Register of Fingo Whistleblowing Channel

1. Controller of the register

Name: Finnish Development NGOs –
FingoElimäenkatu 25-27, 00510 Helsinki
050 317 6690, info@fingo.fi

2. Contact person for the register

Kalle Korhonen
c/o Fingo ry
Elimäenkatu 25-27, 00510 Helsinki
kalle.korhonen@fingo.fi, +358 50 317 6688

3. Name of the register

Register of Fingo Whistleblowing Channel

4. Purpose of the processing of personal data

Personal data collected through the whistleblowing channel shall be processed to the extent necessary for the proper and adequate handling of the matter reported through the channel.

5. Information content of the register

- Name and contact details of the notifier, if provided by the notifier.
- Identifying information on the subject of the notification, to the extent provided by the notifier.
- Information provided in the notification on the suspected person (s) to whom the notification relates and on the activity giving rise to suspected misconduct.
- Information obtained in the course of an internal investigation concerning the conduct of the person concerned by the notification and the assessment of its legality or compliance with the policy.

6. Data sources

- Notification received through the whistleblowing channel and possibly information received from the notifier through further investigation.
- Material received and / or reported in the internal investigation.

7. Data storage

The data shall be kept for as long as is necessary for the purpose for which it was collected and for which purpose it is processed, or for as long as required by law and regulations.

8. Sharing of information

Data is processed within a limited number of processors at Fingo. The information will not be disclosed outside Fingo without a legitimate reason, for example, the case will require an authority (such as the police).

9. Sharing of information outside the EU of the EEA

The data can be transferred and stored on servers / databases outside Finland. At present, personal data is not transferred outside the EU or the EEA. All transfers of personal data take place in accordance with the EU Data Protection Regulation and applicable law.

10. Register security principles

The channel is implemented in Juuriharja Consulting Group Oy's First Whistle system.

The information contained in the register is handled by a limited number of processors. The identity of the parties and other information about them shall not be disclosed to third parties except to the extent necessary for an adequate investigation. The identity of the notifier (if provided by the notifier) will be kept confidential to the extent possible to clarify the matter.

Access to the notification channel is restricted to a few designated individuals. Individuals are committed to confidentiality and adhere to internal security guidelines.

The notifier can only see their own notification in the service.

The processing of data in the register shall be carried out with care and the data processed by the information systems shall be adequately protected. When registry data is stored on Internet servers, the physical and digital security of their hardware is adequately addressed.

11. Rights of inspection, modification or removal

The data subject (notifier) has the right to check the information about him / her stored in the register.

To the extent that the notifier is able to act on his own, he shall, without undue delay, upon receipt of the error or discovering the error himself, rectify, delete or supplement the information which is inaccurate, unnecessary, incomplete or out of date in the register.

To the extent that the notifier is unable to correct the data himself, a request for correction shall be made in writing to the controller.

12. Other rights related to the processing of personal data

Data subjects have other rights under the EU's general data protection regulation. Requests must be sent in writing to the controller. If necessary, the controller may ask the applicant to prove his or her identity. The controller will respond to the customer within the timeframe set out in the EU Data Protection Regulation.