



Ellab

Whistleblower Policy

Ellab A/S
TROLLESMINDEALLÉ 25
DK-3400 HILLERØD
DANMARK
TLF. +45 4452 0500
FAX. +45 4453 0505

<https://www.linkedin.com/company/ellab>



Index:

1.	Whistleblower Policy	3
1.1	Scope and purpose	3
1.2	Purposes and principles	3
1.3	What can be reported?	3
1.4	How do you report?	4
1.5	How are reports processed?	4
1.6	Retaliation	5
1.7	Security	5
1.8	Questions	5



1. Whistleblower Policy

1.1 Scope and purpose

The whistleblower policy aims to explain how the whistleblower scheme works at Ellab. The policy further aims to ensure that potential misconduct reports are not withheld due to lack of clarity on the whistleblower scheme.

1.2 Purposes and principles

Ellab has established a whistleblower scheme following the EU Directive 2019/1937.

Ellab's whistleblower scheme is handled by WhistleSystem ApS, ensuring a completely anonymous and secure process for the whistleblower. The whistleblower scheme shall be used if employees or other stakeholders experience serious misconduct or offences in relation to Ellab. Examples of what can be reported is further described in the whistleblower policy under "What can be reported?".

Ellab 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, Ellab has established a whistleblower scheme 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 offence.

Reports can be made by anyone with access to the system. At Ellab, this includes both internal and external stakeholders who have experienced misconduct.

The whistleblower's report can include people, situations, and incidents. People who can be reported are all stakeholders if the report is relevant under the criteria in "What can be reported?" in this policy and is related to Ellab.

Ellab has appointed the following administrator team:

- Chairman of the Board: Bo Risberg
- CEO: Ludvig Enlund
- VP HR: Jan Fledelius

1.3 What can be reported?

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

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

- Sexism
- Sexual assault
- Physical violence
- Discrimination
- Economic crime



- Workplace safety
- Consumer protection
- Product safety
- Breach of procurement legislation
- Breach of GDPR legislation
- Breach of environmental legislation
- Money laundering

However, it is Ellab's 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 that your report can be reported under the whistleblower scheme, you are encouraged to submit the report.

1.4 How do you report?

Reports are made in WhistleSystem. Whistleblowers can access the system and report via this link: https://app.whistlesystem.com/login/_CMKUqBlrvD9sFt62Jh

The whistleblower link is even available at www.ellab.com/whistleblower-scheme/ and at the company's intranet Get On Track.

The whistleblower then fills the form with necessary information and documentation, so the administrator team can process the report effectively. The report is completely anonymous. WhistleSystem is the only channel at Ellab where misconduct can be reported anonymously.

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

After the report is submitted, a unique report ID will appear, which must be saved and stored in a safe place. You can log in and reopen the report with your report ID. This allows you to start an anonymous dialog, send any further documentation, and answer clarifying questions from the administrator team. Ellab 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.

1.5 How are reports processed?

The reports are processed by Ellab's 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 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. Any personal information in the report is processed to remain GDPR compliant.
6. The report is deleted from the system when no longer relevant.

1.6 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 punishable by Ellab after submitting the report.

This includes the following penalties (Retaliation):

- Termination
- Suspension
- Degradation
- Failed promotion
- Change in working time and tasks
- Decline in wages

Intimidation, harassment, and social exclusion at work.

Ellab's whistleblower policy aims to encourage greater transparency and security for employees and stakeholders.

1.7 Security

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

1. When reporting, everything is encrypted with industry standard encryption throughout the process.
2. ISO27001 approved servers in North Europe.
3. SSL technology that ensures an encrypted connection between browser and server.
4. Architecture built on state-of-the-art technology and continuously AI monitored to ensure the highest level of security.
5. Multifactor login functionality in the administrator login process.
6. Redundancy ensuring that no data is lost.
7. No IP logging.

1.8 Questions

Questions about Ellab's whistleblower scheme can be directed to:
VP HR Jan Fledelius, jfl@ellab.com, mobile +45 4246 0200