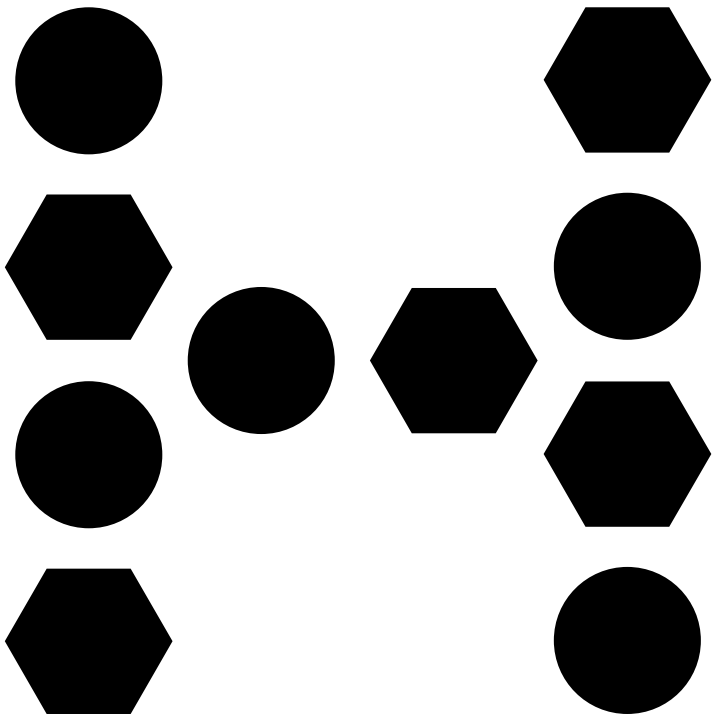
Hexatronic Group

Whistleblowing policy



hexatronic

Content

Introduction – what is whistleblowing, and why is it important?	2
When to blow the whistle?	2
How to blow the whistle?	3
The investigation process	3
Legal basis of the Whistleblowing guidelines	5
Transfer of personal data outside the EEA	5

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

Hexatronic strives to achieve transparency and a high level of business ethics. Our employees are the most important source of insight for revealing possible misconduct that needs to be addressed.

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 openly or anonymously.

The purpose of this Whistleblowing policy is to encourage employees and external stakeholders to blow the whistle on suspected misconduct without any risk of retaliation, as well as to ensure an appropriate investigation process.

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 as regards the security at the place of work and very serious forms of discrimination or harassments.

For issues relating to dissatisfaction in the work place or related matters for example, employees and any other stakeholders are asked to contact their supervisor or manager, 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 are restrictions on the use of a whistleblowing service in certain countries. In Sweden, processing of personal data concerning legal offences may only refer to persons in key positions or a leading position within the own company or group.

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. Anonymous messaging through the whistleblower communication channel:

  https://report.whistleb.com/en/hexatronic

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 (Alternative 2).

The whistleblowing channel allowing 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 does not save IP addresses or other meta-data, (that is data that can be related to the person sending the message). The person sending the message also remains anonymous in the subsequent dialogue with the company/organisation whistleblowing team.

The investigation process

The whistleblowing team

Access to messages received through our whistleblower communication channel is restricted to appointed individuals with the authority to handle whistleblowing cases. The appointed individuals are the chairman of the board of the parent company and the external lawyer of the parent company. 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 inserted into the whistleblowing communication channel and treated according to this policy.

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 this Whistleblowing policy
- 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 this Whistleblowing policy, the whistleblowing team should take appropriate actions to get the issue solved.

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 this Whistleblowing policy.

- 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.

Protection of, and information to, a person specified in a whistleblower message

The rights of the individuals 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 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. Deletion is carried out 30 days after completion of the investigation. Investigation documentation and whistleblower messages that are archived should be anonymised; they should not include personal data through which persons can be directly or indirectly identified.

Legal basis of the Whistleblowing guidelines

This policy is based on the EU General Data Protection Regulation and guidelines on whistleblowing from the Swedish Data Inspection Board.

Transfer of personal data outside the EEA

All 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.

2018-10-29
Henrik Larsson Lyon
CEO Hexatronic Group