Reporting of Serious Misconduct (Whistleblowing)

Table of Contents

1. Introduction

Preem strives to maintain an open corporate climate and high business ethics. Preem works with continuous improvements. Preem encourages the reporting of violations and irregularities that may affect Preem's interests, Preem’s stakeholders, or the lives and health of individuals.

Preem has established a special whistleblower channel that is available to facilitate the reporting of suspected violations. It is possible to report anonymously.

A person that suspects misconduct that violates the law or where disclosure may be a public interest, can report with protection against retaliation according to the law (2021:890) on protection for persons reporting misconduct.

These guidelines aim to outline which violations can be reported via the whistleblower channel, the statutory protection against retaliation, and how the handling of reporting and investigation is conducted.

2. Protection when Whistleblowing

A reporting person can receive protection in the form of immunity from liability for breaches of confidentiality and protection against obstructive actions and reprisals. The protection related to immunity means that the reporting person cannot be held liable for breaching statutory or contractual confidentiality. This assumes that the reporting person had reasonable grounds to believe that the reporting was necessary to disclose the reported misconduct.

Protection against obstructive actions and reprisals due to reporting covers the reporting person and persons connected to the reporting person, such as a relative or a colleague, or a legal entity that the reporting person owns, works for, or is otherwise connected to.

A preventive measure refers to e.g. persuading a person, through punishment or threat of punishment, not to report misconduct. Reprisals refers to e.g. an action or omission that can cause harm to the reporting person, such as, for example, relocation, dismissal, changed work tasks or hours, threats, warnings, or other unfair or punitive treatment.

The protections related to immunity as well as obstructive measures and reprisals assume that the acquisition of information has not been carried out by committing a crime. To obtain protection under the law, there must be a clear connection between the reprisal and the reporting.

The protection applies if the reporting person at the time of reporting had reasonable grounds to believe that the information was true.

2.1 What Can and Should be Reported via the Whistleblower Channel

To be covered by the protection provided by the law, it is required that the reporting occurs in a work-related context and that it involves misconduct of public interest. A clear example of this is a violation of the law (and in some cases regulations and directives) as it is generally in the public interest for legislation to be followed. Examples of other matters that can be reported (not an exhaustive list):

- Irregularities of an economic nature such as accounting violation, bribery, fraud, and forgery;
- Significant deficiencies in workplace safety;
- Significant violations of environmental regulations and pollution of the environment;
- Serious discrimination and harassment;

Issues related to dissatisfaction in the workplace should be addressed with the manager, either directly or through a union representative, as such matters cannot be treated as whistleblower cases.

Suspected misconduct in Preem Norge A/S is reported according to Norwegian legislation and separate guidelines. Separate guidelines also exist for Drivmedelsstation Preem AB and Bensinstation Preem AB.

A reporting (whistleblowing) person does not need to have evidence for their suspicion. However, no accusations may be made with malicious intent or with knowledge that the accusation is false. A reporting person is protected from retaliation even if the suspicion turns out to be incorrect, provided that the whistleblower acts in good faith.

2.2 Who can Whistleblow?

Whistleblowing with protection is available to you if, in a work-related context, you have received or obtained information about misconduct and belong or have belonged to any of the following categories of persons:

- Employees;
- job applicants;
- persons who are seeking or performing volunteer work;
- persons who are applying for or completing an internship;
- persons performing work under the control and direction of an employee (e.g., hired consultants);
- shareholders who are active in the company;
- self-employed individuals seeking or performing assignments;
- persons who are part of a company's administrative, management, or supervisory body

2.3 How to Whistleblow?

There are different ways to report misconduct or share a suspicion:

Alternative 1: Contact the nearest manager or a higher-ranking manager.

Alternative 2: Communicate through the whistleblower channel wb.2secure.se or via phone at (+46) 77-177 99 77. If a person prefers to remain completely anonymous, the whistleblower channel allows for anonymous communication.

2.4 How is a Report Made in the Whistleblower Channel?

Reports are made in writing via the website wb.2secure.se or verbally by phone at +46 77-177 99 77. You can choose to remain anonymous. If you wish to report via a physical meeting, it can be requested by registering a report on the website wb.2secure.se.

When registering a new report on wb.2secure.se, you must provide the company-specific code "enh472" to identify that the report is for Preem. On the website, you will be asked to answer several questions about the matter being reported. You can remain anonymous. You will be assigned a unique case number and a password that must be saved to actively log in to the website, follow the report, and communicate with the case handler at 2Secure.

When a report is registered, it is handled by experienced case officers at 2Secure, who contact Preem's primary contact person (Preem's Internal Audit Manager) or another contact person based on a predetermined contact list with several names. If the primary contact person is the subject of the report, another person on the contact list will be informed. See further in the section regarding those responsible for receiving reports and investigations. It is always Preem that ultimately assesses the report and decides what actions should be taken.

2.5 The Reporting Tool

To ensure the whistleblower's anonymity, the reporting tool is provided by the external and independent entity 2Secure. The reporting channel is encrypted and password protected.

It is important to describe all facts in the report, including conditions that are believed to be less important, carefully and all documentation that may be relevant should be attached. Information should be provided in good faith and with good intentions.

2.6 Reporting via External Channels

In addition to reporting to Preem's internal whistleblower channel, you can report externally to a competent authority within a specific area of responsibility or to any of the EU's institutions, bodies, and agencies. You are entitled to protection under the law (2021:890) on the protection of persons who report misconduct also when you report externally.

The following Swedish authorities (referred to in Swedish) have been designated as competent authorities and have established external reporting channels: *Arbetsmiljöverket, Boverket, Elsäkerhetsverket, Ekobrottsmyndigheten, Fastighetsmäklarinspektionen, Finansinspektionen, Folkhälsomyndigheten, Havs- och vattenmyndigheten, Integritetsskyddsmyndigheten, Inspektionen för strategiska produkter, Inspektionen för vård och omsorg, Kemikalieinspektionen, Konsumentverket, Konkurrensverket, Livsmedelsverket, Läkemedelsverket, Länsstyrelserna, Myndigheten för samhällsskydd och beredskap,*

Naturvårdsverket, Post- och telestyrelsen, Regeringskansliet, Revisorsinspektionen, Skatteverket, Skogsstyrelsen, Spelinspektionen, Statens energimyndighet, Statens jordbruksverk, Styrelsen för ackreditering och teknisk kontroll, Strålsäkerhetsmyndigheten och Transportstyrelsen. See the Swedish *Arbetsmiljöverket* website for a compilation of each authority's area of responsibility and contact information: https://www.av.se/om-oss/visselblasarlagen/extern-rapporteringskanal/lista-over-myndigheter-med-ansvar-enligt-ansvarsomrade-enligt-forordning-2021949/

Preem encourages reporting primarily through Preem's internal channel to have the opportunity to investigate what has occurred and be able to quickly address any potential misconduct.

3 Receiving Reports and Investigations

3.1 Responsible for Receiving Reports and Investigations

When reporting via 2Secure, the case officer at 2Secure is the initial recipient of reports. The main recipient for whistleblower reports at Preem is primarily the Internal Audit Manager. (The officer at 2Secure contacts the Internal Audit Manager). However, a Whistleblower committee has also been established that jointly takes responsibility for receiving reports and investigations. The Whistleblower committee consists of the Internal Audit Manager, Chief Legal department, and Head of HR and Communications.

If the reporting concerns the CEO or someone directly reporting to the CEO, Preem's Audit Committee will be the recipient and responsible for the investigation. This means that if someone in the Whistleblower committee is involved in the reporting, they will not be informed of or handle the case.

If the reporting person chooses to contact a manager when reporting in accordance with Alternative 1, in Section 2.3 above, instead of direct contact with 2Secure via the whistleblower channel, the manager must ensure that the case is immediately registered in 2Secure's whistleblower channel and handled according to these guidelines. Alternatively, the manager can contact someone in Preem's Whistleblower committee for further guidance.

3.2 Investigations

Upon receiving a report, 2Secure, together with the Whistleblower committee, decides whether it should be classified as a whistleblowing case. If the report is classified as whistleblowing, appropriate measures for investigation are taken. Depending on the nature of the case, others within Preem or external investigators may need to be involved.

The whistleblower committee may reject an investigation if, for example:

- the report does not fall within the scope of these guidelines;
- the report has not been made in good faith or has been made maliciously;
- the matter that the report concerns has already been addressed;
- there is not enough information to investigate the case.

A report that is rejected as a whistleblower case will not be investigated by the Whistleblower committee, nor followed up by Audit Committee, but may instead be handled and investigated within a responsible business area or group function. The report may be forwarded to a relevant senior manager unless any of these are the subject of the report.

3.3 Feedback

After registering a report, the reporting person can log in again with the login credentials to see any follow-up questions/comments from the handler at 2Secure. The report can be followed up via wb.2secure.se if the reporting person has saved the case number and password that were generated when the report was made.

The reporting person shall receive confirmation that the report has been received within seven days of receipt.

The reporting person shall also receive feedback to a reasonable extent on the measures taken in the follow-up of the report and the reasons for these within three months from the confirmation. If applicable, the reporting person shall be informed about details that can identify the reporting person will be disclosed, unless the information hinders or complicates the purpose of the follow-up or the measures.

3.4 Follow-up

Preem's management team reviews the number of registered cases on a quarterly basis, but no individual cases are discussed. The Internal Audit Manager also continuously reports the number of registered cases at an aggregated level to the Audit Committee.

Preem Norge A/S, Drivmedelsstation Preem AB and Bensinstation Preem AB shall continuously report necessary information about serious violations or misconduct reported in the whistleblower system to Preem's Internal Audit Manager.

3.5 Deletion of Data

Personal data included in whistleblower reports and investigation documentation shall be deleted at the conclusion of the investigation, except if personal data should be retained with

reference to other relevant legislation. Deletion occurs within 30 days after the conclusion of the investigation.

Investigation documentation and whistleblower messages that are archived must be anonymized according to the GDPR (General Data Protection Regulation), as these documents must not contain personal data through which individuals can be directly or indirectly identified.

See further Appendix for handling of personal data.

4 Other Matters Regarding Protection and Confidentiality

The individuals identified within the framework of whistleblowing are covered by relevant data protection legislation. Therefore, the identified individuals have the right to access information about themselves and can request correction or deletion of data if the information is incorrect, incomplete, or outdated. This right is subject to the exercise of such right not obstructing the investigation.

5 Information and Accessibility

This guideline shall be available in Preem's management system and on Preem's website.

In case of questions or uncertainties regarding this guideline and the reporting of suspected misconduct, please feel free to contact someone in Preem’s Whistleblower committee.

Revision History	**Approved**
Reporting of Serious Misconduct (Whistleblowing)– Version 2	2025-10-07
Reporting of Serious Misconduct (Whistleblowing - Swedish version 1	2022-07-15

Appendix

When you use the whistleblower service, you can remain anonymous. Preem is very careful to protect personal integrity. Below is a summary of some important points regarding the General Data Protection Regulation.

Personal Data

At all times, Preem is obliged to comply with legislation regarding the handling of personal data. It is important that you feel comfortable when providing information about yourself and others in the whistleblower system. We are very considerate to protect personal integrity.

Anonymity

As a whistleblower, you can choose whether to provide your contact information or remain anonymous. Regardless, all reports are taken seriously. For our external handlers, it may facilitate further work if we can contact you for additional information; therefore, contact details will be requested. However, it is always entirely voluntary to provide this information. No IP addresses are recorded and the system does not use cookies. However, if you use a computer connected to Preem, it may appear in the internet log that you have visited the page where the report is made. If you do not want this to be visible, use a computer that is not connected to Preem's network, or a personal smartphone or tablet.

Data Controller Responsibility

Preem and the respective subsidiary where the reported person is employed are responsible for the processing of personal data in accordance with the law.

Purpose of Registration

The personal data will only be used to investigate of what has been reported to the whistleblower system. In the guidelines for whistleblowing, you can read about the types of misconduct that can be reported. If the misconduct is not serious enough to be handled within the framework of whistleblowing, the case will be closed and all personal data will be deleted. You will receive a notification in the whistleblower system that this assessment has been made and information on actions you may take with your case.

Who has Access to the Personal Data?

Personal data will only be used by the investigative function of Preem's whistleblower committee and by the external company tasked with receiving the report. The data is only accessible to individuals working on the current report. The investigation may be handed over to the police or another authority, such as the Swedish Economic Crime Authority.

What Personal Data is Recorded?

Initially, the information provided by you as the reporter will be recorded. During an investigation, the information needed to investigate the case will be registered, which primarily includes the name, position, and suspicion of the misconduct that forms the basis of the report. Information will then be gathered from the sources deemed necessary to investigate the misconduct.

How Long is the Personal Data Retained?

Personal data is usually deleted three weeks after the case is closed, but no later than 2 years after closure if there are special reasons.

Information to the Reported Person

A person reported in the whistleblower service will receive specific information about it. If it could jeopardize the ongoing investigation, the information will not be provided until it is assessed that there is no longer any such risk. During this time, no register extracts will be provided either.

Register Extract

As a reporter, you have the right to receive information free of charge once a year about what personal data is registered about you in the whistleblower service. Such a request for a register extract must be in writing and signed. Send it to: 2Secure, Data Protection Officer, Box 34037, 10026 Stockholm. If any information is incorrect, incomplete, or misleading, you have the right to have it corrected upon request. A register extract to the reported person will not contain information that could identify you as a whistleblower. The information may therefore be summarized.