WHISTLEBLOWING GUIDELINES

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

It is important for Componenta to promote transparency and good business ethics.

Our reporting channel i.e. 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, the society or the environment.

The processing may only refer to serious improprieties concerning:

- law and regulation, human rights, accounting, internal 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 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.

3. 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 Legal Affairs/whistleblowing, whistleblow@componenta.com or Componenta Corporation, Legal Affairs, Teknobulevardi 7, FI-01530 Vantaa, Finland
- **Alternative 3**: Anonymous or confidential messaging through the whistleblower communication channel to the whistleblowing team: https://report.whistleb.com/componenta

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. Dialog with anonymous person is enabled by user ID and password provided in the end of message writing process. The sender of the message may sign in the reporting channel with the user ID and password and read the reply. The dialog my continue as long as the parties want.

4. 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 necessary 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. The following principles are applied in the investigation:

- 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 the report is made including the person's identity
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 whistleblower who expresses his or her identity 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.

Protection of, and information to, a person specified in a whistleblower message
The rights of the individuals submitting the message or specified in a whistleblower message are subject to the relevant data protection laws. Those affected will be entitled to the right to access data relating to themselves and should the information be incorrect, incomplete or out of date to require amendments or deletion of data.

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.

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 General Data Protection Regulation (GDPR); they should not include personal data through which persons can be directly or indirectly identified.

5. Legal basis of the Whistleblowing guidelines

This policy is based on the EU General Data Protection Regulation (EU 679/2016), EU Directive on whistleblower protection (EU 2019/1937) and national legislation on whistleblowing.

6. Transfer of personal data outside the EU and 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 in accordance with the valid regulation and authorities' instructions are used to protect transfer of the data.

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

7. Data Controller and Data Processor

Data Controller
Componenta Corporation, business ID 1635451-6, Teknobulevardi 7, FI-01530 Vantaa, Finland; dataprotection@componenta.com

Data Controller is responsible for the personal data processed within the whistleblowing service.

Data Processor
WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm)

Data Processer is 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.