

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>



1.	Whistleblower Policy	3
1.1	Scope and purpose	3
1.2	Purposes, principles and responsibilities	3
1.3	What can be reported?	4
1.4	How do you report?	4
1.5	How are reports processed?	5
1.6	Retaliation	5
1.7	Security	6
1.8	Reporting	6
1.9	Review and approval	6
1.10	Questions	7



1. Whistleblower Policy

1.1 Scope and purpose

The Ellab Group (the "Group" or "Ellab") is committed to promote a professional and ethical business conduct and overall culture in compliance with applicable law and regulations as well as any internal guidelines applicable from time to time. Further, Ellab aims to encourage transparency and security for all employees and stakeholders.

In order to achieve this ambition, the Group has, among other things, established a whistleblower scheme following the EU Directive 2019/1937.

This whistleblower policy (this "Policy") aims to explain how the whistleblower scheme works at the Group. This Policy further aims to ensure that potential reports on misconduct are not withheld due to lack of clarity on the whistleblower scheme.

This Policy applies to the entire Group (noting however that a subsidiary may have an obligation under local law to establish its own whistleblower scheme and policy).

1.2 Purposes, principles and responsibilities

The Group'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 the Ellab. Examples of what can be reported is further described in this Policy under "What can be reported?", cf. section 1.3 below.

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 an 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 may include people, situations, and incidents affecting the Group as further described under "What can be reported?".

Ellab has appointed the following administrator team responsible for e.g. management of the whistleblower reports, including the assessment of whether a reported incident is covered by the whistleblower scheme or not, initiating further investigation (if needed) and deciding on potential reactions and/or disciplinary actions subject to the limitations of authority as laid out in this Policy.

The administrator team of Ellab consists of:

- Group CEO
- VP, HR
- Director, Head of Legal



Ellab's Head of Legal is responsible for ensuring that the whistleblower scheme is established and managed in a way ensuring confidentiality of the identity of the whistleblower, the implicit party and any third party mentioned in the report. Further, the Head of Legal shall ensure that sufficient procedures are in place in order for (i) the whistleblower to receive a notification within 7 days following submission of the report (ii) the effective handling and follow-up on reports, including that sufficient documentation is prepared and (iii) the whistleblower to receive feedback as soon as possible and no later than three (3) months following the confirmation of receipt.

1.3 What can be reported?

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

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

- 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, in accordance with Ellab's strategy and ambition we will rather have one report too many than one too little, to ensure that we receive all relevant reports. This means that if you are unsure whether an incident or concern can be reported under the whistleblower scheme, you are encouraged to submit a report.

1.4 How do you report?

Reports are made in WhistleSystem. Whistleblowers can access the system and report directly via this [Link](#) and via Ellab's intranet Get On Track. Further, the whistleblower scheme is publicly available via the Gorup's public website. WhistleSystem is the only channel at Ellab where misconduct can be reported anonymously.

The whistleblower then prepares the form with necessary information and documentation in order for the administrator team to process the report effectively. The report is completely anonymous.

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 WhistleSystem's user manual for a detailed description of the reporting process. The manual can be accessed on the whistleblower-site.

1.5 How are reports processed?

The reports are processed by Ellab's administrator team, cf. section 1.2.

The process proceeds as follows:

1. Within 7 days, the administrator team will notify the whistleblower that the report has been received.
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 in which case 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 and with strict confidentiality. 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 within GDPR-compliance.
6. The report is deleted from the system when no longer relevant.

As a main rule, the administrative team has full authority to decide on whether or not reactions should be imposed as a result of the investigation. However, local management of the specific Group-company shall always be involved in case of potential disciplinary actions involving an employee of such company. In incidents involving the Group Executive Management, the Board of Directors has the decisive power to impose actions.

If a report concerns a member of Ellab's administrator team, such member will not be notified by the system of the report and will consequently be excluded from the case-handling without knowledge of its existence. Ellab's procedures on how to handle conflicts of interests is further explained under section 1.8 below.

1.6 Retaliation

In accordance with the law, the whistleblower should not be concerned about private or career consequences following a report relevant under the Whistleblower Directive as no punishment or retaliation for reporting misconduct or violations will be imposed whatsoever.

This includes, but is not limited to 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.

The protection against retaliation is – in accordance with the law – subject to the whistleblower being in good faith about the correctness of the reported and alleged circumstances and that the information is encompassed by the law’s field of application. Any deliberate reporting of incorrect information may result in sanctions towards the whistleblower.

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 Reporting

The administrator team reports to Ellab’s Audit Committee at least bi-annually of incidents reported via the whistleblower-scheme. If the reported incident concerns a potential case in an underlying Group-company, local management hereof is also notified of the report. The Board of Directors are also informed ad hoc of any material incidents reported with prior in debt handling hereof by the Audit Committee and annually of the total number, materiality and justification of all reported cases.

In case of severe incidents reported (e.g. in cases involving a member of the Group Executive Board), the chairmanship of the Board of Directors is informed immediately.

Incidents concerning a member of the administrator team is handled without such member being involved whereas incidents concerning a member of the Group Executive Board is reported to – and handled in cooperation with – the chairmanship. Incidents concerning a member of the chairmanship of the Board of Directors is reported to the other members of the Board of Directors.

Finally, reports may only be closed and refused by the joint approval of at least two (2) members of the administrative team.

1.9 Review and approval

This Policy is reviewed annually and updated as necessary subject to approval by the Board of Directors.



1.10 Questions

Questions about Ellab's whistleblower scheme can be directed to Ellab's Head of Legal at: legal@ellab.com.

Approved by the Board of Directors on September 5th, 2024, and enters into force on this date.