



Whistleblowing Policy

Arise Group

Document Whistleblowing Policy			Type of document Policy
Responsible for the document CEO	Company Arise AB with subsidiaries (Group)	Approved by Group Management	Date approved 2026-01-01

1. Introduction	3
1.1. Purpose	3
1.2. Roles and Responsibilities:	3
2. Who can report?	3
3. What can I report?	3
3.1. Misconduct in the public interest	4
4. How do I report?	4
4.1. Written reporting	4
4.2. Verbal reporting	4
4.3. Physical meeting	4
4.4. External reporting	4
4.1. Follow-up and login	5
4.2. Sensitive personal data	5
4.3. Anonymity	5
5. What are my rights?	5
5.1. Right to confidentiality	5
5.2. Protection against reprisals or retaliation	5
5.3. Publication of information	6
5.4. The right to review documentation	6
6. GDPR and handling of personal data	6
7. Additional contact information	6
7.1. Case Manager	6
7.2. Internal contact persons	7
7.3. Visslan (The Whistle Compliance Solutions AB)	7
8. Definitions	9
Appendix 1	10

Revision history – document is reviewed annually or

Date	Comment
2024-11-29	First version of the document produced.
2026-01-01	Updated to be compliant with the Whistleblowing Act.

1. Introduction

1.1. Purpose

At Arise, we strive to have an open and transparent workplace, where misconduct does not occur. It is therefore important that we provide clear and secure channels for confidential reporting. If you suspect ongoing or past misconduct, it is important that resources are readily available for you to report it. By ensuring an accessible and straightforward reporting process, we work together to build and maintain the trust of our employees, business partners and the general public.

Our cases are initially handled by an external law firm to guarantee independent handling. After the Case Manager's review, our Internal Contact Persons may take over the case, if necessary. The report will never be investigated by anyone who is involved or has any connection to the case. For more information and contact details, please see section 7.1 below.

This whistleblower policy covers the legal entities Arise AB (publ) and its subsidiaries (hereinafter jointly "**Arise**").

For terms used in this policy, please see definitions in section 8 below.

1.2. Roles and Responsibilities:

This policy is owned by the Board of Directors. The CEO is responsible for this policy, which will be reviewed in the event of any relevant changes to legislation. Any questions or comments should be directed to the CEO, HR Manager or Sustainability Manager.

2. Who can report?

You can report misconduct in accordance with this policy if you are an employee, volunteer, intern, or if you work for or represent Arise in any capacity. This includes individuals under our control or management, as well as those who are part of our administrative, management, or supervisory bodies or who active shareholder. 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 misconduct or receiving protection for reporting misconduct in accordance with this policy.

Suppliers, subcontractors and business partners to Arise who have found out about misconduct within Arise can also report.

We will treat all reports in the same way and with the same protections as stated in this policy, even if you may not be covered by the Whistleblower Act.

3. What can I report?

If you suspect possible misconduct or a violation of law or regulation, we urge you to report it to us as a whistleblowing case. When reporting, it is important that, at the time of reporting, you had reasonable grounds to believe that the information you provided about the misconduct was true. The assessment of whether you had reasonable grounds should be based on the circumstances and information

available to you at the time of reporting. Additionally, it is important that the reported issue is indeed a violation that can be reported and therefore eligible for protection against retaliation.

3.1. Misconduct in the public interest

You can report information about misconduct that has emerged in a **work-related context** and that is of **public interest**. For example, you can report serious irregularities or negligence relating to suspected environmental damage, financial crime, systematic discrimination in the workplace, or violations of applicable laws and regulations.

For other personal complaints that are not of public interest, such as disputes or issues relating to the reporting person's own working or employment conditions, we encourage you to contact your immediate manager, HR or another appropriate responsible person. Such matters are normally not covered by the Whistleblowing Act.

You may also report material breaches of the Arise Code of Conduct that are of public interest. Even if such reporting may not reach the requirements of the Whistleblower Act's, we will still provide the same confidentiality and protection against retaliation, provided that the reporting is reasonably believed to be true and made in good faith.

4. How do I report?

For reporting, we use [Visslan](https://arise.visslan-report.se), which is our digital whistleblowing channel available through <https://arise.visslan-report.se>. On the website, you can choose to "report" and then describe the suspected misconduct. Please describe what happened as thoroughly as possible, so that we can ensure that adequate measures can be applied.

4.1. Written reporting

When submitting a report through our digital whistleblowing channel, you can provide a detailed written description of the suspected misconduct. It is also possible to attach additional evidence, in the form of, for example, written documents, pictures or audio files, but this is not a requirement.

4.2. Verbal reporting

It is possible to submit a verbal report by uploading an audio file as an attachment when submitting a report. You do this by selecting that you have evidence for the report, and upload your audio file there. In the audio file, you describe the same facts and details as you had done in a written case.

4.3. Physical meeting

A physical meeting with the Case Manager 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.

4.4. External reporting

We urge you to always report misconduct internally first. However, if internal reporting has not yielded results or if internal reporting is considered inappropriate, you may choose external reporting instead. In that case, we advise you to contact the relevant authorities or, where applicable, EU institutions, bodies or agencies.

4.1. Follow-up and login

After you have reported, you will receive a sixteen-digit code, which you need to access your report at <https://arise.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 has received your report. The Case Manager are the independent and autonomous party that receives reports in the reporting channel. In case of questions or concerns, you and the Case Manager 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 the Case Manager may have. In some cases, the report cannot be processed further without your responses to any follow-up questions from the Case Manager.

4.2. 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, and biometric data used to uniquely identify a person.

4.3. Anonymity

You can be anonymous throughout the process without affecting your legal protection, but you also have the opportunity to state 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 ask you to reveal your identity later, again in strict confidentiality to the Case Manager.

5. What are my rights?

5.1. 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 unauthorised personnel. 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.

5.2. 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.

5.3. Publication of information

Protection also applies to publication of information. This applies if you have reported internally within the company and externally to a government authority, or directly to an external party, 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 is a significant risk to the public interest if it is not made public, such as in an emergency. The same protection applies if there is a risk of retaliation from external reporting, or if it is unlikely that the misconduct will be effectively addressed, for example, if there is a risk of evidence being concealed or destroyed.

5.4. The right to review documentation

If you have requested a meeting with the Case Manager, 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.

6. GDPR and handling of personal data

We ensure that our handling of personal data 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. For more information about our processing of personal data, see Appendix 1 to this policy.

7. Additional contact information

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

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

7.1. Case Manager

Name: Advokatfirman VICI AB

Email: <mailto:visselblasning@vici.se>

7.2. Internal contact persons

HR Manager

Email: <mailto:viktoria.hagg@arise.se>

Sustainability Manager

Email: <mailto:agnes.rottbers@arise.se>

The above Internal Contact Persons may take over the case from the Case Manager, regardless of whether the case is deemed to be a whistleblowing or, for example, a personnel matter. The report will never be investigated by anyone who is involved or has any connection to the case.

7.3. Visslan (The Whistle Compliance Solutions AB)

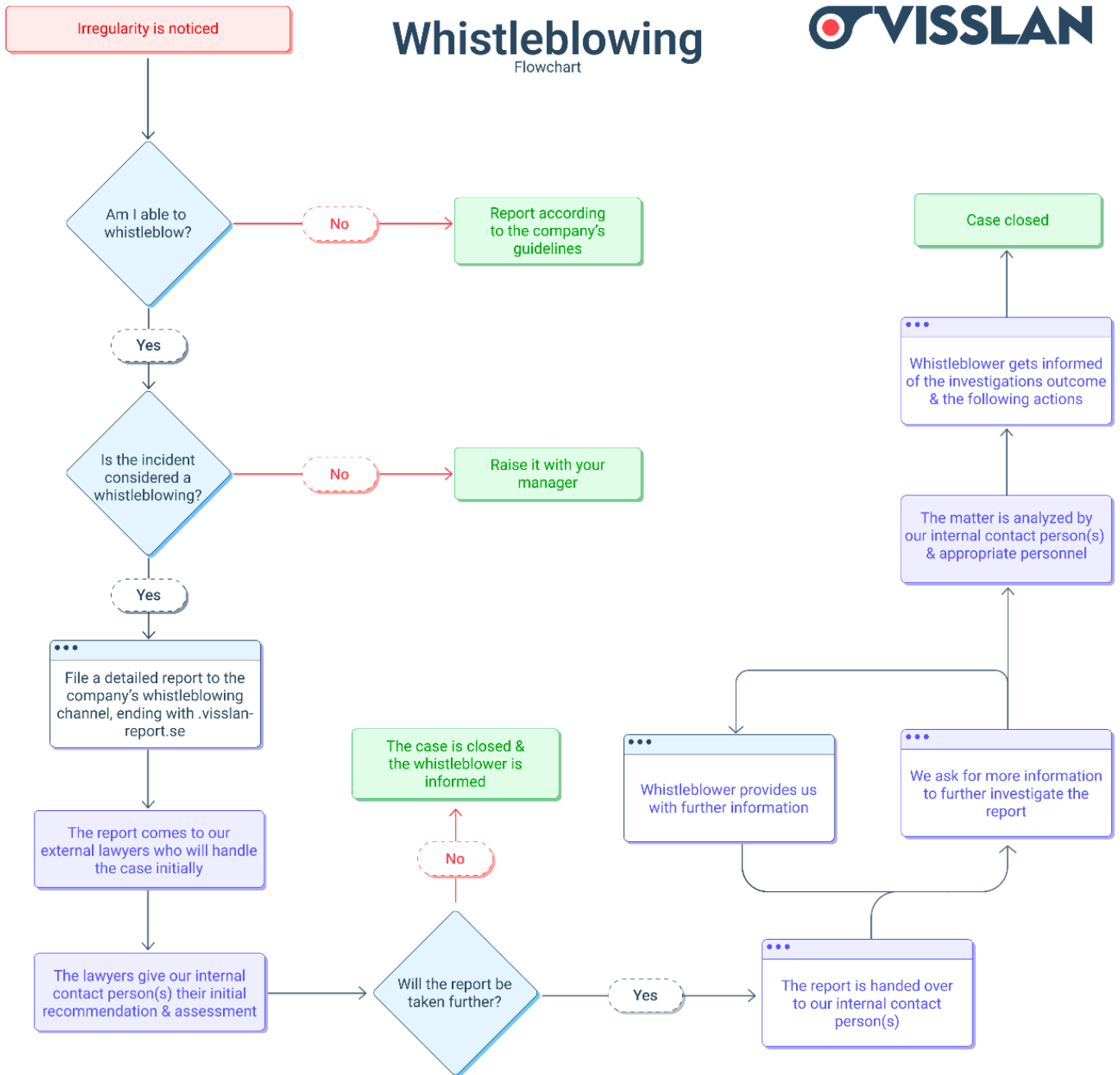
Email: <mailto:clientsupport@visslan.com>

Number: +46 10-750 08 10

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

Whistleblowing

Flowchart



8. Definitions

Arise:	Arise AB (publ) and its subsidiaries.
Case Manager:	The persons listed in section 7.1.
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 of a report to assess the accuracy of the allegations made in the report and, where appropriate, to deal with the reported misconduct, 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.

Appendix 1

Information regarding processing of personal data

Arise AB (publ), reg. no. 556274-6726, is the controller of the processing of personal data within the whistleblowing service. The information in this Appendix is based on the General Data Protection Regulation and other applicable data privacy laws.

The purpose and the legal basis for the processing

The purpose of the processing of personal data in Arise' whistleblowing service is to protect the whistleblower and the organisation in connection with the reporting and investigation of misconduct, irregularities at the workplace and/or criminal activities. The processing is carried out in order to perform a task in the public interest where the processing falls within the scope of the Whistleblowing Act, or on the basis of a balancing interest where Arise' interest in preventing and stopping misconduct and irregularities in the workplace outweighs the individual's rights relating to the protection of their personal data.

Categories of personal data

The personal data that can be processed is data that the whistleblowers give regarding themselves if they choose not to be anonymous, such as for example name and contact details. Through a report, Arise also receives personal data regarding the person or persons that the report relates to, such as for example name, role and contact details.

Recipients or categories of recipients

If a whistleblower reports through the external reporting channel the Case Manager(s) will have access to the data in the report but will not be able to identify the source to the report (unless the whistleblower provides its contact details). The reporting can only be shared, when so required, with external auditor, independent investigator, police, other relevant authority, or persons involved in any criminal or civil proceedings.

Personal data may be processed by third parties, such as Visslan, with whom Arise has entered into data processing agreements.

Rights of the data subject

Each data subject (including the individual who the report concerns) is entitled, free of charge, to request information from Arise regarding the processing of the data subject's personal data. Arise will, at the data subject's request, or on its own initiative, correct or erase any incorrect or misleading personal data, and/or restrict the processing of such data. The data subject may also object to any processing Arise carries out. An application or other inquiries regarding the exercise of the data subject's rights are sent to Arise, see contact information stated in section "Contact details to Arise as controller" below.

Data subjects dissatisfied with Arise's processing of their personal data, should contact Arise at firsthand or submit a complaint to the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, <https://www.imy.se/en/>).

Security measures

Arise takes all appropriate technical and organisational security measures to safeguard the personal data against unauthorised access, alteration or destruction in compliance with the provisions in the General Data Protection Regulation.

Third country

The personal data will not be transferred to and/or processed in a third country (i.e. a country not a member of the EU/EEA).

Deletion and removal of personal data

Reports which are not considered within the scope of the whistleblowing service are immediately deleted after decision of the responsible for the service. Reports which lead to an investigation are saved during the investigation and personal data which have been included in a whistleblowing service are deleted after completed investigation or, if the investigation leads to measures being taken in relation to the registered, when the information is no longer needed for this purpose. Deletion and removal are done in accordance with the General Data Protection Regulation.

Contact details to Arise as controller

If you want to exercise your rights as data subject according to the General Data Protection Regulation or if you have questions about how Arise process your personal data, please feel free to contact us at:

Arise AB (publ)
Reg no 556274-6726
302 50 Halmstad
Sweden
<mailto:info@arise.se>