cons of having a separate consent form:**

  - It would be an additional document for investors to sign, increasing paperwork and potentially slowing onboarding. These drawbacks can be mitigated to some extent through digital consent mechanisms (electronic signatures, online consent forms, or integrated digital onboarding platforms), which are expressly permitted under the DPDP Act since consent must be "in writing".

  - If for any reason, the consent form is not signed (intentionally or otherwise), the data fiduciaries (the AIF, the IM and the trustee) would be in breach. If the consent is taken through the contribution agreement, the risk of missing out on the investor's consent is very much reduced. However, this risk can be addressed through proper operational procedures and system checks that make the consent form mandatory before the contribution agreement is executed. For instance, digital onboarding workflows can be designed so that the subscription cannot proceed without a validly executed consent form. Moreover, if consent is embedded in the contribution agreement and is not sufficiently clear, specific, or unbundled, there is a risk that such consent may be deemed invalid under Section 6(1) of the DPDP Act, creating a greater compliance risk.

  - Having the consent clause in the contribution agreement is likely to provide better clarity on the consequences of withdrawal of consent. It would be more difficult to articulate such consequences clearly if consent is taken in a separate form. If consent is obtained through the contribution agreement, such agreement can explicitly state that withdrawal of consent will require cessation of data processing and may necessitate investor exit from the fund, in accordance with Section 6(4) and 6(5) of the DPDP Act.

WITHDRAWAL OF CONSENT BY AN INVESTOR

Can an investor in a fund withdraw consent for the processing of his/her/its personal data, while continuing to be an investor?

It is clear that if an investor withdraws consent for the processing of his/her/its personal data, such investor cannot continue to remain invested in the AIF because the AIF cannot fulfil its contractual, regulatory, and operational obligations without processing the investor's personal data. It is also clear that the right to withdraw consent cannot be waived by contract.[2] Therefore, AIFs could consider following possible solutions to such a request for withdrawal:

- The contribution agreement could provide that a withdrawal of consent would be treated as a redemption request. This approach would work for a Category III open-ended fund. It is common for open-ended Category III AIFs to prescribe a lock-in period for investors. If an investor withdraws consent during the lock-in period, the PPM may provide for a penalty to be levied on the redemption proceeds to compensate the AIF for the premature redemption of the investment.

- One other possibility could be to continue processing data in light of other existing legal obligations. For example, SEBI AIF Regulations or the IFSCA FM Regulations may cast obligations on AIFs or IMs, compliance with which would necessitate processing of personal data. That said, such an approach has pitfalls. Section 7 of the DPDP Act does not identify compliance with legal obligations as a legitimate use. In fact, the import of Section 7(d) appears to be different. It allows for processing of personal data for fulfilling legal obligation on any personal *to disclose any information to the*

[2] Section 8(1) of the DPDP Act.

State. Therefore, unless the continued processing requires a disclosure of information to the State, it could technically be viewed as a breach.

IMPACT OF STORAGE LIMITATION RULE ON FUNDS

- Under the New DP Regime, personal data must be erased once the purpose for which it was collected is no longer being served, unless retention is required under another applicable law. Section 8(7) of the DPDP Act requires the Data Fiduciary to erase personal data and, importantly, to *"cause its Data Processor to erase"* such data. This obligation also extends to all Data Processors engaged by the IM, who must delete such data once notified that the purpose has ended. Under Section 8(1) of the DPDP Act, the Data Fiduciary (the AIF and/or IM) remains fully responsible for ensuring compliance with this deletion obligation by all Data Processors, irrespective of any agreement to the contrary. This means the liability for failure to delete data rests entirely with the Data Fiduciary, even if the failure is on the part of a Data Processor.
- Under PMLA, records must be stored for at least five years after a client relation ends. Under Section 8(7) of the DPDP Act, retention is permitted where "*necessary for compliance with any law for the time being in force*." So, after the expiry of five years after an investor has exited a fund, all personal data relating to such investor should be deleted, subject to any other applicable legal retention requirements.
- Under the Income Tax Act, 1961, the time limit for the Income Tax Department to issue a reassessment notice is generally three years from the end of the relevant assessment year, but can extend up to ten years if the Assessing Officer has evidence that income of ₹50 lakh or more represented in the form of an asset may have escaped assessment. Many PPMs and contribution agreements have a clawback clause allowing the fund to make a claim on an investor if required to meet any tax liability. Given this, how long can an AIF maintain the personal data of an investor who has exited?
- In any event, IMs and asset management companies ("**AMC**") should constantly review investors' personal data and delete data which is no longer required for its original purpose.
- Further, the IM/AMC will have to maintain a mechanism allowing investors to update/ correct their PAN, address, bank account details, contact details, etc. This mechanism would have to be in sync with other fiduciaries and processors (KRA, RTA, custodian, fund admin, etc.) and would also require a prescribed manner for Data Principals to make erasure/update/correction requests which would trigger the Data Fiduciary's obligation to propagate such updates/corrections/erasures to all Data Processors within a reasonable timeframe. As stated before, the Data Fiduciary remains responsible for ensuring that all Data Processors implement such changes, and failure by any Data Processor to do so will be attributed to the Data Fiduciary for enforcement and penalty purposes. Under DPDP Act, Section 8(2) requires Data Fiduciaries to engage Data Processors only under valid contracts that ensure compliance with the DPDP Act. Accordingly, all data processing agreements between the AIF/ IM (as Data Fiduciary) and service providers (as Data Processors) should include:
    - Obligation to delete/erase personal data upon instruction from the Data Fiduciary or upon cessation of services.
    - Obligation to implement correction/update requests.
    - Obligation to maintain audit logs evidencing deletion/updates.
    - Right of the Data Fiduciary to audit the Data Processor's deletion and update procedures.
    - Indemnification of the Data Fiduciary by the Data Processor for penalties imposed due to the processor's failure to delete/update data (though this does not absolve the Data Fiduciary of primary liability to the Data Protection Board).
    - Immediate notification obligation if the Data Processor is unable to delete data due to legal, technical, or operational constraints.

REASONABLE SECURITY SAFEGUARDS TO PREVENT PERSONAL DATA BREACH

- Every Data Fiduciary is required under Section 8(5) of the DPDP Act to implement reasonable security safeguards to prevent personal data breaches, including in respect of data processed by Data Processors. For Trustees and IMs, this means ensuring that investor personal data is protected through appropriate measures across all stages of processing: collection, storage, access, use, sharing and retention.
- Rule 6 of the DPDP Rules 2025 specifies that *"reasonable security safeguards"* must include, at minimum:
    - These safeguards include securing personal data through methods such as encryption or tokenisation of personal data in storage and transmission, applying strict access controls across systems, and maintaining monitoring mechanisms that record and review all access to personal data. Access to investor data must be strictly role-based, ensuring that only authorised personnel can view or handle personal data. The investment manager must have the ability to detect and investigate unauthorised access promptly. Business continuity requires maintaining appropriate data backups so that the confidentiality, integrity or availability of investor information is not compromised. Relevant logs must be retained for at least one year to support breach detection and remediation. Contracts with Data Processors must be updated to require equivalent safeguards and must include provisions mandating Data Processors to notify the Data Fiduciary immediately upon becoming aware of any personal data breach (as required under Section 8(2) read with Rule 6).
    - Non-compliance with these obligations can attract substantial financial penalties, including for breaches resulting from inadequate safeguards, with statutory penalties extending up to ₹250 crore and which represents the maximum penalty and are determined based on factors including the nature, gravity and duration of the breach, type of personal data affected, repetitive nature of breach, and whether the entity took timely mitigation measures (Section 33(2) of the DPDP Act) In addition to regulatory exposure, a security incident involving investor data can significantly erode investor confidence which is especially a material risk for AIFs.

APPOINTMENT BY INVESTMENT MANAGER OF PERSONNEL RESPONSIBLE FOR DATA PROTECTION

- Every Data Fiduciary including the IM is legally required to designate a specific individual responsible for handling data-protection communications. When obtaining consent, the IM must provide the contact details of this authorized person, and these details must also be published so that investors can easily reach the representative for any queries regarding the processing of their personal data. The designated individual must understand the IM's data flows and be able to manage access, correction, erasure and consent-withdrawal requests, as well as coordinate breach-related communication.
- The IM must ensure that the authorised representative's contact details are prominently displayed on its website, portal or application in a manner that is easy for investors to locate and use. These same details must also appear in the privacy or consent notice provided at the time of data collection, along with the communication channels through which investors may withdraw consent or exercise their statutory rights. To maintain consistency and accessibility, all grievance-related correspondence and rights-related communications should repeat the same contact information so that investors always know whom to approach.

OVERLAP BETWEEN SEBI'S CYBERSECURITY AND CYBER RESILIENCE FRAMEWORK AND THE NEW DP REGIME

- The Cybersecurity and Cyber Resilience Framework ("**CSCRF**"), issued by SEBI on August 20, 2024, via Circular No. SEBI/HO/ITD-1/ITD_CSCRF/P/CIR/2024/113, aims to fortify the digital defenses of SEBI-regulated entities ("**RE**s") against evolving cyber threats in the securities market. The primary objective is to establish a standardized, risk-based approach to cybersecurity that not only prevents breaches but also ensures operational continuity and rapid recovery in the face of disruptions. This framework addresses the growing sophistication of cyberattacks, which have increasingly targeted financial infrastructures, by promoting a culture of proactive cyber hygiene and resilience across the ecosystem. Key goals of the CSCRF include enhancing threat detection, incident response, and information sharing among REs and with SEBI.
- There is substantial overlap between the CSCRF and the New DP Regime. These overlaps arise because both frameworks address the protection of personal data in the securities market, but from complementary angles: CSCRF

focuses on cybersecurity resilience for REs, while the New DP Regime focuses on the individual's privacy rights and consent with respect to the same. A corporate's financial data would be entirely outside the ambit of the New DP Regime, even if such financial data relates to the capital contributed to the corporate by its shareholders, many of whom would be individuals.

- **Key areas of overlap include:**

  - ***Data Security Safeguards:*** Both require robust measures like encryption, access controls, and vulnerability management. The DPDP Rules specify baseline technical safeguards (e.g., mandatory encryption and one-year log retention for audits), which supplement CSCRF's emphasis on threat detection and cyber hygiene. This creates a layered approach for REs handling personal investor data, but risks redundancy in implementation.

  - ***Breach Notification and Incident Reporting:*** CSCRF mandates quarterly cyber incident reporting to SEBI and rapid response protocols, overlapping with DPDP Act's stringent two-fold breach notifications (to the Data Protection Board within specified timelines and to affected Data Principals). For financial entities, this results in dual reporting streams—e.g., CERT-In notifications under broader IT rules align imperfectly with both—potentially increasing administrative burdens and inconsistencies in timelines (e.g., 6-hour CERT-In reporting vs. DPDP Act's variable thresholds).

  - ***Consent and Data Principal Rights:*** DPDP Act prioritizes consent, withdrawal rights, and erasure requests for personal data, but CSCRF/SEBI's statutory data collection for investor KYC and compliance limits full withdrawal. Since Section 8(7) of the DPDP Act permits retention of personal data when it is necessary for compliance with any law, in such situations, the Data Principal's rights under the New DPDP Regime would play second fiddle.

DATA PRIVACY POLICY

- The DPDP Act does not use the expression *"data privacy policy"* or *"privacy policy"* as a defined or mandatory document. However, read with the DPDP Rules 2025, it effectively requires every operational Data Fiduciary to provide a detailed external-facing privacy / consent notice to Data Principals and also put in place internal technical and organisational measures, which in practice must be embodied in written policies (security, retention/erasure, breach response, processor management, rights-handling, etc.).

- It is suggested that IMs must accordingly re-draft their existing privacy policies to ensure that all the New DP Regime mandated disclosures are included and are accessible through the IM's website, onboarding documents and consent notices.

GRIEVANCE REDRESSAL MECHANISM TO BE PUT IN PLACE BY FUNDS AND THEIR MANAGERS

- The Data Fiduciary, including the IM has to maintain an effective and responsive grievance-redress mechanism for Data Principals. This obligation ensures that any concern raised by an investor regarding the processing of their personal data is acknowledged and addressed in a timely manner.[3]

- IMs are required to designate an authorized representative for grievance-redressal with provision of their contact details which must be made available for all communication from investors in a clear and accessible manner. The investment manager should keep records of all grievances received, actions taken and outcomes, and retain these logs for the statutory period to demonstrate compliance.

- The same mechanism must also support investor requests to access, correct, update or erase their personal data, as these rights operate through the same communication channel. Neither the Act nor the DPDP Rules specify any deadline for responding to a request for information/access or for responding to a request for correction, completion,

[3] Rule 14(3) of the DPDP Rules states that every Data Fiduciary and consent manager must prominently publish on its website / app "the period under its grievance redressal system for responding to the grievances of data principals". That published period must be "within a reasonable period not exceeding ninety days" for responding to the grievances of Data Principals. The Data Fiduciary must implement appropriate technical and organisational measures to ensure the system is capable of responding within that published period.

updating, or erasure. Nevertheless, the mechanism should ideally issue an acknowledgment within a reasonable timeline, take appropriate verification steps for confirming the identity of the investor, and establish an internal workflow for routing grievances to the legal, compliance or operations teams.

SIGNIFICANT DATA FIDUCIARY

- A Significant Data Fiduciary ("**SDF**") is a Data Fiduciary notified by the Government based on factors such as the volume and sensitivity of personal data processed, risk to the rights of Data Principal, impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State and public order.
- **Are Mutual Funds, AIFs, AMCs, IMs or trustees likely to be classified as an SDF?**

  It remains to be seen if any AIF or its IM or trustee would be classified as an SDF, as their operations generally involve limited volumes of personal data and do not typically process data of national or systemic importance.

  However, there is a possibility that a large mutual fund may be classified as an SDF.

CONCLUSION

- The New DP Regime will require AIF IMs to review and modify several core processes, including consent collection, investor communication, data retention, security safeguards and coordination with service providers.
- Many of these changes intersect with existing SEBI and operational requirements, making it important to adopt a consolidated compliance approach rather than treating DPDP obligations in isolation. A structured review of current practices, documents and systems will help identify gaps early and allow IMs to implement the necessary controls with minimal operational disruption.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -RavisekharNair@elp-in.com

Parthsarathi Jha, Partner – Email - ParthJha@elp-in.com

Abhay Joshi, Partner – Email - AbhayJoshi@elp-in.com

Vinay Butani, Partner – Email – VinayBurani@elp-in.com

Vinod Joseph, Partner – Email - VinodJoseph@elp-in.com

Ketki Agrawal, Principal Associate- Email – KetkiAgrawal@elp-in.com

Paridhi Jain, Associate – Email - ParidhiJain@elp-in.com

Akhil Ganatra, Associate – Email - AkhilGanatra@elp-in.com

Zaynali Badami, Associate – Email – ZaynaliBadami@elp-in.com