Privacy statement for the Whistleblowing data file

1. Controller responsible for personal data processed in the Whistleblowing channel
Ilkka Oyj
PO Box 60, FI-60101 Seinäjoki, Finland
Street address: Koulukatu 10, Seinäjoki
Tel: +358 6 247 7100
Business ID: 0830230-2

2. Controller's contact person
Ari Monni, Data Protection Officer
Tel. +358 6 247 7100
e-mail: firstname.lastname@ilkka.com

3. Processor of personal data

WhistleB Whistleblowing Center Ab (World Trade Center, Klarabergsviadukten 70, SE-107 24 Stockholm) is responsible for the technology used in the whistleblower reporting channel under the EU Whistleblower Protection Directive and applicable legislation, including the processing of messages containing classified information such as whistleblower reports. WhistleB or its subcontractors may not decrypt and read encrypted messages. As such, WhistleB or its subcontractors do not have access to the content of the messages.

The processors of reports are persons separately appointed and authorised by the company/Group to read the report and investigate the matter. Reports are encrypted and password protected. Reports are processed confidentially.

4. Name of the data file
Whistleblowing channel.

5. Purpose of processing personal data
The Whistleblowing channel can be used by employees of Ilkka-group and third parties to confidentially report suspected serious breaches in accordance with the EU Whistleblower Protection Directive and serious violations of the law or the company's policies within the business segments of Ilkka-group.

6. Legal basis for processing
The collection and processing of personal data received through the Whistleblowing channel is based on meeting the obligations of the EU Whistleblower Protection Directive and Finnish data protection legislation as well as the legitimate interest of the controller.

7. Description of the controller's legitimate interest
Ilkka-group collects personal data submitted by the whistleblower in the Whistleblowing channel, the personal data of persons named in the whistleblower report, and the personal data of possible third parties.
The data is needed for the purpose of investigating the suspected breach or abuse of regulations or violation of the controller's internal policies. Processing is based on the controller's legitimate

interest to prevent possible abuses, promote activities that are in line with guidelines and internal policies, and prevent reputational risks.

8. Categories of personal data

a) whistleblower's name and contact information or other identifying information
b) personal data of persons whom the report concerns
c) personal data of any other persons who may have information about the reported breach
d) names of the processors

9. Regular sources of personal data

The Whistleblowing channel and data imported to the channel from other sources.

10. Retention period of data

Only necessary personal data are processed, and processed data contained in the reports is retained only for as long as is necessary to investigate the matter. Personal data contained in whistleblower reports and investigation documents are erased upon the investigation's completion unless the retention of personal data is required by other applicable legislation.

As a general rule, reports and personal data contained in them are retained for 2 years after the investigation's completion unless a longer retention period is necessary due to an investigation by the authorities.

11. Rights of data subjects

The parties concerned have the right to access their personal data and request the rectification or erasure of inaccurate, incomplete or outdated data in accordance with local data protection legislation. These rights may be superseded by precautionary measures aimed at preventing the destruction of evidence or other obstruction of the investigation or processing of the case. All requests to exercise the right of access must be made in writing and signed to the address stated in section 1.

12. Meaningful information regarding automated decision-making or profiling

The processing of personal data does not involve automated decision-making or profiling.

13. Regular disclosures of data and transfer of data outside the EU or European Economic Area

No data is transferred or disclosed outside the EU or the European Economic Area.

14. Safeguards employed

Only persons separately designated and authorised by the company/Group have the right to access the system containing personal data. Each user is given a username and password to the system. Data is stored in information systems that are protected by passwords and other technical measures. The data files and their backups are maintained by the service provider and safeguarded in the manner described in the respective service provider agreement.

Last updated
6 June 2022

Koulukatu 10, PO Box 60, FI-60101 Seinäjoki, ilkka-yhtyma.fi
tel. +358 6 247 7100
business ID: 0182140-9