

Order Nordic Whistleblowing guidelines

1. Introduction – what is whistleblowing, and why is it important?

Our organisation strives to achieve transparency and a high level of business ethics.

Our whistleblowing service offers a possibility to alert the company/organisation about suspicions of misconduct in confidence. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage.

Whistleblowing can be done by any person openly or anonymously.

2. When to blow the whistle?

The whistleblowing service can be used to alert us about serious risks affecting individuals, our company/organisation, the society or the environment.

The processing may only refer to data about serious improprieties concerning:

- ✓ accounting, internal accounting controls, auditing matters, fight against bribery, banking- and financial crime, or
- ✓ other serious improprieties concerning the company's or the group's vital interests or the life or health of individual persons, as for instance serious environmental crimes, major deficiencies that regard the security at the place of work and very serious forms of discrimination or harassments.

Employees are asked to contact their supervisor or manager for issues relating to dissatisfaction in the workplace or related matters, as these issues cannot be investigated in the scope of the whistleblowing.

A person who blows the whistle does not need to have firm evidence for expressing a suspicion. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service is a serious disciplinary offence.

Please note there could be restrictions on the use of a whistleblowing service in certain countries.

How to blow the whistle?

There are different ways to raise a concern:

- ✓ **Alternative 1** Contact a supervisor or manager within our organisation.
- ✓ **Alternative 2** Contact:
 - ✓ Anna Persson, Finance Department, 070-283 95 82, anna.persson@order.se
 - ✓ Cecilia Lissing Frost, Finance Department, 070-712 40 90, cecilia.lissingfrost@order.se
- ✓ **Alternative 3** Anonymous or confidential messaging through the whistleblower communication channel to the whistleblowing team:
<https://report.whistleb.com/en/ordernordic>

We encourage anybody who shares their suspicions to be open with their identity. All messages received will be handled confidentially. For those wishing to remain anonymous, we offer a channel for anonymous reporting. The whistleblowing channel enabling anonymous messaging is administrated by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB deletes all meta data, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with responsible receivers of report.

3. The investigation process

THE WHISTLEBLOWING TEAM

Access to messages received through our whistleblowing channel is restricted to appointed individuals with the authority to handle whistleblowing cases. Their actions are logged and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process. These people can access relevant data and are also bound to confidentiality.

If a person raises a concern directly to a supervisor, manager or by contacting the whistleblowing team in person the message is treated according to these guidelines.

RECEIVING A MESSAGE

Upon receiving a message, the whistleblowing team decides whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken, please see Investigation below.

The whistleblowing team may decline to accept a message if:

- ✓ the alleged conduct is not reportable conduct under these Whistleblowing guidelines
- ✓ the message has not been made in good faith or is malicious
- ✓ there is insufficient information to allow for further investigation

- ✓ the subject of the message has already been solved

If a message includes issues not covered by the scope of these Whistleblowing guidelines, the whistleblowing team should take appropriate actions to get the issue solved.

The whistleblowing team will send appropriate feedback within 3 (or maximum 6 months) upon the date of receiving the report.

Do not include sensitive personal information about anybody mentioned in your message if it is not necessary for describing your concern.

INVESTIGATION

All messages are treated seriously and in accordance with these Whistleblowing guidelines.

- ✓ No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.
- ✓ The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication.
- ✓ A message will not be investigated by anyone who may be involved with or connected to the misgiving.
- ✓ The whistleblowing team decides if and how a whistleblowing message should be escalated.
- ✓ Whistleblowing messages are handled confidentially by the parties involved.

WHISTLEBLOWER PROTECTION IN THE CASE OF NON-ANONYMOUS WHISTLEBLOWING

A person expressing genuine suspicion or misgiving according to these guidelines will not be at risk of losing their job or suffering any form sanctions or personal disadvantages as a result. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

Subject to considerations of the privacy of those against whom allegations have been made, and any other issues of confidentiality, a non-anonymous whistleblower will be kept informed of the outcomes of the investigation into the allegations.

In cases of alleged criminal offences, the whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

PROCESSING OF PERSONAL DATA

This whistleblowing service may collect personal data on the person specified in a message, the person submitting the message (if not sent anonymously) and any third person involved, in order to investigate facts on the declared misdeeds and inappropriate behaviour eligible under our code of conduct or internal rules. This processing is based on the legitimate interest to prevent reputational risks and to promote an ethical business activity. The provided description and facts under this processing are only reserved to the competent and authorized persons who handles this information confidentially. You may exercise your rights of access, of rectification and of opposition, as well as of limited processing of your personal data in accordance with the local data protection legislation. These rights are subject to any overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and



investigation of the case. For any further questions or complaints please address your request to Anna Persson, Finance Department, 070-283 95 82, anna.persson@order.se.

DELETION OF DATA

Personal data included in a whistleblowing messages and investigation documentation is deleted when the investigation is complete, with the exception of when personal data must be maintained according to other applicable laws. Permanent deletion is carried out 30 days after completion of the investigation. Investigation documentation and whistleblower messages that are archived should be anonymised under GDPR; they should not include personal data through which persons can be directly or indirectly identified.

PERSONAL DATA CONTROLLER:

Anna Persson, Finance Department, 070-283 95 82, anna.persson@order.se is responsible for the personal data processed within the whistleblowing service.

PERSONAL DATA PROCESSOR:

WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm) responsible for the whistleblowing application, including processing of encrypted data, such as whistleblowing messages. Neither WhistleB nor any sub-suppliers can decrypt and read messages. As such, neither WhistleB nor its sub-processors have access to readable content.

4. Legal basis of the Whistleblowing guidelines

This policy is based on the EU General Data Protection Regulation, EU Directive on whistleblower protection and national legislation on whistleblowing.

5. Transfer of personal data outside the EEA

Data is stored within the EU. There is a general prohibition on the transfer of personal data out of the European Economic Area (EEA) unless specific mechanisms are used to protect data.

NB. The scope of this Whistleblowing guideline does not include potential transfer of personal data from the EEA to affiliates located outside the EEA.