WhistleB
WHISTLEBLOWING CENTRE

Guidelines for whistleblowing

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

RFSU strives to be a transparent organization, that practices what it preaches, in our principles, our core values and at the organizational level in the everyday life in which we operate. Our employees, members and elected representatives play a key role in detecting any irregularities that need to be highlighted and addressed. The same applies to our partners, consultants, clients and recipients of information and support in Sweden and in the countries in which we operate together with our partner organizations.

Our whistleblower service offers an opportunity to confidentially communicate any suspicions of irregularities. The service is important for reducing risks, and for maintaining confidence in our business, by enabling us to detect and address suspected irregularities at an early stage.

Whistleblower reports can be submitted openly or anonymously.

The purpose of these whistleblower guidelines is to encourage submitters to communicate suspected irregularities without the risk of retaliation, and to ensure an adequate investigation process.

2. When can you blow the whistle?

The whistleblower service can be used to draw our attention to serious irregularities and risks that can harm individuals, our organization, society or the environment. This may be linked to, for example, accounting, internal accounting controls, auditing, combating bribery, banking and financial crime, or other serious irregularities related to RFSU, i.e. vital interests or the lives and health of individuals, such as serious environmental crimes, major shortcomings in workplace safety and serious forms of discrimination and harassment.

Issues such as dissatisfaction in the workplace, in the association or related issues must be raised with a supervisor, elected representatives or managers, directly or via a union representative, as these issues cannot be treated as whistleblower issues. A person who

submits a report through the whistleblower service does not need proof of their suspicion. However, no accusations may be made with malicious intent or with the knowledge that the accusation is false.

Whistleblowing in Sweden: Personal data about violations of the law shall only be processed for key or executive personnel in accordance with the guidelines of the Swedish Data Protection Authority.

Do not use the service in the event of emergencies and crimes that involve serious and immediate risks to human life and health, or to buildings and the environment. In such cases, contact the police and emergency services immediately at telephone number 112.

3. How to use the whistleblower service?

There are different ways to report your suspicions:

Option 1: Contact an executive within the organization. This may be: a manager or a chairperson. At national or local level.
Option 2: Contact the manager of the whistleblower service: RFSU's organizational secretary or HR manager. Contact information is available on the website and on the intranet.
Option 3: Communicate anonymously through the whistleblower channel: report.whistleb.com/rfsu

We encourage persons who share their suspicions to be open with their identity. Received reports will be processed confidentially. If a person prefers to be anonymous, the whistleblower channel is available for anonymous communication (Option 3).

The whistleblower channel, which offers anonymous communication, is managed by WhistleB, an external service provider. All reports are encrypted. To ensure anonymity, WhistleB does not store IP addresses or other metadata (i.e. data that can be traced to the person who sent the report). Persons submitting reports will remain anonymous, even during an ongoing dialogue with those responsible for RFSU's whistleblower service.

4. The investigation process

RESPONSIBILITY FOR THE WHISTLE BLOWER SERVICE

Only persons responsible for the whistleblower service have access to reports received through the whistleblower channel. Their activities are logged and their processing is confidential. If necessary, people with specific expertise may be included in the

investigation. These persons will enjoy access to relevant data, and commit to a duty of confidentiality.

If a person makes direct contact regarding a concern with a supervisor, manager or chairperson, or personally contacts those responsible for the whistleblower service, the report shall be directed through the whistleblower channel and processed in accordance with these guidelines.

RECEIVING REPORTS

Upon receipt of a report, those responsible for the whistleblower service decide whether the report shall be approved or rejected. If the report is approved, appropriate investigative measures are implemented. Refer to the Investigation section below.

Those responsible for the whistleblower service will provide full feedback within 3 (or a maximum of 6) months from the date the report was received.

Those responsible for the whistleblower service may refuse to accept a report if:

- ✔ the report does not fall within the scope of these guidelines,
- ✔ the report has not been submitted in good faith or is malicious,
- ✔ there is insufficient information to investigate the matter,
- ✔ the matter to which the report relates has already been resolved.

If a report is not covered by these Whistleblowing Guidelines, those responsible for the whistleblower service shall take appropriate action to resolve the matter.

Do not provide sensitive information about persons you mention in your report unless it is necessary to explain your suspicion.

INVESTIGATION

All whistleblower reports will be treated seriously and in accordance with these guidelines.

- ✔ No person responsible for the service or any other person involved in the investigation process will attempt to identify the whistleblower.
- ✔ Those responsible for the whistleblower service can, if necessary, send follow-up questions through the whistleblower channel for communicating with an anonymous whistleblower.
- ✔ No report shall be investigated by anyone affected by or involved in the case.

- ✔ Those responsible for the whistleblower service shall decide when and how a whistleblower report shall progress.
- ✔ Whistleblower reports are handled confidentially by everyone involved.

PROTECTION FOR WHISTLEBLOWERS WHO OPENLY IDENTIFY THEMSELVES

A whistleblower who reports a genuine suspicion or fear according to these guidelines will not risk losing his/her job or suffer any kind of sanctions or personal damage as a result of their report. It does not matter if the suspicion turns out to be incorrect, provided that the whistleblower has acted in good faith.

Unless it is inappropriate with regard to the named person's integrity and other confidentiality issues, a whistleblower who chooses to state his/her identity will be informed of how the investigation is progressing.

In the event of a suspected crime, the whistleblower will be informed that their identity may be disclosed during court proceedings.

PROTECTION OF, AND INFORMATION FOR, A PERSON NAMED IN A WHISTLEBLOWER REPORT

The rights of persons named in the context of the whistleblower service are covered by relevant data protection legislation. The named persons have the right to access information about themselves and may demand the amendment or deletion of data if the information is incorrect, incomplete or outdated.

This right applies to the extent it does not hinder the investigation or leads to the destruction of evidence.

ERASURE OF DATA

Personal data included in whistleblower reports and investigation documentation must be deleted upon completion of the investigation, unless the personal data must be stored in accordance with other relevant legislation. The data must be deleted no later than 30 days after the investigation has been completed.

Investigation documentation and whistleblower reports that are archived must be anonymised, and they must not contain personal data through which persons can be directly or indirectly identified.

5. Legal basis for the guidelines

These guidelines are based on the Data Protection Ordinance, the GDPR and the Swedish Data Protection Authority's guidelines.

6. Transferring personal data outside the EEA

All data is stored within the EU. There is a general ban on the transferring of personal data from the European Economic Area (EEA) unless specific provisions on data protection can be guaranteed.