Privacy statement for Whistleblowing – confidential feedback channel

Latest update of the statement: 16 March 2023

1. Controller

Finnvera plc (Business ID: 1484332-4)
Street address: Porkkalankatu 1, 00180 Helsinki, Finland
Switchboard: +358 (0)29 460 11

2. Contact information

Tietosuojavastaava@finnvera.fi

3. Register name

Whistleblowing – confidential feedback channel

4. Purpose of and grounds for the processing of personal data

The purpose of the Whistleblowing channel is to provide customers, employees and other stakeholders with a confidential channel where they can report any suspected cases of misconduct or violations of Finnvera's operating principles to Finnvera for internal investigation.

The processing of personal data collected through the Whistleblowing channel is based on the Act on the Protection of Persons who Report Breaches of European Union and National Law, or the Whistleblower Protection Act (1171/2022) which obliges the establishment of a reporting channel and provides for the protection of whistleblowers who report violations falling within the scope of the Act. Personal data is processed to the extent that is required to appropriately and adequately handle the case reported through the channel.

5. Data content of the register

The following information about the data subject can be recorded in the register:

- Name and contact information of the person who submitted the notification (if provided by the person)
- Specification details regarding the person(s) reported (to the extent that they have been provided)
- Information that the notification provides about the suspected person(s) reported in the notification and his/her violations of law or ethical principles
- Information that the internal investigation of the case yields with regard to the actions of the person reported in the notification and the assessment of their compliance with law/operating principles

6. Storage period of personal data

Information on notifications is stored for five years from the date when the notification was received. However, the data may be stored for a longer period if deemed necessary for the purpose of criminal investigation, a pending trial or for safeguarding the rights of either the person who filed the notification or the subject of the notification. The need to continue storing the data is reviewed at one year's intervals. If the notification made is found to be unfounded and it does not cause further investigation, the notification data will be

destroyed no later than one year from the date when the notification was submitted. Personal data that is clearly not relevant for the processing of the notification will be deleted without undue delay.

7. Regular sources of data

- The notification received through the whistleblowing channel and information, if any, received in further investigation from the person who submitted the notification
- The material received and/or reported in connection with the internal investigation of the case

8. Regular disclosure of data and groups of recipients

Data is only processed by predetermined, named persons at Finnvera. Data is not disclosed outside Finnvera without a legal basis (e.g. the handling of the case requires authorities, such as the police).

9. Transfer of data outside the EU or the EEA

Data is not regularly transferred to countries outside the EU or the European Economic Area.

10. Principles of register protection

Information contained in the register is processed by a restricted group of processors. Information about the identity of the persons involved or any other information about them is not disclosed to outsiders, except to the extent that is necessary for the adequate investigation of the case. The identity of the person who submitted the notification (if the person provided this information) is kept as confidential as possible considering the investigation of the case.

The access rights of the notification channel are restricted to a few designated persons. The controller's personnel are committed to complying with confidentiality obligations. In addition, the employees have committed to complying with internal information security guidelines.

The information system that contains electronically stored data and its backup copies are located in locked facilities that are under surveillance. The hardware on which the register is stored is protected and separated from the public network with a firewall and other technical means.

11. Automated decision-making

The data contained in the register is not used for decision-making that has legal consequences to the person affected and is based on automated processing of data, such as profiling.

12. Restriction of the data subject's rights

Under section 31(1) of the Whistleblower Protection Act, the data subject's right to restrict the processing of their personal data does not apply to the processing of personal data under the Whistleblower Protection Act.

In addition, in accordance with section 31(2) of the Whistleblower Protection Act, the data subject's right of access to the data may be restricted with regard to the personal data

included in the whistleblowing notification, if this is necessary and proportionate to ensure that the notification is accurate or to protect the identity of the whistleblower. However, if only part of the data relating to the data subject is excluded from the right, the data subject has the right to access the other data relating to them.

The data subject has the right to be informed of the reasons for the above restriction and to request that the data be disclosed to the Data Protection Ombudsman.

13. Data subject's right to object to direct marketing

Data in the register is not used for direct marketing.

14. Contact information

The data subject should contact the controller in all matters concerning the processing of personal data and the exercise of their rights. The data subject may exercise their rights by contacting Finnvera's data protection officer at tietosuojavastaava@finnvera.fi.