Guidelines for Sdiptech's whistleblower program

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 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.

2. When to blow the whistle?

The whistleblowing service can be used to alert us about serious risks affecting individuals, our organisation, the society or the environment, related to for example:

- conflicts of interest in the procurement or conclusion of agreements,
- accounting, auditing, or management of the companies' financial resources,
- fight against bribery and corruption, or
- other serious irregularities concerning the vital interests of the company or the group or the lives and health of individuals, such as environmental crimes, deficiencies in workplace safety and all forms of discrimination and harassment.

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:** Communicate anonymously through the whistleblower communication channel: https://report.whistleb.com/en/sdiptech

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.

4. The investigation process

RESPONSIBLE FOR THE WHISTLE BLOWER SERVICE
Only an external lawyer who is responsible for the whistleblower service has access to messages received through the whistleblower channel. If necessary, people who add expertise can be included in the investigation. These persons have access to relevant data and commit 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 receipt of a message, the person in charge of the whistleblower service decides whether the message should be approved or rejected. If the communication is approved, appropriate measures are taken for investigation, see Investigation below.

The whistleblower service manager may refuse to receive 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 is not covered by these Whistleblowing Guidelines, those responsible for the whistleblower service should take appropriate action to resolve the matter in another way.

Those responsible for the whistleblower service will send appropriate feedback within one (or no more than three) months of receiving the message.

Do not leave sensitive information about people you mention in your message unless it is necessary to explain your suspicion.

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.

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.

DELETING 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.

5. 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.

6. 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.