

# Whistleblower policy

Whistleblower policy .....	1
Background.....	1
Definitions .....	1
1. Who can report? .....	2
2. What can I report?.....	2
3. How do I report? .....	3
3.2 Verbal reporting .....	4
3.3 External reporting.....	4
4. What are my rights? .....	4
5. GDPR and handling of personal data .....	5
6. Additional contact.....	5
Appendix 1: 5 Questions to Determine if you are Protected by the Whistleblower Act .....	6

## Background

At Sesami Cash Management Technologies, 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.

This whistleblower policy covers the legal entities:

- |  |           |
|--|-----------|
| Sesami Cash Management Technologies Nordic AB  | – Sweden  |
| Sesami Cash Management Technologies Nordic A/S | – Denmark |

## 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:** Acting or omissions that have emerged in a work-related context that there is a public interest in it occurring.
- **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 reports or publishes information about misconduct acquired in connection with his work-related activities.
- **Retaliation:** Any direct or indirect act or omission which occurs in a work-related context and which is caused by internal or external reporting or by a publication, and which gives rise to or may give rise to unjustified injury to the reporting person.
- **Follow-up:** Any action taken by the Case Manager(s) of a report to assess the accuracy of the allegations made in the report and, where appropriate, to deal with the reported infringement, 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.

## 1. Who can report?

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. What can I report?

In case of suspicion of possible misconduct, law and/or regulation violation, we urge you to report this to us as a whistleblowing case. When reporting, it is important that you at the time of reporting had reasonable grounds to believe that the information about the misconduct that was reported was true. Assessing whether there were reasonable grounds, circumstances and information that were available to 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 actually be considered a violation that can be reported, and thus give you protection against retaliation.

Before you blow the whistle, read [Appendix 1](#): 5 questions to determine if you are protected by the Whistleblower Act.

### 2.1 Malpractice in the public interest

You can report information about misconduct that has emerged in a work-related context that there is a public interest in it coming to light. In the event of other types of personal complaints that do not have a public interest in them coming to light, such as disputes or complaints regarding the workplace or the work environment, we encourage you to contact your immediate manager. This is to ensure that these matters are prepared in the best possible way.

Examples of malpractices of a serious nature that should be reported:

- Deliberately incorrect accounting, internal accounting control or other financial crime.
- Incidence of theft, corruption, vandalism, fraud, embezzlement or hacking.
- Serious environmental crimes or major deficiencies in workplace safety.
- If someone is exposed to very serious forms of discrimination or harassment.
- Other serious misconduct affecting the life or health of individuals.

## 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 <https://sesami.vissslan-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.

#### 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 reported, you will receive a sixteen-digit code, which you will in future be able to log in to Visslan with from <https://sesami.vissslan-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.

## 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 <https://sesami.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.

## 3.3 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.

## 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 compel us to, and we will ensure that you are not subjected to retaliation.

### 4.2 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 person, your 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 as 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.

## 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 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.

## 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 a case where the information can be collected in a secure way, with the option to communicate securely.

## 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.

## 6. Additional contact

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

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

## 6.1 Contact information for Case Manager(s)

### Denmark

Name: Gitte Andersen (internal, Service Manager Region Nordic)  
E-mail: gitte.andersen@sesami.io

Name: Lotte Larsen (internal, Customer support and dispatch)  
E-mail: lotte.larsen@sesami.io

### Sweden

Name: Mikael Mellberg (external, Law Firm Lindahl)  
E-mail: mikael.mellberg@lindahl.se

Name: Elinor Söderberg (external, Law Firm Lindahl)  
E-mail: ellinor.söderberg@lindahl.se

Name: Christina Hagert (internal, Quality Assurance Manager)  
E-mail: christina.hagert@sesami.io

Name: Lena Collin (internal, HR)  
E-mail: lena.collin@sesami.io

## 6.2 Contact information for Visslan (The Whistle Compliance Solutions AB)

Email: [clientsupport@visslan.com](mailto:clientsupport@visslan.com)

Number: +46 10-750 08 10

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

# Appendix 1: 5 Questions to Determine if you are Protected by the Whistleblower Act

How do you know if you're protected by the Whistleblower Act? What should you consider before blowing the whistle? To whom should a whistleblower errand be reported?

Oscar Fredriksson is a Swedish lawyer and head of investigations at Starck & Partner, with long experience of investigating violation, harassment, bullying, whistleblower errands and other kinds of business-related incidents. In this blog post, he provides us with five questions to ask yourself before deciding to blow the whistle, in order to determine if you're protected by whistleblower law.

## 1. Am I protected by the Whistleblower Act?

The first question to consider as a whistleblower is: – Am I protected by the Whistleblower Act?

In the Whistleblower Act, it is stated who is protected by it. The current Whistleblower Act names the following groups as protected by law:

- employees
- persons seeking employment
- persons seeking or doing volunteer work
- persons seeking or doing an internship
- persons being considered for doing work or persons actively doing work under the control and leadership of the organisation
- self-employed persons seeking or doing work for the organisation
- persons being considered for or persons participating in the management, administrative, or regulatory body
- shareholders being considered for or actively doing work in the company
- persons who have belonged to any of the above categories and have received or obtained the information during their time in the business.

This is a rather extensive list of people with connections to the business. If you belong to any of the categories above you are protected by the Whistleblower Act.

## 2. Has applicable legislation or regulation been violated?

Issues related to environmentally hazardous emissions, corruption, criminal activities, or the operation of the business in violation of applicable regulations may serve as grounds for whistleblowing. The support you need to make a whistleblowing report can be based on your own experiences or documentation showing that the reported activities are in breach of national legislation, EU law, or specific regulatory requirements.

## 3. Is the information of public interest?

You should be aware that perceived misconduct concerning personal employment conditions typically falls outside the whistleblowing legislation. The Whistleblower Act can only be applied when a report concerns misconduct that is of so-called "public interest".

Being subjected to offensive discrimination, harassment, or bullying in the workplace is generally not considered a matter of public interest. "Public interest" means that for a reported issue to be considered whistleblowing, the issue should not be limited to your personal conditions and experiences in the workplace. There has to be reasons to make the issue publicly known. Common personnel matters such as feelings of dissatisfaction or personally targeted offenses, harassment, or bullying are therefore typically not subjects to be investigated under the protection of whistleblowing law. In such cases, labor laws and anti-discrimination laws serve as the legal basis instead.

## 4. Do I have to report the issue internally first?

Whistleblower reports can be made in three different ways under the protection of the Whistleblower Act. You can report the misconduct to the employer where the wrongdoing is occurring, make an external report to the relevant authority, or disclose the information by sharing it with, for example, the media, politicians, or trade unions. Before choosing to disclose the information publicly, you must first attempt to raise the issue internally and also report it to the appropriate authority. If the authority has a specific reporting channel, you can directly approach them without first raising the issue internally.

If you don't receive any response within a reasonable time, you are allowed to disclose the information publicly. The Whistleblower Act states that a confirmation that the whistleblower report has been received should be given within seven days, and there should be feedback regarding what actions have been taken



within three months. If you don't receive a response within these time frames, you can proceed with disclosing the information publicly under the protection of the Whistleblower Act.

## 5. Do I need to prove that the information is correct?

You don't have to be able to prove that the information you provide is correct, but it can't be based solely on rumors either. You can share things that you have personally witnessed and experienced or provide supporting documents for your claims. In such cases, the employer must investigate whether the information is accurate and, if so, take measures to address the issue. Even if the information turns out to be untrue, you are still protected by the Whistleblower Act as long as you provided the information in good faith - meaning that you believed the information you provided was correct.

## In conclusion

It should also be noted that the legislation regarding source protection and freedom of expression when contacting journalists remains unchanged, and the Whistleblower Act does not alter these regulations. However, the fastest way to address any misconduct is often to report the information to the responsible manager or blow the whistle internally.

If there is no internal response, there may be grounds to escalate the matter to the relevant authority and, if that step doesn't lead to any action either, to disclose the information publicly. Although the Whistleblower Act grants the right to report anonymously, a whistleblower may still be required to testify about what they have experienced in order to have the issue examined legally.