# Prevent by Whistleblowing

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

# About

group.one'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 group.one. Examples of what can be reported is further described in the whistleblower policy under "What can be reported?".

group.one 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, group.one has established a whistleblower scheme that, if you do not want or cannot 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 group.one, this includes both internal and external stakeholders who have experienced misconduct.

# Reporting

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.

However, it is group.one'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 you report can be reported under the whistleblower scheme, you are encouraged to submit the report.

## Examples of Subjects

Subjects that can be reported through the whistleblower scheme include, but is not limited to the following points:

- **Sexism**
- **Sexual Assault**
- **Physical Violence**
- **Discrimination**
- **Product Safety**
- **Economic Crime**
- **Consumer Protection**
- **Breach of procurement legislation**
- **Money laundering**
- **Breach of environmental legislation**
- **Workplace Safety**
- **Breach of GDPR legislation**

## How to report?

Reports are made in WhistleSystem. Whistleblowers can access the system and report as follows:

**https://group-one.whistlesystem.com/login/3gqmCagZHn_BbLNWldq**

## How are reports processed?

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

# 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.

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

# Security

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

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