PRIVACY POLICY

Whistleblowing channel

In this Privacy Policy, we disclose how we collect and process personal data within Nordea Pension Foundation's whistleblowing channel.

1. Controller

Nordea Pension Foundation
Business ID: 0201436-9
Address: C/O Mandatum, P.O. Box 1210, FI-00101 Helsinki
Tel: +358 (0) 400 996 435
Email: katriina.hyvonen@mandatum.fi

2. **Data Protection Officer** (the pension foundation has not appointed a DPO; if necessary, the Group's DPO is called on)

Data protection officer: -
Email: -

3. Purpose of processing

The purpose of processing personal data is to detect, investigate and intervene in misconduct and breaches referred to in the act on the protection of persons who report breaches of EU or national law ("**Whistleblower Act**", 1171/2022) and other legislation governing our operations or our Code of Conduct, based on reports made through the whistleblowing channel.

4. Legal basis for processing

The legal basis for processing personal data referred to in this Privacy Policy is, for reports referred to in the Whistleblower Act, the statutory obligation to ensure that the Pension Foundation and our co-operation partners operate in compliance with our Code of Conduct and the legislation governing our operations.

The anonymous whistleblowing channel can be used to submit a report without disclosing any personal details based on which an individual could be identified. If the reporting person provides their personal data or submits a report about another person, the processing of personal data shall be carried out in order to identify and review actions in breach of provisions and regulations concerning the Pension Foundation and to bring the matter before the authorities for investigation and to monitor the stages of the investigation.

5. Categories of data subjects and data to be processed

The data subjects referred to in this Privacy Policy are the reporting persons, the persons concerned, persons who may otherwise know about the reported incidents, as well as the persons participating in the processing of the reports.

Personal data to be processed includes data that is collected when whistleblowing reports are received and processed, for instance:

- The name, position/title, contact details (email address, phone number, address) of the reporting person and other information provided by the reporting person. A report can also be made anonymously, in which case this personal data is not processed;
- The name, position/title, contact details (email address, phone number, address) of the person concerned;
- The name, position/title, contact details (email address, phone number, address) of possible witnesses;
- Information about the suspected misconduct, image recordings;

- Information necessary to determine the accuracy of the report and the necessary measures;
- Information compiled and arising from the investigation into reports;
- Essential information, such as log data, to be saved on the persons processing the report.

Reports made through the whistleblowing channel may, depending on the nature of the reported incident, also contain information belonging to special categories of personal data. Personal data belonging to special categories of personal data is only processed when necessary for the establishment, exercise or defence of legal claims, and in compliance with applicable data protection legislation.

6. Regular sources of data

We collect personal data:

- from data subjects themselves, when they submit a report in their own name and
- in connection with processing the report, when the persons associated with it provide their personal data;
- from persons other than the data subject themself, for instance if the report contains the personal data of people other than the reporting person, or if personal data is obtained from a person other than that data subject themself during the processing of the report;
- from other sources in connection with processing the report, such as the company's document materials and surveillance camera recordings within the limits allowed by data protection legislation.

7. Regular disclosures of data and categories of recipients

No regular disclosures of data.

Due to the nature of the matter, however, we may disclose personal data contained in the reports to the authorities in order for them to perform their statutory tasks, such as for the investigation of crimes or for legal proceedings, and, if necessary, to our advisors to establish, exercise or defend legal claims. The personal data of data subjects may also, if required by EU or national legislation, be disclosed to relevant authorities and, based on the controller's legitimate interest, to the controller's advisors in connection with exercising and defending legal claims.

8. Subcontractors

The technical platform for our whistleblowing channel is provided by our subcontractor WhistleB. BDO is responsible for maintaining the service and, as the processor of the reports, has access to the personal data we process in the service. In addition, the Pension Foundation is managed by Mandatum Life Ltd. All three of the aforementioned parties therefore act as our processors of the data in the whistleblowing channel. In addition, other suppliers of our IT systems and service providers we use to maintain the systems, as well as their subcontractors, may have access to the personal data processed in the whistleblowing channel when carrying out the duties under their service agreements. We require all our subcontractors to comply with the applicable data protection legislation in their operations, and with all our subcontractors, we enter into appropriate data processing agreements that require them to process the personal data exclusively for us and in accordance with our instructions and data protection legislation.

9. Transfer of data outside the EU or EEA

Personal data is not transferred outside the EU or the EEA.

11. Principles of data protection

We always process personal data in the strictest confidence and in the manner required by data protection legislation. Data is stored electronically in databases that are protected with firewalls and other technical safeguards and through the use of personal user IDs and passwords. Only designated persons who, based on their job description, participate in investigating reports, have the right to process the personal data obtained through the whistleblowing channel and are bound by the appropriate non-disclosure obligation.

12. Data storage period

The information received through the whistleblowing channel will be deleted when the investigation has been completed, however no later than five (5) years after the report was received, unless the information must be retained for the execution of rights or obligations stipulated by law or for the preparation, presentation or defence of a legal claim.

The need for further storage of the data is reviewed at least three years after the previous review.

Personal data that is clearly irrelevant to the processing of the whistleblowing report is deleted without undue delay.

13. Rights of the data subject

In terms of the data registers concerning the whistleblowing procedures, the right of the data subject to access the data is restricted in the Finnish Act on Supplementary Company and Industry-wide Pension Funds and in the Finnish Data Protection Act. The law provides for the retention and erasure periods, which is why the right of erasure is not applied to the register. Nor is the right to data portability from one system to another or the right to object to the processing of personal data applied to the statutory processing of personal data.

Under the EU's General Data Protection Regulation (GDPR), data subjects have the following rights related to the processing of personal data. Please note, however, that the exercising of a data subject's rights may be limited to some extent in order to comply with the provisions of the GDPR or other legislation, for instance, to safeguard the investigation of an incident or to protect the reporting person.

- **Inspection**: Data subjects have the right to access their personal data and to obtain copies of it. The right to inspect may be limited based on a legal non-disclosure stipulation in favour of a third party.

- **Rectification:** Data subjects have the right to demand the rectification, completion or erasure of inaccurate, incomplete or expired personal data relating to them. To the extent that a data subject has access to personal data relating to them, the data subject must primarily modify their data on their own initiative if necessary.

- **Erasure:** Data subjects have the right to demand the erasure of their personal data if the processing of personal data is no longer necessary for the purposes for which it was collected.

- **Restriction of processing:** Data subjects have the right to demand that the controller restrict the processing of their personal data, e.g. for a period enabling the rectification of the data subject's personal data.

- **Right to object:** Data subjects have the right object to the processing of their personal data if they consider their personal data to have been processed unlawfully.

- **Complaints:** Data subjects have the right to lodge a complaint with the competent supervisory authority if they consider their rights under data protection legislation to have been violated. The contact details of the Data Protection Ombudsman are available at www.tietosuoja.fi.

14. Contact details in matters concerning processing

If you have questions concerning the processing of personal data referred to in this Privacy Policy, or if you wish to exercise your rights as a data subject, please contact:

BDO Oy

Contact person:	Sami Vainio-Palkeinen
Address:	Vattuniemenranta 2, 00210 Helsinki
Email:	sami.vainio-palkeinen@bdo.fi

15. Updates to the Privacy Policy

We reserve the right to update and amend this Privacy Policy. Unless otherwise required by law, we do not necessarily inform data subjects personally of changes. We encourage data subjects to check this Privacy Policy for changes from time to time.