Aegir

Whistleblower Policy
Aegir Insights

November 2024

Background

At Aegir Insights, we strive to have an open and transparent workplace, where misconduct does not occur. It is important for us to have clear information on how to report misconduct in a confidential and secure way. In the event of locating ongoing or previous misconduct, resources must be able to disclose them. By making it easy to report, we work together to promote the trust of employees, customers and the public.

Definitions

- **GDPR**: General Data Protection Regulation, which is a European regulation governing the processing of personal data and the free movement of such data within the European Union.
- **The Whistleblower Directive**: EU Directive 2019/1936 on the protection of persons reporting irregularities in Union law.
- **Whistleblower Act**: National implementation of the Whistleblower Directive in EU Member States.
- **Visslan**: The Whistle Compliance Solutions AB's service Visslan, which enables digital reporting of misconduct: https://visslan.com/
- **Misconduct**: Public interest in its occurring of acting or omissions, that have emerged in a work-related context.
- **Reporting**: Written or verbal submission of information about misconduct.
- **Internal reporting**: Written or verbal provision of information about misconduct within a company in the private sector.
- **External reporting**: Written or verbal provision of information about misconduct to the competent authorities.
- **Publication or to make public**: To make information about misconduct available to the public.
- **Reporting person**: A person who report or publish information about misconduct acquired in connection with their work-related activities.
- **Retaliation**: Any direct or indirect act or omission which occurs in a work-related context, caused by internal or external reporting or by a publication, which gives rise to or may give rise to unjustified damages to the reporting person.
- **Follow-up**: Any action taken by the Case Manager(s) of a report to assess the accuracy of the claims made in the report and, where appropriate, to deal with the reported violations, including through measures such as internal investigations, investigations, prosecutions, actions to recover funds and to close the procedure.
- **Feedback**: providing reporters ("whistleblowers") with information on the actions planned or taken as a follow-up and on the grounds for such follow-up.

Aegir

Table of Content

1. Who can report through the whistleblower mechanism?

Aegir Insights' whistleblower mechanism can be used by the following persons:

- Current employees, i.e. all employees work for Aegir Insights, including student assistants and other part-time staff, and short- and long-term advisors.
- Former employees.
- Persons not yet employed, who are reporting information in relation to the hiring process or other pre-contractual negotiations.
- Employees of partners with whom Aegir Insights has a more formalized and continuous cooperation with.

2. What can I report?

In case you suspect a possible misconduct, law and/or regulation violation, we urge you to report it as a whistleblowing case. When reporting, it is important that you at the time of reporting have reasonable proof to believe that the information about the misconduct that was reported was true. Assessing whether there were reasonable foundation, circumstances, and information available for you, at the time of reporting, should be the basis for whether you may have assumed that the misconduct was true. In addition, it is also important that it can be considered as a violation reported, and thus give you protection against retaliation.

Please notice that the Danish whistleblower act (in Danish only) does not limit the rules on speaking freely (Danish: 'Fri ytringsfrihed'), which means that as a private person you can express yourself freely.

2.1 Misconduct in the public interest

Misconduct means, for example, violations or irregularities within our company where persons in senior positions or key personnel commit to:

- accounting, internal accounting control, auditing, bribery and corruption, financial crime, or
- other serious irregularities concerning the vital interests of the company or the life or health of individuals, such as serious environmental crimes, major deficiencies in workplace safety and serious forms of discrimination or harassment.

2.2 Misconduct contrary to EU law

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.

3. How do I report?

3.1 Written reporting

For written reporting, we use Visslan, which is our digital whistleblowing channel. It is always available through the platform on https://aegir.visslan-report.se. On the platform, you 'report a case' and describe your suspected misconduct through there. 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, however not a requirement.

3.1.1 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.

3.1.2 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 later ask you to reveal your identity later, again in strict confidentiality to the Case Manager(s).

3.1.3 Follow-up & login

After you have submitted your report, you will receive a 16-didgit code, which you will need to log in to platform and follow your case (https://aegir.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 stating 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 16-didgit code, log in regularly to answer any follow-up questions Case Manager(s) may have. In some cases, the report cannot be brought forward without answers to such follow-up questions from you as the reporting person.

3.2 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 the platform. 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.

3.3 External reporting

We urge you to always report misconduct 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.

4. What are my rights?

4.1 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 require us to, and we will ensure that you are not subjected to retaliation.

4.2 Protection against reprisals or retaliation

As reporting person, you are protected against negative consequences from having reported misconduct in the form of a ban on reprisals and retaliation. The protection also applies in relevant cases to persons in the workplace who assist the reporting person, your colleagues and relatives in the workplace, and legal entities that you own, work for or 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, if 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 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. You shall not be held liable in any way as consequence of reports or disclosures provided, where you had reasonable grounds to believe that it was necessary to report or publish such information in order to expose a misconduct.

4.3 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 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, if there is a risk that evidence may be concealed or destroyed.

4.4 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 the case, from where, the information can be collected and communicated in a secure way.

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. The longest a case will be processed is two years after its conclusion. For more information about our handling of personal data, see the Aegir company policies_December 2023.

6. Additional contact

If you have further questions regarding how we handle whistleblower cases, you are always welcome to contact Case Manager(s), see below.

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

6.1 Contact information for Case Manager(s)

Name: Lise Markvard Pejtersen
Position: Head of HR & Business Support
Email: lise.pejtersen@aegirinsights.com
Phone number: +45 24790382

6.2 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