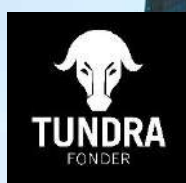


APPENDIX 24: PERSONAL DATA POLICY

APPROVED BY THE BOARD 2026-04-21



1. Table of Contents

1. Table of Contents.....	2
2. Introduction	3
3. Definition of personal data	3
4. The collection of personal data	3
1.1 Sign and administer agreements	3
1.2 Fulfill requirements and legal obligations	3
5. Personal data controller	4
6. Storage of personal data.....	4
7. Sensitive personal data.....	5
8. Rectification, erasure and restriction of processing	5
9. Personal data breaches.....	5
10. Personal data assistants.....	5
11. Company's website	6
12. Processing of personal data outside the EU/EEA.....	6
13. Complaint.....	6

2. Introduction

The General Data Protection Regulation (2016/679) has applied since 25 May 2018. In accordance with its fundamental principles, Tundra Fonder AB [the Company] processes personal data lawfully, fairly and transparently in relation to the person whose personal data is processed [the Data Subject].

3. Definition of personal data

A personal data is any information relating to an identified or identifiable natural person, whereby an identifiable natural person is a person who can be directly or indirectly identified in particular by reference to an identifier such as a name, an identification number, or one or more factors specific to the identity of the natural person. Certain other data may also constitute personal data, such as cookies and IP addresses (see below).

4. The collection of personal data

When the Company processes personal data, it is usually done on the legal basis that the processing is necessary to fulfill a legal obligation. The Company can also process personal data on the basis of consent or agreement. It may happen that the same personal data is processed on the basis of several legal grounds.

1.1 Sign and administer agreements

In connection with a user providing personal data, for example, when purchasing fund units, the user must receive information about the processing of personal data. The legal basis for processing personal data when signing and administering agreements is the fulfillment of agreements. The Company keeps a register of the client who have registered or bought shares in one of the Company's funds. The register contains personal data such as name, social security number, postal address, telephone number, electronic addresses, and information based on the use of the Company's services. The Company processes personal data to see how many fund units their clients own, send control information to the Swedish Tax Agency, prepare and send settlement notes and half-yearly and full-year statements.

1.2 Fulfill requirements and legal obligations

In addition to fulfilling contracts, the Company also processes personal data to fulfill obligations according to law, other constitutions or authority decisions. Examples of processing as a result of legal obligations:

- Customer Awareness: Actions to Prevent, Detect and Investigate Money Laundering, Terrorist Financing and Fraud
- Accounting legislation: Reporting to tax authorities, police authorities, enforcement authorities, and regulatory authorities
- Management of risks regarding, for example, capital coverage and insurance
- Other obligations regarding products and services covered by special legislation, for example, securities, funds and insurance

The company may also collect information from third parties, e.g. public or other externally accessible sources: registers kept by authorities (for example, civil registration registers, tax authorities' registers, company registers and law enforcement authorities' registers), sanctions lists (with international organizations such as the EU), registers kept by credit reference companies and other commercial information providers of information about, for example beneficial owners and persons in a politically exposed position (PEP).

For subscribers to the Company's distribution lists, the following data is processed: email address, name, information on when newsletters have been opened, IP address, geographic location, email application, and email

format. The data is used to administer and monitor the Company's mailings and is only shared to the extent necessary for this purpose or as otherwise required by law.

5. Personal data controller

Tundra Fonder AB, as data controller, is responsible for the processing of personal data within the Company's operations. The CEO is responsible for leading, organising and monitoring the Company's work on personal data matters, and for ensuring that appropriate procedures, controls and security measures are in place to ensure that personal data is processed in accordance with the GDPR and other applicable legislation:

- all processing of personal data is based on a valid legal basis,
- personal data is processed in accordance with the rights of data subjects under the GDPR, including the rights of access, rectification, erasure, restriction of processing, data portability, objection and, where applicable, withdrawal of consent,
- where processing is based on consent, such consent is freely given, specific, informed and unambiguous,
- personal data relating to children is processed with particular care and in accordance with applicable rules on consent and information,
- personal data breaches are documented and, where required, notified to the Swedish Authority for Privacy Protection within 72 hours of the Company becoming aware of the breach,
- the data subject may, free of charge, obtain information as to whether personal data concerning him or her is being processed and, where applicable, access to such data, and
- personal data is erased regularly in accordance with applicable rules and the Company's internal procedures.

6. Storage of personal data

The Company has taken appropriate technical, organizational, and administrative security measures to protect the information the Company has against loss, misuse and unauthorized access, disclosure, alteration, and destruction.

Personal data must not be saved longer than necessary. This means that when the personal data are no longer needed for the purpose for which they were collected, they must be deleted.

Personal data is saved during the time you have an ongoing customer relationship and for a time thereafter, or in accordance with special legislation in the financial sector, which normally means that the Company must by law keep the personal data longer than what the Data Protection Regulation (2016/679) stipulates, e.g.:

- Prevent, detect, and investigate money laundering, terrorist financing, and fraud: at least five years after the end of the business relationship or completed individual transaction
- Accounting legislation: at least seven years, or such longer period as may be required under other applicable legislation or for the Company's establishment, exercise or defence of legal claims.
- Specific provisions for services and products relating to securities and insurance: up to seven years
- Data on the fulfillment of an agreement: up to ten years after the end of the customer relationship for the purpose of providing evidence in the event of any claims (rules regarding statute of limitations)

Personal data is stored electronically in the Company's systems and with approved service providers and, where applicable, in physical form on the Company's premises. The Company shall implement appropriate technical and organisational security measures to protect personal data. Physical records shall be stored securely and be accessible only to authorised persons.

7. Sensitive personal data

As a general rule, the Company does not process special categories of personal data except where such processing is permitted under the GDPR or other applicable legislation.

8. Rectification, erasure and restriction of processing

Subject to the conditions set out in the GDPR, the data subject has the right to request rectification of inaccurate personal data, erasure of personal data (the right to be forgotten), and restriction of processing. These rights are not absolute and must be assessed on a case-by-case basis, taking into account the specific circumstances and applicable legislation.

Where the Company has disclosed personal data to recipients, it shall, to the extent required under the GDPR, inform such recipients of any rectification, erasure or restriction of processing, unless this proves impossible or would involve a disproportionate effort. The data subject shall, upon request, be informed of such recipients.

9. Personal data breaches

The GDPR sets out requirements for how the Company shall act in the event of a personal data breach, i.e. where personal data is destroyed, lost, altered, disclosed or made accessible to unauthorised persons, or where the Company otherwise loses control over the personal data being processed. The Company and its service providers shall document such breaches.

Where the breach is not unlikely to result in a risk to the rights and freedoms of natural persons, the Company shall notify the Swedish Authority for Privacy Protection within 72 hours of becoming aware of the breach. Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the Company shall also inform the data subjects without undue delay, enabling them to take the necessary protective measures.

10. Personal data assistants

The Company may share a user's personal data with others, such as authorities, suppliers and business partners. Before the Company shares such information, the Company always ensures that confidentiality obligations are followed. Personal data is disclosed to authorities only where required by law or authority decision.

A personal data processor is a natural or legal person, public authority, institution or other body that processes personal data on behalf of the personal data controller. The Company may disclose personal data to subcontractors who process data on behalf of the Company. However, these parties may not use the personal data for any purpose other than to provide the service or on the terms specified by the Company. Personal data processing agreements have been entered into with these parties and these agreements always state the subject of the processing, the duration, nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the Company's obligations and rights as a personal data controller.

The company may also share personal data with independent personal data controllers.

11. Company's website

The Company's website uses cookies. Certain cookies are necessary for the website to function as intended and therefore do not require consent. Other cookies may be used, for example, for statistics, analytics or enhanced functionality, and may only be used to the extent permitted under applicable rules and, where required, after the user has provided consent.

The Company uses a consent management solution on its website to inform users about the use of cookies and, where required, to obtain, manage and document consent. Information regarding Tundra Fonder AB's processing of personal data shall be made available on the Company's website under the section "About the Website", where the Company's guidelines on the processing of personal data are also made available to the public.

12. Processing of personal data outside the EU/EEA

The Company may transfer personal data to a country outside the EU/EEA only where the conditions set out in the GDPR are fulfilled. Such transfers may, for example, take place where the European Commission has determined that the recipient country ensures an adequate level of protection, where appropriate safeguards have been implemented, or where a relevant derogation applies in a specific situation.

Where necessary, the Company shall also assess whether additional safeguards are required to ensure an adequate level of protection for data subjects.

13. Complaint

Any person who has questions or wishes to raise a complaint regarding the Company's processing of personal data should, in the first instance, contact Tundra Fonder AB. The Company may be contacted via the CEO, Simon Norenus, at simon.norenus@tundrafonder.se.

The data subject also has the right to lodge a complaint with the Swedish Authority for Privacy Protection (IMY).
