Anneberg Group Whistleblower policy

The whistleblower policy explains how the whistleblower system works at Anneberg Group. The policy further aims to ensure that potential misconduct reports are not withheld due to a lack of clarity on the whistleblower system.

Anneberg Group Whistleblower system

Anneberg Group has established a whistleblower system following the EU Directive 2019/1937.

Anneberg Group whistleblower system is operated by WhistleSystem ApS, ensuring a completely anonymous and secure process for the whistleblower. The whistleblower system shall be used if employees or other stakeholders experience serious misconduct or offenses in relation to Anneberg Group. Examples of what can be reported are further described in the whistleblower policy under "What can be reported?".

Anneberg Group encourages you to contact your manager about incidents or misconduct. However, this is not always the most optimal approach and can cause reports to be withheld. Therefore, Anneberg Group has established a whistleblower system that, if you do not want or can go to your manager, or simply wish to remain anonymous, makes it possible to still report the offense.

Reports can be made by anyone with access to the system. At Anneberg Group, this includes internal stakeholders who have experienced misconduct.

The whistleblower's report can include people, situations, and incidents. All stakeholders can be reported if the report is relevant under the criteria in "What can be reported?" in this policy and is related to Anneberg Group.

Anneberg Group has appointed the following administrator team:

Thomas Anneberg

What can be reported?

The whistleblower system can only be used to report serious misconduct or violations. Subjects such as cooperation difficulties, dissatisfaction with facilities, or dissatisfaction with conditions cannot be reported through the whistleblower system. In such cases, please refer to your manager.

Examples of subjects that can be reported through the whistleblower system include, but are not limited to, the following points.

- Sexism
- Sexual assault
- Physical violence
- Discrimination
- Financial crime
- Workplace safety
- Consumer protection
- Product Safety
- Breach of procurement legislation
- Breach of GDPR legislation
- Breach of environmental legislation
- Money laundering

However, it is Anneberg Group policy that we would rather have one report too much than one too little, to ensure that we receive all relevant reports. This means that if you are unsure whether you report can be reported under the whistleblower legislation, you are encouraged to submit the report.

How do you report?

Reports are sent through WhistleSystem.

Whistleblowers can access the system and report as follows:

1. Go to Anneberg Group Whistleblower System here:
https://Anneberg.whistlesystem.com/login/7I4PtduA0tm3HAf6rIj

2. Fill the form with the necessary information and documentation, so the administrator team can process the report effectively.
The report is completely anonymous. WhistleSystem is the only channel at Anneberg Group where misconduct can be reported anonymously.

Reports can be submitted by all relevant stakeholders with whom Anneberg Group has shared access information to the system.

After the report is submitted, a unique report ID will appear, which must be saved and kept in a safe place. You can log in and reopen your report with your report ID. This allows you to start an anonymous dialog, send further documentation, and answer clarifying questions from the administrator team. Anneberg Group encourages the whistleblower to log in regularly after the report has been submitted to respond to any follow-up questions.

Please see the user manual for a detailed description of the reporting process.

How are reports processed?

The reports are processed by Anneberg Group administrator team.

The process proceeds as follows:

1. The administrator team will notify the whistleblower that the report has been received within 7 days.
2. The administrator team assesses and categorizes the report and conducts an initial investigation. At this stage, it is possible that the administrator team needs more information or documentation from the whistleblower. The team will start an anonymous dialogue with the whistleblower through the system.
3. The processing of the report is based on the type and severity of the report. Initially, the report is processed internally. In case of particularly severe misconduct or violations, the authorities can be involved in the investigation.
4. The whistleblower is informed of the actions taken within 3 months of the submission of the report. In long-term cases, the whistleblower is updated on a regular basis.
5. The reports are stored for as long as necessary to meet requirements arising from the Whistleblower Act, including registration and documentation obligations. The purpose of the storage may be based on legal evidence or if there is reason to believe that the report may be strengthened by subsequent reports received (linking).

Retaliation

The directive states that whistleblowers cannot be punished for reporting misconduct or violations. Thus, the whistleblower should not be concerned about private or career consequences following the report. If the report is relevant under the Whistleblower Directive, the whistleblower will not be punished by Anneberg Group after submitting the report.

This includes the following penalties (retaliation): Termination, suspension, degradation, failed promotion, change in working time and tasks, a decline in wages, intimidation, harassment, and social exclusion at work.

Anneberg Group whistleblower policy aims to encourage greater transparency and security for all employees and stakeholders.

Security

The system utilizes several security measures that protect the whistleblower and the system in general. Some of these include:

1. Full encryption throughout the process
2. ISO 27001 certified (Information security)
3. ISO 27701 certified (GDPR compliance)
4. ISO 27001 approved servers in Europe
5. Schrems II compliant
6. SSL technology
7. Shield and WAF on the application level
8. Two-factor authentication at administrator level'
9. Redundancy at both application and database level
10. Architecture built on the latest technology
11. Continuous AI monitoring
12. No IP logging

Questions

Questions about Anneberg Group whistleblower system can be directed to:

Thomas Anneberg

External whistleblower channels

We recommend reporting directly to Anneberg Group whistleblower system, as in most cases the report can be processed most effectively internally. However, it is also possible to report to external whistleblower channels provided by the government. These can be found by searching the internet for the relevant government agency name followed by “whistleblower”.

Moreover, external whistleblower channels in the EU, including the European Commission, the European Anti-Fraud Office (OLAF), the European Maritime Safety Agency (EMSA), the European Aviation Safety Agency (EASA), the European Securities and Markets Authority (ESMA) and the European Medicines Agency (EMA).