



Guidelines for whistleblowing

Document manager: Chief Legal Officer
Approved by: Management Team
Date of approval: 25 November 2025

1. Purpose

These guidelines shall ensure that Eolus complies with applicable laws and regulations as well as to ensure the employees and others can, and are encouraged to, report misconduct and serious incidents without fear of negative consequences.

2. Our Best Practice

At Eolus, we strive to have an open and transparent workplace, where malpractice does not occur. It is therefore important to us that there is clear information on how to report confidentially and securely.

In the event of suspicion of ongoing or previous malpractice, resources must therefore be available to disclose them. By making it easy to report, we work together to promote the trust of employees, customers and the general public in us.

A reported matter will initially be handled by the external Case Manager set out below to ensure independent handling of case whereafter internal contact person at Eolus may take over the matter.

2.1 Who can report in the whistleblower channel?

You can report and receive protection from the Whistleblower Act if you are an employee, volunteer, trainee, active shareholder, person who is otherwise available for work under our control and management or is part of our administrative, management or supervisory body.

Contractors, subcontractors and suppliers to us who have found out about malpractices within the company can also report. The fact that you have ended your work-related relationship with us, or that it has not yet begun, is not an obstacle to reporting malpractice or receiving protection for reporting malpractice externally.

2.2 What can be reported?

All irregularities and serious incidents that are perceived as violations of laws, ordinances, regulations or policies, guidelines or routines adopted by Eolus can be reported. Reports must always be made in good faith and not be unfounded accusations or attempts to achieve personal gain in any way.

Reports to the whistleblower channel can include suspicions of:

- An unlawful act, whether civil or criminal
- Fraud or financial crime
- Bribery or corruption
- Conflicts of interest
- Serious security deficiencies
- Serious misconduct and discrimination including sexual harassment
- Serious practices likely to cause environmental hazards or damage
- Leaking of sensitive information
- Manipulation of company data / records / systems.

This list is not exhaustive but is intended to give an indication of the kind of conduct, which might be considered as wrongdoing.

In addition, there is the possibility to report information about misconduct that emerged in a work-related context that is contrary to EU laws or regulations. If you suspect that this occurs, then please read the scope of the [Whistleblower Directive](#) in Article 2 and Annex Part 1 for applicable laws. The whistleblower channel is not for dissatisfaction and will not handle:

- General views on leadership
- Salary setting
- Recruitment
- Business planning

Employees who wish to raise issues in these areas should in the first instance turn to their immediate superior.

2.3 How to report?

Written reporting

For written reporting, we use Visslan, which is our digital whistleblowing channel. It is always available through <https://Eolus.visslan-report.se>. On the website, you choose to "report" in order to then be able to describe your suspected misconduct. Please describe what happened as thoroughly as possible, so that we can ensure that adequate measures can be applied. It is also possible to attach additional evidence, in the form of, for example, written documents, pictures or audio files, even though this is not a requirement.

Sensitive personal data

Please do not include sensitive personal information about people mentioned in your report unless it is necessary to be able to describe your case. Sensitive personal data is information about; ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, a person's sexual life or sexual orientation, genetic data, biometric data used to uniquely identify a person.

Anonymity

You can be anonymous throughout the process without affecting your legal protection, but you also have the opportunity to confess your identity under strict confidentiality. Anonymity can in some cases complicate the report's follow-up possibilities and the measures we can take, but in such a case we can also ask you to reveal your identity later, again in strict confidentiality to the Case Manager(s).

Follow-up & login

After you have reported, you will receive a sixteen-digit code, which you will in future be able to log in to Visslan with from <https://Eolus.visslan-report.se>. It is very important that you save the code as otherwise, you will not be able to access your report again.

If you lose the code, you can submit a new report referring to the previous report.

Within seven days, you will receive a confirmation that the Case Manager(s) has received your report. The Case Manager(s) is/are the independent and autonomous party that receives reports in the reporting channel, whose contact information is attached in "6.1 Contact information for Case Manager(s)". In case of questions or concerns, you and the Case Manager(s) can communicate through the platform's built-in and anonymous chat function. You will receive feedback within three months on any measures planned or implemented due to the reporting.

It is important that you, with your sixteen-digit code, log in regularly to answer any follow-up questions Case Manager(s) may have. In some cases, the report cannot be taken forward without answers to such follow-up questions from you as the reporting person.

Verbal reporting

In addition, it is also possible to conduct a verbal report by uploading an audio file as an attachment when creating a report at <https://Eolus.visslan-report.se>. You do this by selecting that you have evidence for the report and uploading an audio file there. In the audio file, you describe the same facts and details as you had done in a written case.

In addition, a physical meeting with the Case Manager(s) can be requested via Visslan. This is most easily done by either requesting it in an existing report or creating a new report asking for a physical meeting.

External reporting

We urge you to always report malpractice internally first, but in the event of difficulties or it is considered inappropriate, it is possible to conduct external reporting instead (or after internal reporting without results). We then refer you to contact the competent authorities or, where applicable, to EU institutions, bodies or agencies.

2.4 What are my rights?

Right to confidentiality

During the handling of the report, it will be ensured that your identity as a reporting person is treated confidentially and that access to the case is prevented for unauthorized personnel, i.e. Case Manager(s). We will not disclose your identity without your consent if applicable law does not compel us to, and we will ensure that you are not subjected to retaliation.

Protection against reprisals or retaliation

In the event of a report, there is protection against negative consequences from having reported misconduct in the form of a ban on reprisals and retaliation. The protection against this also applies in relevant cases to persons in the workplace who assist the reporting colleagues and relatives in the workplace, and legal entities that you own, work for or are otherwise related to.

This means that threats of retaliation and attempts at retaliation are not permitted. Examples of such are if you were to be fired, have been forced to change tasks, imposed disciplinary measures, threatened, discriminated against, blacklisted in your industry, or the like due to reporting.

Even if you were to be identified and subjected to reprisals, you would still be covered by the protection as long as you had reasonable grounds to believe that the misconduct reported was true and within the scope of the Whistleblower Act. Note, however, that protection is not obtained if it is a crime in itself to acquire or have access to the information reported.

The protection against retaliation also applies in legal proceedings, including defamation, copyright infringement, breach of confidentiality, breach of data protection rules, disclosure of trade secrets or claims for damages based on private law, public law or collective labour law, and you shall not be held liable in any way a consequence of reports or disclosures provided that you had reasonable grounds to believe that it was necessary to report or publish such information in order to expose a misconduct.

Publication of information

The protection also applies to the publication of information. It is then assumed that you have reported internally within the company and externally to a government authority, or directly externally, and no appropriate action has been taken within three months (in justified cases six months).

Protection is also obtained when you have had reasonable grounds to believe that there may be an obvious danger to the public interest if it is not made public, for example in an emergency. The same applies when there is a risk of retaliation in the case of external reporting or that it is unlikely that the misconduct will be remedied in an effective manner, for example in the event that there is a risk that evidence may be concealed or destroyed.

The right to review documentation at meetings with Case Manager(s)

If you have requested a meeting with the Case Manager(s), they will, with your consent, ensure that complete and correct documentation of the meeting is preserved in a lasting and accessible form. This can be done, for example, by recording the conversation or by keeping minutes. Afterwards, you will have the opportunity to check, correct and approve the protocol by signing it.

We recommend that this documentation is kept in Visslan's platform by the whistleblower creating a case where the information can be collected in a secure way, with the option to communicate securely.

2.5 GDPR and handling of personal data

We always do our utmost to protect you and your personal information. We therefore ensure that our handling of these is always in accordance with the General Data Protection Regulation ("GDPR").

In addition to this, all personal data without relevance to the case will be deleted and the case will only be saved for as long as it is necessary and proportionate to do so. The longest a case will be processed is two years after its conclusion.

2.6 Additional contact

If you have further questions regarding how we handle whistleblower cases, you are always welcome to contact Case Manager(s) or Internal Contact Person.

Contact information - Case Manager(s)

Name: Julia Lundqvist

Position: Associate

Email: jl@vici.se

Phone number: +46 (0)735-98 12 21

Name: Adam Gullstrand

Position: Advocate

Email: ag@vici.se

Phone number: +46 (0)701-41 59 97

Contact information - Internal Contact Person

Name: Karl Olsson

Position: Chief Legal Officer

Email: karl.olsson@eolus.com

Phone number: +46 (0)701 93 73 27

Name: Åsa Lamm

Position: Chief People & Culture Officer

Email: asa.lamm@eolus.com

Phone number: +46 (0)702 03 95 80

For technical questions about Visslan's platform, feel free to create a case at <https://Eolus.visslan-report.se>. Should this not be possible, contact Visslan. Contact information for both can be found below.

Contact information for Visslan (The Whistle Compliance Solutions AB)

Email: clientsupport@visslan.com

Number: +46 10-750 08 10

Direct number (Daniel Vaknine): +46 73 540 10 19

3. Relevant Entity

These guidelines apply to employees of all legal entities within the Eolus group of companies.

4. Roles and Responsibilities

The CEO is owner of these guidelines. These guidelines are approved by the Management Group and reviewed annually.

Document Manager:

- Prepares annual updates the governing documents in Q4.
 - o Ensures the governing documents are clear, consistent, and aligned with corporate governance requirements.
 - o Removes outdated or redundant content.
 - o Submits documents for approval by the designated authority.
- Publishes the governing documents on Eolus Intranet (/About Eolus/Corporate Governance).
- Implementing the governing documents by specific training sessions or other appropriate communication activities.
- Monitors the policy/guidelines compliance.

5. Exceptions

Any need for exceptions to these Guidelines must be clearly defined and documented. All exceptions shall be approved by the CEO.

6. Monitoring of compliance

The following monitoring of compliance actions shall be taken to ensure that the objectives of these guidelines can be met:

- Annual confirmation by the Document Manager that:
 - o the guidelines have been timely updated, and
 - o specific training sessions or other appropriate communication activities have been made.
 - o report to the Board the number of received reports including, on overall level, the number of reports received and the number of reports that led to investigations or other actions.
- Bi-annually
 - o Send test messages to Visslan

7. References

- Code of Conduct
