Instructions for the Whistleblowing channel

1. Introduction – What is whistleblowing and why is it important?

We strive to maintain an atmosphere of transparency in our Group and follow the relevant laws, regulations and policies in all of our companies' business operations. The Whistleblowing channel is a tool that is used for detecting and responding to potential breaches at an early stage. For the list of Ilkka-group companies, visit www.ilkka.com.

The Whistleblowing channel provides our customers, employees and other stakeholders with a confidential channel for notifying Ilkka-group's internal investigation team of suspected serious breaches and abuses within the scope of the EU Whistleblower Protection Directive or serious violations of the law or company policy.

The report can be made anonymously, but you can also leave your contact information if you wish.

2. When should I report my concerns?

The Whistleblowing channel can help us become aware of serious risks to individuals, the company, society or the environment.

The Whistleblowing channel is used to address abuses and serious breaches of the law or company policy that fall within the scope of the EU Whistleblower Protection Directive.

A. The following areas fall within the scope of the Whistleblower Protection Directive:
    1) public procurement
    2) financial services, products and markets, and prevention of money laundering and terrorist financing
    3) product safety and compliance
    4) transport safety
    5) protection of the environment
    6) radiation protection and nuclear safety
    7) food and feed safety, animal health and welfare
    8) public health
    9) consumer protection
    10) protection of privacy and personal data, and security of network and information systems

B. Serious violations of the law or company policy

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

The whistleblower does not need to have solid evidence of a violation, abuse or breach of policy before reporting their concerns. However, whistleblower reports must be made sincerely and in good faith. Abusing the Whistleblowing channel is a serious violation. If it is found that the report is deliberately misleading and made with the intent to cause harm, the whistleblower may be subject to criminal or employment-related sanctions.

If the matter concerns something other than the areas listed above, such as grievances or dissatisfaction at the workplace, general feedback or development ideas, please contact your supervisor or the director responsible for the matter. Such matters are not investigated as whistleblower reports. News tips are also handled elsewhere and can be sent directly to the editor.

3. How do I submit a report?

There are several ways to report a concern:

- ✓ **Option 1** Notify your own supervisor or another supervisor within the organisation.
- ✓ **Option 2** Submit a report in the Whistleblowing channel at: **https://report.whistleb.com/fi/ilkka-yhtyma**
    - Reports can be submitted anonymously
    - If you wish, you can leave your contact information with the report. In this case, the report is not anonymous but is processed confidentially

We encourage anyone who reports a suspicion to disclose their identity openly. All reports are processed confidentially, regardless of how they are received. If you wish, you can leave your contact information when submitting a report in the Whistleblowing channel. In this case, the report is not anonymous but is processed confidentially.

If you wish to remain anonymous, you can submit the report anonymously. The channel for anonymous whistleblower reports is maintained by a third-party service provider, WhistleB. All messages are encrypted. WhistleB protects the whistleblower's anonymity by deleting all metadata such as the IP address. The whistleblower also remains anonymous in any further conversations with the report's investigators.

After submitting a report in the Whistleblowing channel, you will be given an ID number and password. Store them in a secure place. The ID and password are not known to anyone else or stored in any other location. You can use the ID and password to follow the report's progress. By using the ID and password, you remain anonymous at all times while discussing the repot. Ilkka-group or WhistleB cannot know the source of the report unless you include your contact information in the report.

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

4. Course of the investigation

Internal whistleblowing investigation team

Only designated members of the internal whistleblowing investigation team have access to reports made through the channel. Their activities are confidential and recorded in the Whistleblowing channel's logs. During the investigation, the team may consult other individuals for information and expertise. These individuals may access information they need, in which case the obligation of confidentiality applies to them as well. Members invited to the investigation team must sign a non-disclosure agreement.

If the person reports their concern directly to a supervisor or in their own name through the Whistleblowing channel, the report is processed confidentially in accordance with these guidelines.

After a report is submitted

After receiving a report, the internal whistleblowing investigation team decides whether to accept or ignore the report. If the report is accepted, the necessary measures are taken to launch an investigation. See Investigation below.

The whistleblowing team may reject the report when, for example:

- ✓ the alleged breach does not fall within the scope of matters to be reported under these whistleblowing guidelines
- ✓ the report is not made in good faith
- ✓ there is insufficient information available to warrant further investigation
- ✓ the reported matter has already been resolved

If the report contains matters that do not fall within the scope of the whistleblowing guidelines, the internal whistleblowing investigation team takes the necessary measures to resolve the issue.

The internal whistleblowing investigation team confirms that it has received the report within seven days and begins reviewing the report. Reports that fall within the scope of the EU Whistleblower Protection Directive are processed within three month of receiving the report. Other reports are processed as soon as possible. You can follow the progress of the case with the ID and password you received when submitting the report at **https://report.whistleb.com/fi/ilkka-yhtyma**

Do not include any sensitive personal information in your report unless necessary for describing your concern.

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

Investigation

All reports are taken seriously and in accordance with these whistleblowing guidelines.

- ✓ None of the members of the internal whistleblowing investigation team or other persons involved in the investigation will attempt to identify the whistleblower in any way.
- ✓ If necessary, the internal whistleblowing investigation team will ask follow-up questions through the Whistleblowing channel. You can answer the follow-up questions from the investigators using the ID and password you received at the address **https://report.whistleb.com/fi/ilkka-yhtyma**. Pay attention to the channel so that you can provide additional information if needed and read the decision on the case. If you submitted the report anonymously, you will remain anonymous throughout the process.
- ✓ The person whom the suspicion concerns and any other persons connected to the matter cannot participate in the investigation.
- ✓ The internal whistleblowing investigation team decides whether and how the report is investigated.
- ✓ All reports made in the whistleblowing channel are processed confidentially.

When reporting a breach that falls within the scope of the EU Whistleblower Protection Directive

Whistleblowers who report breaches that fall within the scope of the EU Whistleblower Protection Directive are protected against retaliation provided that the whistleblower has reasonable grounds to believe that the report is accurate at the time it was made, the information reported falls within the scope of the law and the whistleblower follows the whistleblowing procedure laid down in the law. Protection against retaliation is provided to, among others, the company's current and former employees, members of the board, managing director, shareholders, persons employed by subcontractors and suppliers, and persons and companies affiliated with them.

When reporting on serious breaches of the company's policies or practices, the matter is resolved within the company with the person concerned and, if necessary, handed over to the authorities. No sanctions or inconvenience will be caused to a whistleblower who reports a breach of the company's policies.

Whistleblowing reports must always be made sincerely and in good faith. If it is found that the report is deliberately misleading and made with the intent to cause harm, the whistleblower may be subject to criminal or employment-related sanctions.

The whistleblower is informed of the results of the investigation of the alleged breach, while respecting the privacy of persons against whom the allegations have been made and other matters related to confidentiality.

When the report concerns a suspected crime, the whistleblower's identity may need to be disclosed.

Privacy of the person named in the report and information disclosed to them

Persons who submit a whistleblower report or whom a report made in the Whistleblowing channel concerns are entitled to rights specified in the applicable data protection legislation. Data subjects have the right to access their personal data and demand the rectification or erasure of inaccurate, incomplete or outdated data.

All necessary security measures to prevent the destruction of evidence and other obstruction of the processing and investigation of the report apply to these rights of data subjects.

Erasure of data

Personal data contained in reports made in the Whistleblowing channel and in the investigation documents and the material used to process the report are 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 two years after the investigation's completion unless a longer retention period is necessary due to an investigation by the authorities.

5. Legal basis of the whistleblowing guidelines

This policy is based on the EU General Data Protection Regulation, the EU Whistleblower Protection Directive and national legislation on whistleblowing.

6. Transfer of personal data outside the EEA

No data is transferred or disclosed outside the EU or the European Economic Area. Transfer of personal data outside the European Economic Area (EEA) is generally prohibited unless specific measures are taken to safeguard the data.

Note! These Whistleblowing guidelines do not cover the transfer of personal data from the EEA to partners located outside the EEA.