15 December 2023

Whistleblowing privacy notice

Finnish Fund for Industrial Cooperation Ltd. ("Finnfund") offers a whistleblowing channel for receiving reports of suspected misconduct related to the activities of Finnfund and its investee companies. This privacy notice provides information on how Finnfund processes the personal data of the whistleblower and other individuals related to suspected misconduct when receiving reports and taking necessary actions to investigate the cases.

1. Purposes of processing

The processing of personal data is carried out for the purpose of receiving reports of suspected misconduct in accordance with the Finnish national Act on the Protection of Persons Reporting Infringements of European Union and National Law 1171/2022 (“Whistleblower Act”), as well as to detect and investigate those misconducts, breaches, and violations. Additionally, the processing is carried to receive and investigate reports of suspected misconduct related to actions contrary to Finnfund's Code of Conduct and the international standards and frameworks adhered to by Finnfund.

2. Legal basis for processing

The processing of personal data that is carried out for the purpose of receiving reports of suspected misconduct and for detecting and investigating misconduct, crimes, and violations under European Union and national law is based on a legal obligation imposed by the Whistleblower Act. Finnfund's legal obligation is to provide a whistleblowing channel for reporting suspected misconduct and to take necessary actions to investigate the reported misconduct.

For processing reports not covered by the Whistleblower Act, the processing is based on Finnfund's legitimate interest in ensuring compliance with its Code of Conduct and the international standards and frameworks adhered to by Finnfund.

3. Categories of personal data

In the investigation of reports regarding suspected misconduct, only the personal data necessary for the investigation is processed. The processed personal data varies depending on the nature of the investigation and includes, inter alia, the following personal data:

- name, email address, and phone number of the whistleblower unless the report is submitted anonymously and other personal data about the whistleblower given in the report
- personal data provided by the whistleblower regarding other individuals related to the suspected misconduct, such as the alleged perpetrator, target, or witness of the misconduct
- personal data collected for the investigation of suspected misconduct, such as video recordings, log data, and employment-related

information of individuals involved in the case, as well as data compiled and accumulated during the investigation

Depending on the nature of the case, personal data may include special categories of personal data or personal data relating to criminal convictions and offences. Finnfund processes such personal data only when necessary for the investigation and when processing is justified under the EU's General Data Protection Regulation (GDPR) or specifically in Union law or national legislation. Special categories of personal data refer to personal data revealing an individual's:

- racial or ethnic origin
- political opinions
- religion or philosophical beliefs
- trade union membership
- data concerning health
- sexual orientation or activity
- genetic and biometric data for identifying the person

4. Sources of personal data

The primary source of personal data is the whistleblower. The whistleblowing channel is open to everyone, and potential whistleblowers include, for example:

- employees of Finnfund
- employees of investee companies
- other stakeholders of Finnfund and its investee companies
- third parties with a business relationship with Finnfund or its investee companies
- other entities affected by Finnfund or projects invested by Finnfund

Finnfund may, in the investigation of misconduct, obtain personal data from other sources, such as public sources, systems used by Finnfund, Finnfund's employees, investee companies, and other financial institutions investing in the same company.

5. Transfers and disclosures of personal data

Finnfund uses Navex as a service provider in providing the whistleblowing channel. Navex acts as a processor of personal data. If the misconduct is related to an investee company, Finnfund may also use consultants or lawyers from the investee company's country of origin to assist in the investigation. When transferring personal data to such service providers or subcontractors, contractual arrangements are made to ensure data protection.

Finnfund discloses personal data to third parties only when necessary for the investigation of suspected misconduct. Personal data may be disclosed to authorities if the investigation requires official measures, such as a criminal investigation. Additionally, Finnfund may disclose personal data to investee companies or other financial institutions investing in the same company if the investigation is related to the activities of these entities and the disclosure of personal data is necessary for the investigation of suspected misconduct.

6. Transfers of personal data outside of the EU/EEA

Finnfund may transfer personal data outside the EU/EEA when necessary for the investigation, and the recipient, such as an investee company, another financial institution investing in the same company, an authority, or a consultant or lawyer, is located outside the EU/EEA. When transferring personal data outside the EU/EEA, Finnfund uses applicable transfer methods and safeguards in accordance with the GDPR.

7. Data retention

Personal data received through the whistleblowing channel is deleted five years from the receipt of the report unless further retention is necessary to fulfill legal rights or obligations or for the establishment, exercise, or defense of legal claims. For data that must be kept longer for the reasons above, the necessity of retaining such data is reassessed at least every three years. Personal data with no apparent relevance to the investigation is deleted without undue delay.

8. Rights of the data subject

Data subjects have the following rights according to the GDPR. Data subjects can exercise their rights by contacting Finnfund using the contact details provided in section 9.

Right of access

Data subjects have the right to access the processed personal data and obtain information about the processing of personal data. However, this right may be restricted if it is necessary and proportionate to ensure the accuracy of the report regarding suspected misconduct or to protect the identity of the whistleblower.

Right to rectification

Data subjects have the right to demand the rectification of inaccurate personal data and to have incomplete personal data completed.

Right to erasure

Data subjects have the right to demand the deletion of personal data concerning them if certain conditions are met.

Right to restriction

Data subjects have the right to demand that the data controller restricts the processing of personal data concerning them if certain conditions are met. However, the data subject’s right to restrict processing does not apply to processing under the Whistleblowing Act.

Right to object to the processing

Data subjects have the right to object to the processing of personal data concerning them.

Right to complain with a supervisory authority

Data subjects have the right to complain concerning the processing of personal data with the Office of the Data Protection Ombudsman (https://www.tietosuoja.fi/en).

9. Data controller and contact information

Finnish Fund for Industrial Cooperation Ltd.
Address: Porkkalankatu 22 A, 00180 Helsinki
Telephone: +358 9 348 434
https://www.finnfund.fi/en/contact-us/enquiry-form/