

Whistleblowing policy

LOGENT GROUP

Administered by: HR Logent Group
Approved by: CEO Logent Group
Valid from: 20260401
Valid blank: Indefinitely

Introduction

Logent is committed to maintaining an open and transparent business environment, guided by high ethical standards. We prioritise safety and demonstrate respect for all individuals affected by our operations.

Logent provides a secure Whistleblowing channel through Falcony, an external whistleblowing system that enables confidential and anonymous reporting.

The channel is available to employees and other individuals who have obtained information about suspected misconduct in a work-related context, including former employees, job applicants, consultants, contractors, suppliers, shareholders, trainees and individuals belonging to the administrative, management or supervisory bodies of a Logent company.

When Can I Use the Whistleblowing Channel?

The Whistleblowing Channel is a tool for maintaining ethical principles and trust. We expect every member of our staff to follow our ethical principles and the laws that govern our organisation in their daily work.

What Can Be Reported?

The Whistleblowing channel should be used to report misconduct or irregularities that there is a public interest in bringing to light. The reporter should have reasonable grounds to believe that the information reported is true at the time of reporting.

Examples of misconduct that may be reported include:

- Bribery, corruption, fraud or money laundering
- Financial irregularities, tax offences or accounting misconduct
- Breaches of competition law or other unlawful business practices
- Serious violations of environmental, health and safety legislation
- Serious breaches of data protection or information security requirements
- Violations relating to product, food, transport or pharmaceutical safety
- Serious discrimination, harassment or abuse of authority
- Attempts to conceal any of the above
- Other serious violations of applicable laws, Logent's Code of Conduct or ethical principles

Please note: The Whistleblowing channel is generally not intended for matters relating solely to an individual's own employment, such as salary, performance feedback, scheduling, interpersonal disagreements or other employment terms, unless the matter involves serious misconduct or is of broader public interest. Such matters should normally be raised with the employee's manager, HR representative or another appropriate internal contact.

How to Submit a report:

Logent uses Falcony, an external and secure whistleblowing system, for the submission and management of whistleblowing reports.

Select the link for the country in which the relevant Logent company is located and follow the instructions in the reporting form. You may submit your report anonymously.

- [Report a concern in Sweden](#)
- [Report a concern in Belgium](#)
- [Report a concern in the Netherlands](#)
- [Report a concern in Norway](#)
- [Report a concern in Denmark](#)
- [Report a concern in Finland](#)

After submitting the report, Falcony will generate an anonymous username and password. Save these credentials securely, as Logent cannot retrieve them for you. You will need them to follow the progress of your report, respond to questions and provide additional information.

Handling of Whistleblowing Reports

All whistleblowing reports are treated with strict confidentiality. Logent prohibits all forms of retaliation against individuals who report concerns and are entitled to protection under applicable whistleblowing legislation. Logent will take appropriate measures to prevent and address any suspected retaliation.

This protection also extends to any Logent personnel assisting or connected to the whistleblower, as well as legal entities owned by, employing, or otherwise linked to the whistleblower.

Reports are handled by specifically authorised and impartial representatives appointed by Logent. Where a report concerns, or may involve a conflict of interest for, a designated case handler, the report will be reassigned to another authorised and independent person. External legal or specialist support may be engaged where appropriate.

Reports are never investigated by individuals involved in or connected to the alleged misconduct. Whistleblowing cases are handled confidentially by authorised parties.

Cases will not be investigated if:

- The alleged behaviour does not fall within the scope of reportable matters under these whistleblowing guidelines.
- The report contains information that is knowingly false or has been submitted with the deliberate purpose of causing harm.
- The information provided is insufficient for further investigation.
- The matter has already been appropriately investigated and resolved, and no relevant new information has been provided.

Protection and Confidentiality

Whistleblowers may choose to remain **fully anonymous**. There is no requirement to disclose personal information. Regardless of whether the reported information is ultimately substantiated, individuals who had reasonable grounds to believe that the information was true at the time of reporting will be protected against retaliation in accordance with applicable law.

Receipt of the report will normally be acknowledged within seven days. The reporter will receive feedback on the follow-up of the report within three months, or within any other period required under applicable national law. Feedback may be limited where necessary to protect confidentiality, personal data, legal privilege or an ongoing investigation.

Processing of Personal Data

Personal data may be processed through the Falcony whistleblowing system and in connection with the assessment, investigation and follow-up of a report.

Depending on the circumstances and applicable law, individuals may have rights relating to access, rectification, restriction, objection and deletion of their personal data. These rights may be limited where necessary to protect the rights and freedoms of others, preserve evidence or avoid obstructing an ongoing assessment or investigation.

Data Deletion and Retention

Personal data that is clearly irrelevant to the handling of a report will be deleted without undue delay. Other personal data will be retained only for as long as necessary to assess, investigate and follow up the report and, unless a longer retention period is required or permitted by applicable law, for no longer than 24 months after the follow-up case has been closed.

Archived case information will be anonymised where possible and appropriate. Identifiable information will not be retained longer than necessary or permitted under applicable law.