Whistleblower policy

Background

At Signmax AB, 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 our employees, customers and the public.

Our cases are handled by Visslans ärendemottagning to guarantee independent handling of cases. See more information and contact details under "6.1 Contact details for case managers".

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**: Acts or omissions occurring in a work-related context for which there is a public interest in disclosure.
- **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 discloses information about misconduct acquired in the course of his/her 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 disclosure, which causes or is likely to cause unjustified harm 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, recovery measures and closure of 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.

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.

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 or other suitable person instead. 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.
- Other serious misconduct affecting the vital interests of the company.

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://skyltmax.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.

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 whole 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 actions we can take, but in such a case we may also ask you, under strict confidentiality, to reveal your identity later on.

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://skyltmax.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 can not 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://skyltmax.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. Their contact details are available at the following web address: External whistleblowing reporting channels.

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 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.

If the call was not recorded, case managers have the right to document the conversation through a transcript. Afterwards, you will have the opportunity to check, correct and approve the transcript 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. For more information about our handling of personal data, see the Company's policy on personal data.

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://skyltmax.visslan-report.se. Should this not be possible, contact Visslan. Contact information for both can be found below.

6.1 Contact details for case managers

External Case managers:External Case managers:

Visslans Ärendemottagning

intakemanagement@visslan.se

Internal Case managers:

Name: Andreas Neander

Company/Position: Signmax AB

Email: andreas@skyltmax.se

Phone number: 0739 539 647

Name: Sara Olsson

Company/Position: Signmax AB

Email: sara.olsson@skyltmax.se

Phone number: 0705 246 339

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

Email: clientsupport@visslan.com , intakemanagement@visslan.se

Number: +46 10-750 08 10

Please visit the Visslan website for more information about Visslan.