

Whistleblower policy

Background

At Concejo, we strive to have an open and transparent workplace, where there will be no misconduct. 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 misconduct, there must therefore be resources to disclose them. By making it easy to report, we work together to foster employees, customers and the public's trust in us.

Our cases are initially handled by Starck & Partner to guarantee independent handling of cases. Our internal contact persons may then take over the case from the initial case managers. See more information and contact details under "6.1 Contact information for case managers"

This whistleblower policy covers the legal entities Concejo AB (publ), Albion Holding AB, Concejo AIF AB, Concejo Invest AB, CMG International AB, Concejo SALNAV AB, Concejo IP AB and Firenor International AS.

Definitions

- **GDPR:** The General Data Protection Regulation ((EU) 2016/679), which is a European regulation that regulates the processing of personal data and the free movement of such data within the European Union.
- **Whistleblower Directive:** Directive 2019/1936 on the protection of persons who report wrongdoings of Union law.
- **The Whistleblower Act:** Act (2021:890) on the protection of persons who report misconduct.
- **Visslan:** The Whistle Compliance Solutions AB's whistleblower service Visslan, which enables digital reporting of misconduct.
- **Misconduct:** Actions or omissions that have come to light in a work-related context for which there is a public interest in bringing it to light.
- **Reporting:** Verbal or written provision of information about misconduct.

- **Internal reporting:** Verbal or written provision of information about misconduct within a private sector company.
- **External reporting:** Provision of information on irregularities to the competent authority(ies) in verbal or written terms.
- **Publication or publication:** To make information about misconduct available to the public.
- **Reporting person:** A person who reports or makes public information about misconduct acquired in the course of his or her work-related activities.
- **Retaliation:** Any direct or indirect act or omission which occurs in a work-related context and which is the result of internal or external reporting or of a publication, and which causes or may cause unjustified harm to the reporting person.
- **Follow-up:** Any action taken by the recipient of a report to assess the accuracy of the allegations made in the report and, where applicable, to address the reported breach, including through measures such as internal investigations, investigations, prosecutions, recovery measures and the closure of the procedure.
- **Feedback:** providing reporting persons ('whistleblowers') with information on the actions planned or taken as a follow-up and on the grounds for such follow-up.

1. Who can whistleblow?

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

Contractors, subcontractors and suppliers to us who have become aware of irregularities 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 a misconduct.

2. What can I report?

If you suspect a possible misconduct, legal and/or regulatory violation, we encourage you to report this to us as a whistleblowing case. When reporting, it is important that you had reasonable grounds to believe that the information about irregularities that was reported was true at the time of the report. When assessing whether reasonable grounds existed, circumstances and information that were available to you at the time of reporting must form the basis for whether you may have assumed that the misconduct was true. The requirements above must be met in order for you to receive protection under the Whistleblower Act.

2.1 Maladministration in the public interest

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

Examples of misconduct of a serious nature that can be reported:

- Deliberately incorrect bookkeeping, internal accounting control or other financial crime.
- Occurrence of theft, bribery, corruption, vandalism, fraud, embezzlement or data breach.
- Serious environmental crimes or major deficiencies in workplace safety.
- If someone is subjected to 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.

Within our company, we have chosen to also consider all unethical and illegal behavior as irregularities worth whistleblowing. We therefore treat all reports received equally based on the intention of the law and offer protection to everyone.

If the reporting does not meet the criteria of the Whistleblower Act, the law itself cannot offer protection, whereupon we will still provide the same confidentiality and retaliation protection as lawful reporting, provided that the reporting is true and/or made in good faith.

The following are examples of unethical or illegal behavior that could be reported:

- Actions and omissions that go against our culture, vision, goals and values.
- Actions that are contrary to good practice and standards in the labour market.
- Drug and alcohol abuse during working hours.
- Dangerous acts that could cause physical injury to persons or property.
- Discrimination of any kind.
- Abuse of position and/or abuse of power.

2.2 Misconduct contrary to EU law

In addition, there is the possibility to report information about misconduct that has come to light in a work-related context that is contrary to EU legal acts or regulations.

If you suspect that this is occurring, please read [the Whistleblower Act](#) § 2 and the [Whistleblower Directive's scope of](#) application in Article 2 and Annex Part 1 for applicable laws.

3. How do I report?

3.1 Written reporting

In the case of a written case, we use our digital whistleblower function **Visslan**. It is always available through the Concejo website: <https://concejo.se/visselblåsning/>. On the website, you choose to "report" in order to then be able to describe your suspected misconduct.

Please describe what has happened in as much detail as possible, so that we can ensure that adequate measures can be applied. It is therefore also possible to attach additional evidence, in the form of written documents, images or audio files, for example.

3.1.1 Sensitive personal data

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

3.1.2 Anonymity

You can remain anonymous throughout the process without affecting your legal protection, but you also have the option to confess your identity under strict confidentiality. Anonymity may in some cases make it difficult to follow up the case and the measures we can take, but in such cases we may also ask you to confess your identity later under strict confidentiality.

3.1.3 Follow-up & login

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

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

Within **seven days**, you will receive a confirmation that the case manager has received your report. A case manager is the independent party that receives cases in the reporting channel, whose contact information is attached in "6.1 Contact information for case managers". In the future, you and case managers can communicate through the platform's built-in and anonymous chat function. You will receive feedback within **three months** with any measures planned or implemented due to the reporting.

It is important that you, with your sixteen-digit code, log in at regular intervals to answer any follow-up questions the case manager may have. In some cases, the case cannot be taken further without answers to such follow-up questions from you as a 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 case on <https://concejo.se/visselblåsning/>. You then select "Yes" when asked for evidence to be able to upload your file.

In addition, a physical meeting with the case manager can be requested via Visslan. This is most easily done by either requesting it in an existing case, or creating a new report.

3.3 External reporting

We encourage you to always report misconduct internally first, but if difficulties should exist or that it is considered inappropriate, it is possible to conduct an external report instead. We will then refer you to contact the competent authorities or, where applicable, to the EU institutions, bodies, offices or agencies. Contact information for these can be found at the following web address: [https:// www.visslan.com/resources/visselblasarpolicy/extern-rapportering](https://www.visslan.com/resources/visselblasarpolicy/extern-rapportering).

4. What are my rights?

4.1 Right to confidentiality

During the processing of the case, it will be ensured that the identity of you as a reporting person is treated confidentially and that access to the case is prevented by unauthorized personnel. We will not disclose your identity without your consent unless applicable law compels us, and we will ensure that you are not subject to retaliation.

4.2 Protection against retaliation

In the case of whistleblowing, there is protection against negative consequences from having reported a misconduct, in the form of a prohibition of retaliation. The protection against retaliation 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 have a connection with.

This means that threats of reprisals and attempts at reprisals are not allowed. Examples of such are if you were to be dismissed, have your work changed, disciplinary measures imposed, threatened, discriminated against, blacklisted in your industry, or the like because you have whistleblowed.

Even if you were to be identified and subjected to retaliation, 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. Please note, however, that protection is not obtained if it is a crime in itself to obtain or have access to the information that has been reported.

Protection against retaliation also applies to legal proceedings, including defamation, copyright infringement, breach of professional secrecy, breach of data protection rules, disclosure of trade secrets or claims for damages based on civil, public or collective labour law, and you shall not be liable of any kind as a result of reports or disclosures provided that you had reasonable grounds to believe that it was necessary to report or make such information public in order to disclose any wrongdoing.

4.3 Disclosure 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 an 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 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 situation. The same applies when there is a risk of reprisals in external reporting or that it is unlikely that the misconduct will be remedied in an effective way, for example if there is a risk that evidence can be hidden or destroyed.

Please note, however, that this protection does not apply if you as a reporting person disclose information directly to the media in accordance with an otherwise applicable protection system for freedom of expression and information. You therefore still have whistleblower protection and freedom of procurement where applicable.

4.4 Right to review documentation at meetings with case managers

If you have requested a meeting with the case manager, he/she will ensure, with your consent, that the complete and accurate documentation of the meeting is kept in a durable 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 minutes by signing them.

If the call was not recorded, the case manager has the right to document the call through minutes. Afterwards, you will have the opportunity to check, correct and approve the transcription 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 manner.

5. GDPR and handling of personal data

We always do our best to protect you and your personal data. 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 that is not relevant 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. At most, a case will be allowed to be processed two years after its closure. For more information about our handling of personal data, please see <https://concejo.se/privacy-policy/>.

6. Further contact

If you have further questions regarding how we handle whistleblower cases, you are always welcome to contact the case manager.

If you have technical questions about the Visslan platform, feel free to create a case on <https://concejo.se/visselblåsning>. Should this not be possible, contact The Whistle Compliance Solutions AB, which developed Visslan. Contact details can be found below.

6.1 Contact information for case managers

Starck & Partner

Marita Bark

+46 (0)8 40 90 46 48

marita.bark@starckpartner.se

Jesper Wigzell

+46 (0)8 40 90 46 52

jesper.wigzell@starckpartner.se

6.2 Internal contacts

Concejo AB (publ)

Ann-Marie Åström

Chairman of the Board

ami.astrom@concejo.se

+46 707 900 075

Thorleif Jener

VP, business development

thorleif.jener@concejo.se

+46 708 660 213

The above-mentioned internal contact persons may take over the case from the case manager, regardless of whether the case is deemed to be a whistleblower or, for example, a personnel matter.

6.3 Contact information for The Whistle Compliance

Solutions AB

Email: clientsupport@visslan.com

Switchboard: +46 10-750 08 10

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

Visit Visslan's website for more information about Visslan: www.visslan.com