WHISTLEBLOWING POLICY

iLOQ Oy (or the "Company")

Last Modified: 11 November 2024

Table of Contents

1. Introduction

This whistleblowing policy, which is drafted in line with the principles articulated in the Company's Code of Ethics, is a vital part of the Company's Corporate Compliance Program.

Employees are often the first to discover misconduct at their workplace, and it is important that an employee who discovers wrongdoing by the Company or any of its employees, consultants, contractors, or suppliers is able to report it without risk of retaliation or discrimination.

The purpose of this policy is to encourage employees to raise concerns about matters occurring within or related to the Company, rather than overlooking a problem or seeking a resolution of the problem outside the Company.

This policy applies to everyone at the Company – all employees, managers, executive officers, and members of the board of directors (all of whom are included in the term "employees" as used in the remainder of this policy).

2. The Whistleblowing System

In order to allow employees to raise concerns about wrongdoing, the Company has established a whistleblowing system that serves as a contact interface designed specifically for receiving and handling employees' reports on suspected misconduct.

However, laws and regulations on protection of personal data set limitations on the circumstances under which a company may process information indicating that one of its employees has been involved in suspected misconduct.

For this reason, the whistleblowing system may only be used in the following circumstances:

First, **only serious misconduct may be reported** through the whistleblowing system. Serious misconduct involves irregularities or improper actions concerning the Company's vital interests or individuals' health and safety. This may for example include:

- financial crime and accounting irregularities;
- the offering or acceptance of bribes;
- environmental risks or crimes;
- security vulnerabilities which constitute a risk for employees' or customers' health or safety;
- serious forms of harassment or discrimination; or
- violations of the Company's Code of Ethics.

Second, **only misconduct by persons in a key or leading position within the Company may be reported** via the whistleblowing system. This means that only misconduct by the Company's board of directors, executive officers, or individuals responsible for major

purchases or other key business functions may be reported through the whistleblowing system.

Third, the whistleblowing system **may only be used to the extent that it is justified not to turn to the Company's standard information and reporting channels**, as described in the last section of this policy. This may for example be the case when the reported person is part of the management or the suspected misconduct, for that or other reasons, runs the risk of not being properly handled.

The whistleblowing system complements the Company's internal information and reporting channels and is available for use on a voluntary basis.

3. How to Report a Concern Through the Whistleblowing System

To report a concern related to an issue which fits the description above, please use iLOQ's whistle-blowing channel, which can be found on Intranet (for internal employees) or on www.iloq.com (for external parties) or you can contact the Company's Chief Compliance Officer at jaana.klinga@iloq.com or +358 (0)44 435 2403.

4. Process

The Company will act upon any concerns raised. Dedicated whistle-blowing team consists of Company's Chief Compliance Officer and General Counsel, CFO and Chief Human Resources Officer as internal members and Chairman of the Board of Directors representing Capnor Wiesel Topco Oy, a beneficial owner of iLOQ Oy. Please note that the Company can assess a concern only after having conducted an initial inquiry and, most likely, after properly investigating the matter in question.

Where appropriate, matters raised may:

- be investigated by management, the board of directors, internal audit, or through the disciplinary process;
- be referred to the police or other law enforcement authorities;
- be referred to an independent auditor; or
- become the subject of an independent inquiry.

In order to protect the individuals involved and those suspected of the alleged wrong-doing, an initial inquiry will be made to decide whether an investigation is appropriate and, if so, what form it should take. If urgent action is required, it will be taken before any investigation is conducted.

5. Timing

Concerns will be investigated as quickly as is practicable. It may be necessary to refer a matter to an external advisor, which may result in an extension of the investigative process. The seriousness and complexity of a complaint will also have an impact on the time needed to investigate the matter.

The Company acknowledges that any person who raises a concern will need assurance that the concern has been addressed. Subject to legal constraints, the Company will provide the person raising the concern with information about the outcome of any investigation.

6. Prevention of Retaliation

The Company will not tolerate any attempt to penalize, or discriminate against, an employee who has used the whistleblowing system to report a genuine concern regarding wrongdoing. Any such retaliation may be subject to disciplinary action by the Company, up to and including termination of employment.

7. Anonymity

Complaints can be made anonymously through the whistleblowing system. However, it normally facilitates any subsequent investigation and handling of the matter if contact details have been provided. Therefore, the Company encourages employees to provide name and contact details when reporting a complaint.

8. False and Malicious Allegations

The Company strives to meet the highest standards of honesty and integrity and will ensure that sufficient resources are put into investigating any complaint received.

However, it is important for any employee considering making allegations to ensure that they are sincere. The making of any deliberately false or malicious allegations may result in disciplinary action.

9. Processing of Personal Data

Reports made through the whistleblowing system are likely to contain personal data – data which directly or indirectly pertains to an identified or identifiable individual. The personal data may pertain to the person who has made the notification, and/or to a person suspected of the alleged wrongdoing.

The Company is the data controller of any personal data collected via the whistleblowing system, and is responsible to ensure that the personal data collected is processed in accordance with applicable laws and regulations on data protection.

The details of the Company for purposes of its role as data controller are as follows:

ILOQ Oy

1842821-6

Elektroniikkatie 10, 90590 Oulu, Finland

info@iloq.com

+358 (0)40 3170 200

9.1 What types of personal data can be processed?

The types of personal data which may be processed in conjunction with an investigation are typically the following:

- The name, position, and contact details (for example e-mail and telephone number) of the employee who submitted the complaint and the individual to whom the compliant relates, as well as any witnesses or other individuals affected.
- Details of the misconduct of which the person reported is suspected.

The Company will only process personal data which is correct and relevant to the investigation. Superfluous personal data will not be processed. Sensitive personal data, such as information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation may not be submitted unless essential for the reported issue, and will be erased unless legal to process and deemed absolutely necessary for the investigation.

9.2 Why is personal data processed?

Any personal data collected via the whistleblowing system will be processed for the purpose of administering and investigating allegations raised, and dealing with discovered misconduct, as described in this policy.

9.3 What is the legal basis for processing personal data?

The Company's processing of your personal data is based on the legitimate interests pursued by the Company. This means that the Company is of the view that its interest in processing your personal data for the purposes listed above outweighs the privacy interest in the processing. In making this determination, we note that the processing of personal data is: (i) necessary to enable employees to raise serious concerns internally that may not be raised in the absence of a whistleblowing channel; (ii) narrowly tailored to achieve the objectives the Company's legitimate interests; and (iii) in compliance with guidelines on whistleblowing issued by the relevant data protection supervisory authority where the report is conducted (if applicable).

9.4 Who has access to the personal data?

The Company takes both technical and organisational security measures to protect the personal data processed. The personal data collected will be processed only by those individuals at the Company who are involved in the investigation. In this context, personal data may be transferred to a department within the Company (such as internal audit), management, the board of directors, or other persons closely related to the Company. In addition, personal data may be transferred to the police or other law enforcement authorities, forensic companies, or independent auditors as well as provider of the whistle blowing system WhistleB Whistleblowing Centre AB, a limited company in Stockholm, Sweden. To the extent deemed necessary, it may also be transferred to the Company's affiliates or joint venture partners.

9.5 For how long is the personal data kept?

The personal data which is compiled and processed will not be retained longer than is necessary. Complaints, reports, and information regarding misconduct which have been investigated will be deleted within two months of the conclusion of the investigation or, if the investigation results in action being taken against the individual who has been reported, when the information is no longer needed for the purpose of carrying out an investigation and taking action. If it is decided that no investigation will be initiated, the information will be deleted immediately after such decision has been made.

9.6 What are your rights?

Subject to any legal preconditions, the applicability of which have to be assessed in each individual case, you have the rights set out below.

If your personal data is incorrect or needs to be updated, you may at any time request that we correct or update the personal data. You may also contact us if you no longer would like us to process your personal data, if you would prefer us to restrict our processing in any manner, or if you want us to erase your personal data. In addition, you may receive a copy of the personal data relating to you, and information regarding our processing of such personal data, by making a request in writing. In such case, we will provide your personal data to you in a commonly used data format.

When personal data pertaining to an individual is collected via the whistleblowing system, the individual must be informed. If it is not possible to inform the individual immediately, for example if such information could jeopardize the Company's investigation, information will be provided at a point of time where it would no longer constitute a risk to the investigation.

If you have any queries regarding the processing of your personal data or wish to exercise any of the rights stated above, please write to the data controller at the contact details provided in this section. The Data Protection Compliance Officer is General Councel Jaana Klinga.

You have the right to lodge a complaint regarding how we processes your personal data to the relevant data protection authority or similar body within your jurisdiction.

10. Standard Reporting Channels

Employees with a concern related to a person or issue which does not fit the description of matters which may be reported through the whistleblowing system should not use the whistleblowing system.

Instead, employees should raise these issues through their standard reporting channel, which consists of the employee's direct supervisor, another supervisor whom the employee trusts, or the human resources department.[1]

11. Related Documents

This policy should be read in connection with the following documents.

- Corporate Compliance Program Description
- Code of Conduct
- Data Protection Manual

Version	Date	Author(s)	Comment
0.2	15th April 2021	T. Pirskanen	1st draft created
1.0	6th October 2021	Board	Approved by Board
1.1	24th November 2023	T. Pirskanen	Reviewed and updated
2.0	12th December 2023	Leadership Team E. Sankari, V. Tolvanen, H. Hiltunen, J. Klinga, J. Lampinen, M. Tuomikoski, T. Thörewik, T. Ainali, T. Pirskanen, T. Karjalainen	Reviewed and approved
3.0	11 November 2024	Leadership Team	Reviewed and approved to be presented to the Finance and Audit Committee and thereafter to the Board for approval
4.0	4th December 2024	Leadership Team	Reviewed and Approved