COMPONENTA

WHISTLEBLOWING GUIDELINES

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

For Componenta, it is important to promote transparency and good business ethics.

Our whistleblowing service, or whistleblowing channel, allows you to draw the company's attention to suspected misconduct in confidence. It is an important tool for reducing risks and maintaining trust, as it helps us detect potential abuses and respond to them at an early stage.

Anyone can submit a whistleblowing notification with their identity or anonymously.

2. When should I report?

Our whistleblowing service can help us to be aware of serious risks to individuals, businesses, society or the environment.

The whistleblowing channel only deals with serious irregularities that may relate to the following topics:

- Laws and regulations, human rights, accounting, internal controls, audit matters and anti-corruption, banking and financial crimes or
- Other serious violations related to the vital interests of the company or group or the life or health of individuals, including serious environmental crimes, major occupational safety deficiencies and serious discrimination or harassment.

If the issue concerns dissatisfaction in the workplace or similar issues, please contact your manager as these issues cannot be investigated in the whistleblowing process.

The complainant does not need to have solid evidence of the misconduct before notifying the suspicion. However, notifications should be made honestly and in good faith. Misuse of the Whistleblowing channel is a serious violation.

3. How to report?

There are different ways to report a concern:

- Option 1: Report internally to your supervisor or another supervisor
- Option 2: Contact: Componenta Group, Legal/whistleblowing, Teknobulevardi 3–5, 01530 Vantaa
- Option 3: Anonymously or confidentially notify the messaging whistleblowing team via the whistleblowing notification service at: https://report.whistleb.com/componenta.

We encourage anyone who expresses suspicion to openly disclose their identity. All notifications received will be treated confidentially. However, if you want to remain anonymous, you can report anonymously. The whistleblowing channel for anonymous reporting is managed by an external service provider, WhistleB. All messages are encrypted. WhistleB secures the anonymity of the person who submitted the notification by deleting all metadata, such as IP addresses. The person who submitted the notification will also remain anonymous in further discussions with the notification handlers. Dialogue with an anonymous person is possible using the ID and password provided at the end of the notification. The sender of the message can log in to the notification channel with their ID and password and read the response. The dialogue can continue for as long as the parties wish.

4. Investigation process

Whistleblowing Team
Only designated whistleblowing team members have access to listings through our reporting channel. Their activities are logged and all activities are confidential. During the investigation process, the team may request any information and expertise it deems necessary from other individuals. These persons have access to the information relevant to the processing and the confidentiality also applies to them.

If a person reports a concern directly to a manager or whistleblowing team in their own name, the report will be processed in accordance with these guidelines.

Receiving a notification
Upon notification, the whistleblowing team will decide whether to accept or decline the notification. If the notification is approved, appropriate action will be taken for the investigation. See “Finding out what's going on” below.

The whistleblowing team may reject a notification if:

- the alleged misconduct is not a matter to be reported under these whistleblowing guidelines
- the report is not made in good faith or is malicious
- there is not enough information available to allow further clarification
- the issue in the notification has already been resolved.

If a listing contains issues that are not within the scope of the whistleblowing guidelines, the whistleblowing team should take appropriate action to resolve the issue.

The whistleblowing team will provide feedback on the listing three (or a maximum of six) months after the date the listing was received.

Do not include sensitive personal information unless it is necessary to describe the concern.

Finding out what’s going on
All reports are taken seriously and in accordance with these whistleblowing guidelines. The following principles apply to the investigation:

- No member of the whistleblowing team or other person involved in the investigation process attempts to identify the whistleblower in any way
- If necessary, the whistleblowing team will ask follow-up questions through an anonymous reporting channel
- The person who is the subject of the suspicion or who is connected to it is not involved in the investigation of the matter
- The whistleblowing team will determine whether the report will be investigated and how
- All whistleblowing notifications are treated confidentially.

Whistleblower protection when a whistleblowing report is submitted with an identity notification
If a reporter reports genuine suspicion, they are not at risk of losing their job and will not suffer any consequences or personal harm as a result of the report. Any error by the notifier in the state of affairs is irrelevant, provided, however, that he or she acts in good faith.

The reporting person shall be kept informed of the results of the investigation of the allegations made, taking into account, however, the protection of the privacy of the persons subject to the report, as well as other aspects of confidentiality.

In criminal matters, the identity of the whistleblower may have to be disclosed in connection with court proceedings.

Protection of the person identified in the notification and information to be communicated to him/her
The processing of personal data of persons submitting a notification through the whistleblowing notification channel, as well as of the persons subject to the notification, is subject to the data protection legislation in force at the time. The interested parties have the right to access the data concerning them and to request that the data be revised or deleted if the data is incorrect, incomplete or outdated.

The aforementioned rights of the parties may be overridden if the situation requires necessary precautionary measures to prevent the destruction of evidence and other inconveniences to the processing and investigation of the notification.

Deleting data
Personal data contained in whistleblowing notices and explanatory documents will be deleted upon completion of the investigation, unless the retention of personal data is required by other applicable laws. The data will be permanently deleted 30 days after the completion of the survey. The information documents and whistleblowing notices to be archived must be anonymised in accordance with the General Data Protection Regulation (GDPR): they must not contain personal data that can be used to identify a person directly or indirectly.

5. Regulatory background for whistleblowing guidelines

These guidelines are based on the EU General Data Protection Regulation (EU 679/2016), the EU Whistleblower Directive (EU 2019/1937) and national law on whistleblowing.

6. Transfer of personal data outside the EU and EEA

The data is stored within the EU. The transfer of personal data outside the European Union (EU) and the European Economic Area (EEA) is generally prohibited, unless special measures are taken in accordance with applicable regulations and official guidelines to protect the transfer of data.

Note: These Whistleblowing Guidelines do not cover the transfer of personal data to partners outside the EU and EEA.

7. Data Controller and Data Processor

Data Controller
Componenta Corporation, Business ID 1635451-6, Teknobulevardi 3-5, 01530 Vantaa; tietosuoja@componenta.com The controller is responsible for the personal data processed in the whistleblowing channel.

Personal data processor
NAVEX Global UK Limited Address (owner of NAVEX WhistleB system): 1 Queen Caroline Street, Part 4th Floor, Hammersmith, London, W6 9HQ

The personal data processor is responsible for the reporting channel service, including the processing of encrypted data, such as messages intended to reveal misconduct. WhistleB or its subcontractors cannot decrypt and read encrypted messages. WhistleB or its subcontractors do not have access to readable content.