Privacy Policy

1. Introduction

TIND Asset Management AS ("TIND", "we", "us" or "our") is committed to protecting your privacy. This Privacy Policy describes how we collect, use, disclose and retain personal data in accordance with the Norwegian Personal Data Act and the General Data Protection Regulation ("GDPR").

This Privacy Policy applies to individuals whose personal data TIND processes, including:

- investors and prospective investors
- individuals representing an investor
- beneficial owners, board members, authorised representatives and signatories
- contacts at suppliers and business partners
- visitors to our websites
- recipients of newsletters and other communications
- participants in meetings and events
- job applicants
- other individuals who interact with TIND

This Privacy Policy may be updated from time to time. The current version will be made available on TIND's website.

2. Data controller

TIND Asset Management AS is the data controller for the processing of personal data described in this Privacy Policy, unless otherwise stated.

TIND Asset Management AS
Fridtjof Nansens plass 5
0160 Oslo, Norway
Company registration number: 930 961 469
Telephone: +47 901 25 532
Email: ir@tindam.com

Questions about privacy and requests to exercise your rights may be directed to the contact details above.

3. Personal data we process

The personal data we process depends on your relationship with TIND and the services you use. We only process personal data that is relevant and reasonably necessary for the applicable purposes.

Identity data

- name
- date of birth and national identification number
- nationality and country of residence
- tax residence and tax identification number
- passport, driving licence or other identification document
- signature

- electronic identification

Contact and professional data

- address
- telephone number
- email address
- employer, position and role
- contact details associated with an undertaking

Client and investment data

- investor and product agreements
- subscription and redemption orders
- transactions and fund holdings
- amount invested
- bank account and payment information
- tax and reporting information
- powers of attorney and signing authorities
- communications relating to investments and the client relationship

Client due diligence and investor protection data

- ownership structure and beneficial owners
- source of funds and source of wealth
- financial circumstances
- investment objectives and time horizon
- knowledge of and experience with financial instruments
- risk tolerance and ability to bear losses
- politically exposed person status, including information about family members and known close associates
- matches against sanctions and screening lists
- other information necessary for client due diligence, suitability assessments or ongoing monitoring of the client relationship

Communications

- email and other electronic communications
- documentation of subscription and redemption orders
- meeting minutes and call notes
- enquiries, complaints and other correspondence
- audio recordings, if TIND makes such recordings and has a lawful basis for doing so

Technical data

- IP address
- device and browser information
- login and activity logs
- use of the client portal and other digital services

- cookies and similar technologies

Recruitment data

- application and CV
- education and work experience
- certificates and references
- other information provided as part of a recruitment process

4. Sources of personal data

We normally receive personal data directly from you or from the undertaking you represent. We may also obtain personal data from:

- public registers
- the Norwegian National Population Register and the Brønnøysund Register Centre
- tax and company registers in other countries
- service providers assisting with client due diligence and electronic identification
- sanctions, PEP and screening lists
- administrators, registrars, banks and other financial institutions
- public authorities
- the investor's representatives or advisers
- publicly available sources

5. How and why we process personal data

TIND processes personal data only where a valid lawful basis under the GDPR applies.

5.1 Compliance with legal obligations

TIND processes personal data where necessary to comply with legal obligations, cf. Article 6(1)(c) GDPR, including requirements under the Norwegian Anti-Money Laundering Act (Act of 1 June 2018 No. 23 relating to measures to combat money laundering and terrorist financing). This includes processing in order to:

- carry out client due diligence and ongoing monitoring
- identify investors and beneficial owners
- prevent and detect money laundering and terrorist financing
- screen for politically exposed person status and sanctions
- prevent fraud and other financial crime
- conduct suitability assessments and comply with investor protection requirements
- document and retain communications and orders
- comply with tax, accounting and reporting obligations
- respond to requests from supervisory, tax, law-enforcement and other public authorities
- comply with other obligations under the rules governing financial services and alternative investment fund management

5.2 Performance of a contract and pre-contractual measures

We process personal data where necessary to enter into or perform a contract with you, cf. Article 6(1)(b) GDPR.

This includes processing in order to:

- register and onboard investors
- carry out onboarding
- receive and transmit subscription and redemption orders
- administer investments and client relationships
- process payments and reporting
- provide access to the client portal
- respond to requests relating to agreements or services
- communicate with investors about their investments
- provide agreed services and fulfil contractual obligations

Where the investor is an undertaking, the processing of personal data relating to its representatives will normally be based on TIND's legitimate interest in establishing and administering the business relationship.

5.3 Legitimate interests

TIND may process personal data where necessary for the purposes of a legitimate interest and where that interest is not overridden by the data subject's interests, rights or freedoms, cf. Article 6(1)(f) GDPR. This may include:

- following up existing and prospective investors
- administering business relationships
- relevant marketing within the limits of applicable law
- client service and quality assurance
- internal administration and corporate governance
- statistics and analysis of our own business
- employee training
- improving our services and working processes
- operating and securing IT systems
- preventing misuse and unauthorised access
- handling complaints and disputes
- establishing, exercising and defending legal claims

Before relying on legitimate interests, we assess the necessity of the processing and its impact on the data subject. You have the right to object to processing based on legitimate interests.

5.4 Consent

Where required, we process personal data on the basis of consent, cf. Article 6(1)(a) GDPR. This may include:

- certain forms of electronic marketing
- optional cookies and analytics technologies
- other processing for which we expressly request your consent

Consent must be freely given, specific, informed and unambiguous. You may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

6. Information and marketing

We may send you information necessary to administer the client relationship or comply with our regulatory and contractual obligations. This may include investor reports, fund reports, notices concerning investments or funds, regulatory information and information about changes to agreements or services.

Such information does not necessarily constitute marketing and may not always be opted out of while the client relationship continues.

We may also send newsletters, product information and invitations to events where we have a lawful basis to do so. You may opt out of direct marketing at any time by using the unsubscribe function in the relevant message or by contacting us.

7. Cookies

TIND's website may use cookies and similar technologies to ensure that the website functions properly, maintain security and improve the user experience.

Strictly necessary cookies may be used without consent where they are necessary for the website or a service expressly requested by you to function.

Optional cookies, for example for analytics or marketing, are used only with your consent where required. You can manage your choices through the website's cookie solution. Further information should be provided in a separate Cookie Policy.

8. Disclosure of personal data

TIND may disclose personal data where necessary to provide services, administer funds and investments, comply with legal obligations or pursue other legitimate purposes. Recipients may include:

- the fund administrator and registrar
- the depositary
- banks, payment service providers, brokers and other financial counterparties
- the auditor
- lawyers, compliance advisers and other professional advisers
- providers of client portals and investor systems
- providers of client due diligence, electronic identification and signing services
- IT, cloud storage, security and communications providers
- providers assisting with marketing or events
- public authorities and supervisory bodies
- tax authorities and law-enforcement authorities
- other recipients where you have requested or consented to the disclosure

Service providers processing personal data on behalf of TIND shall be subject to a data processing agreement. To the extent that they act as processors, they may process personal data only in accordance with our documented instructions.

Certain recipients may act as independent controllers. These may include public authorities, banks, auditors, lawyers and regulated service providers. Such recipients are responsible for their own lawful basis and processing of personal data.

9. Transfers of personal data outside the EEA

Some of our service providers or business partners may process personal data outside the European Economic

Area ("EEA").

Where personal data is transferred to a country that the European Commission has not recognised as providing an adequate level of protection, TIND shall rely on a valid transfer mechanism. This may include the European Commission's standard contractual clauses, binding corporate rules, an express statutory basis or another transfer mechanism approved under the GDPR.

Where necessary, we assess the level of protection and implement supplementary safeguards. You may contact us for further information about the applicable transfer mechanism and safeguards.

10. Information security

TIND and our authorised service providers use technical and organisational measures to protect personal data against, among other things, loss, misuse, unauthorised access, unlawful disclosure, accidental or unlawful alteration, erasure or destruction, and other personal data breaches.

The measures are adapted to the nature of the personal data, the scope of the processing and the relevant risks. Access is restricted to employees and service providers with a need to know. Persons with access are subject to confidentiality obligations.

If a personal data breach is likely to result in a high risk to your rights and freedoms, we will notify you in accordance with applicable law.

11. Automated decision-making and profiling

TIND does not make decisions based solely on automated processing, including profiling, which produce legal effects concerning an individual or similarly significantly affect an individual.

If this changes, affected individuals will be informed and TIND will implement the safeguards required under the GDPR.

12. Children's personal data

TIND's services are not directed at children. TIND does not normally process personal data relating to individuals under the age of 18. If we become aware that such personal data has been collected without a sufficient lawful basis, it will be deleted or the processing will be corrected.

13. Retention of personal data

We retain personal data for as long as necessary for the purposes for which it was collected and for as long as required by legal, regulatory or contractual obligations.

When determining retention periods, we consider, among other things:

- the type of personal data
- the purpose of the processing
- statutory retention requirements
- regulatory expectations
- limitation periods
- potential complaints, disputes and legal claims
- the need to document matters to authorities and investors

Personal data relating to client relationships, client due diligence, transactions, orders, tax and accounting may therefore be retained after the client relationship has ended.

When there is no longer a lawful or legitimate need for retention, the personal data will be securely deleted or anonymised.

14. Your rights

Subject to the conditions set out in the GDPR, you may have the right to:

- receive information about how we process your personal data
- access the personal data we hold about you
- have inaccurate or incomplete personal data rectified
- request erasure of personal data
- request restriction of processing
- receive certain personal data in a structured, commonly used and machine-readable format
- object to processing based on legitimate interests
- object to direct marketing
- withdraw consent
- not be subject to certain decisions based solely on automated processing
- lodge a complaint with the Norwegian Data Protection Authority

These rights are not absolute. TIND may be required or entitled to continue processing, including under anti-money laundering rules, financial markets legislation, tax and accounting rules, or where necessary to establish, exercise or defend legal claims.

We may request information necessary to verify your identity before handling a request.

15. Complaints

If you believe that TIND processes personal data in breach of applicable law, please contact us so that we can investigate the matter.

TIND will respond to all complaints within 10 business days.

You also have the right to lodge a complaint with the Norwegian Data Protection Authority:

Datatilsynet
P.O. Box 458 Sentrum
0105 Oslo, Norway
Website: www.datatilsynet.no

16. Amendments

We may update this Privacy Policy to reflect changes in our business, our processing of personal data or applicable law.

The updated version will be published on TIND's website. In the event of material changes, we may also notify affected individuals directly.

Oslo 27 October 2026