Guideline to the Whistle Blowing System

Document name	WE GL Guideline for whistleblowing	**Last updated**	19/08/2022
Owner	Chirag Nagpal	**Applies to**	Global

TABLE OF CONTENTS

1 Purpose ____ 3
2 Definition ____ 3
3 When and How can I use the Whistle Blowing System? ____ 3
4 Protection of the Whistle-blower ____ 4
5 Reporting and Dialogue ____ 4
6 Deletion of Data ____ 5

1 PURPOSE

The purpose of this guideline is to describe the We Effect Whistle Blowing System and encourage the public, colleagues, and collaborators to report and communicate all suspected irregularities with full confidentiality.

The Whistle Blowing System is a channel to report deviations from our policies and guidelines. The service decreases the risk of anomalies and is a part of our strategy to improve We Effects Anti-Corruption work. The strategy, including the Whistle Blowing System, shows our commitment to be a trustworthy actor that takes responsibility to prevent and stop unethical behaviour and illegal actions.

2 DEFINITION

A whistle-blower is a person, who could be an employee of We Effect, partner organisation, donor agency, project stakeholder or society in general, disclosing information about any wrongdoing in the whole organisation or a specific department/project. The wrongdoing could be in the form of fraud, corruption, embezzlement, etc. Even those who report anomalies to their managers in their own organisation are counted as whistle-blowers.

3 WHEN AND HOW CAN I USE THE WHISTLE BLOWING SYSTEM?

The Whistle Blowing System can be used when you suspect that our policies and/or ethical guidelines are not complied with, for example:

- Financial irregularities or corruption
- Safety risks at your place of work
- Sexual Exploitation and Abuse and Sexual Harassment (SEAH)
- Other types of harassment (related to gender, sexual orientation, age, etc.)

Open reporting: Primarily, we encourage our employees to talk to their immediate manager or someone in the management group.

Anonymous Reporting: We respect those who want to make their report anonymously. Therefore, we provide a secure channel for anonymous reporting. The channel is provided by an external supplier, WhistleB.

How do I find the system: follow the link: https://report.whistleb.com/weeffect

How is the whistle-blowers anonymity protected?

"The Whistle blowing system is completely disconnected from the employer's IT-system and web services. WhistleB does not save IP addresses or information about the source of uploaded documents. Therefore, we can never investigate the identity of the whistleblower. All reports are highly encrypted and can only be decrypted by individuals chosen by the employer. WhistleB cannot decrypt and read reports." Gunilla Hadders, Founder, WhistleB

4 PROTECTION OF THE WHISTLE-BLOWER

Our co-workers have a key role in detecting irregularities and the Whistle Blowing System should be used to report serious risks for employees, our organisation, the society or the environment. Cases concerning dissatisfaction in the work environment should be raised to immediate manager or Human Resources department.

A person raising a message through the Whistle Blowing System does not need to provide any evidence. No accusations should, however, be made with bad intention or with the knowledge that the accusation is false. The identity of a whistle-blower who comes forward for reporting the suspected wrongdoing is protected.

The whistle-blower will be protected even if the accusation turns out to be wrong, under the prerequisite that the whistle-blower was acting with a correct intention.

5 REPORTING AND DIALOGUE

The whistle-blower reports through an external web-based reporting channel. The service is available in Swedish, English, Spanish, Swahili, Portuguese and Arabic.

The dialogue with the anonymous whistle-blower is enabled by providing a password and ID at the end of the reporting occasion. The whistle-blower can then log in and

read a response from the investigators. The dialogue can last as long as the investigator and the whistle-blower wish.

Only persons in charge of the system, so called investigators, can see the information. Depending on the nature of the case, it can be handled by another authorised person, such as Head of Human Resources.

Persons responsible for the system can reject the message if:

- The message has been made with bad intension or spitefulness
- There is not enough information to handle the message
- The message is not a whistle-blowing case

6 DELETION OF DATA

Personal data included in the message will be deleted within 60 days after closure of the case.