Stockholm 07.02.2023

Created by Amelie Geijer

Whistleblower Policy

Swedish Institute of International Affairs

UTRIKESPOLITISKA INSTITUTET
The Swedish Institute of International Affairs

Postal address: Box 27035, SE-102 51 Stockholm
Visiting address: Drottning Kristinas väg 37
Tel: +46 8 511 768 00 Fax: +46 8 511 768 99
info@ui.se www.ui.se

Org.nr 802005-9518. VAT.nr SE802005951801
Plusgiro 15 93 55-7 Bankgiro 569-3254

1. Purpose

Wrongdoings can occur in all organisations, despite efforts to prevent them. And even in the best of organisational cultures, there can be a reluctance or even a fear among employees to report something that may be a wrongdoing that has been detected. An employee may feel that they are somehow letting the side down if they 'tell on' a colleague or manager. The employee might be scared of damaging their own career prospects as a result of retaliation such as smaller pay rises, poorer promotion opportunities or less favourable assessments and references.

The Swedish Institute of International Affairs (UI) considers that it is part of employees' duty of loyalty to report wrongdoings. By ensuring an open organisational culture characterised by accountability, UI can investigate and remedy wrongdoings, hopefully at an early stage, and in doing so eliminate or minimise internal and external damage. This helps UI to learn, create better working methods and achieve an even more effective organisation. The interests of UI and those of its employees, its owners, the industry and the public alike are protected. Having a whistleblower system in place may also be a matter of credibility in itself, both inwardly and outwardly.

The purpose of this policy is to clarify the possibilities that exist for raising the alarm in the event that wrongdoings are perceived within the organisation ('whistleblowing') and ensure that employees feel safe reporting wrongdoings without having to fear any negative consequences. It also aims to ensure that employees' reports are taken seriously and treated in a professional and confidential manner. The policy is based on the rights and obligations stipulated in the *Act on the Protection of Persons Reporting Irregularities (2021:890)* (hereinafter referred to as the 'Whistleblower Act'), which in turn is based on the EU Whistleblower Directive.

2. The 'Whistleblower Act'

2.1 General information

The 'Whistleblower Act' entered into force on 17 December 2021 and applies to all employers.

A whistleblower (referred to as the 'reporting person' in the Act) may not be prevented from reporting wrongdoings and must be protected against retaliation. Whistleblowers have the right to report directly to a public authority and in some cases also the right to make public the wrongdoings as a last resort.

2.2 Who is protected by the Whistleblower Act?

A whistleblower is protected by the Whistleblower Act if they have, in a work-related context, accessed or gathered information about wrongdoings and reported them. The whistleblower must also belong to one of the following categories: employees (including temporary staff and staff of contractors/suppliers), jobseekers, self-employed people, shareholders, people in an organisation's management or oversight bodies, interns and volunteers. Whistleblower protection also covers people who have belonged to one of the categories above and accessed the information at that time.

In addition to the whistleblower, protection also applies to people who assist the whistleblower in reporting, people who are associated with the reporting person, and legal persons that the reporting person owns, works for or in any other way has a work-related association with.

2.3 What can be reported?

The whistleblowing is to refer to wrongdoings that have occurred or are highly likely to occur in the activities in which the reporting person is/has been/may in future be involved or in other activities with which the reporting person is in contact or has come into contact through their work.

There must be a public interest in the disclosure of the reported wrongdoings or the wrongdoings must be breaches of EU law. (The Whistleblower Act does not apply to activities classified as secret or information concerning national security.)

Whistleblower protection does not normally cover an employee's grievances concerning their own working conditions and terms of employment.

To be covered by whistleblower protection, the whistleblower must have had reasonable cause to believe that the information about the wrongdoings was true at the time of reporting.

2.4 What does whistleblower protection entail?

A whistleblower must not be made responsible for having disregarded their duty of confidentiality as long as the person at the time of reporting had reasonable cause to assume that reporting the information was necessary to reveal the reported wrongdoing. The kind of duty of confidentiality that may be disregarded is such that follows from contracts (such as employment contracts and collective agreements), management decisions and unqualified confidentiality by law.

Qualified confidentiality means that the right to report information does not apply pursuant to the *Public Access to Information and Secrecy Act (2009:400)*; it may not be disregarded under the protection of the Whistleblower Act. Nor is it permitted to disregard a duty of confidentiality under the *Defence Inventions Act (1971:1078)*.

Nor does the Whistleblower Act give whistleblowers the right to disclose documents.

A whistleblower must not be made responsible for having breached provisions that apply to the gathering of information if the person, when gathering the information, had reasonable cause to assume that it was necessary to gather the information in order to reveal the reported wrongdoing. However, this freedom from responsibility does not apply if the whistleblower commits a criminal offence by gathering the information.

Employers are not permitted to prevent/attempt to prevent whistleblowers from reporting wrongdoings.

Employers are not permitted, because of reporting, to take retaliatory action against:

- a whistleblower;
- a person at the place of employment who assists the whistleblower (such as an elected representative or a safety representative);
- a person at the place of employment who is associated with the whistleblower (such as a relative or a colleague); or

- a legal person that the reporting person owns, works for or is otherwise associated with.

Employers must not take retaliatory action because someone consults their employee organisation for advice on reporting; nor are employers permitted to obstruct or attempt to obstruct such consultation.

A person who commits a criminal offence by reporting or gathering information is not protected against retaliation.

2.5 How is reporting done?

Reporting should primarily be done through an **internal channel** (the employer's own whistleblower system) or an **external channel** (a competent Swedish authority or an EU body) and alternatively through public disclosure.

The internal channel must enable the whistleblower to:

- report both in writing and orally, and in a physical meeting that is held within a reasonable period of time;
- receive confirmation within seven days that the report has been received, unless the whistleblower has stated that they do not require confirmation or the recipient of the report has reason to assume that confirmation would reveal the person's identity;
- receive feedback to a reasonable extent on the measures that have been taken and the reasons for these, within three months of receiving confirmation or – if no confirmation was given and this was not due to the whistleblower – within seven days of the report being received; and
- be informed that information that might identify the reporting person is to be disclosed, unless informing them would jeopardise the purpose of disclosing the information (for example, a legal obligation to disclose information in connection with an inquiry by a public authority or legal proceedings).

It is important that the employer's internal reporting channel provides the option of anonymous reporting, for example by ensuring internal and external information security and preventing the possibility to trace IP and email addresses.

Whistleblower protection also applies if a person reports internally using a method other than the internal channel if:

- there is no internal channel or it does not meet the legal requirements; or
- the person reports wrongdoings before having started within the activities in question.

The annex to the *Ordinance on the Protection of Persons Reporting Irregularities (2021:949)* states which authorities are competent external report recipients. In general, the authority that is normally responsible for supervision is also the competent whistleblower authority. The Swedish Work Environment Authority is the competent authority regarding wrongdoings that do not fall under any other competent authority's area of responsibility and is also the national coordinating authority (special competent authority).

In the event of external reporting, reports may also be made to a non-competent authority if:

- internal reporting has not resulted in reasonable measures or a reasonable response within three months;

- there is reasonable cause to assume that the wrongdoing constitutes an imminent or obvious danger to life, health or safety, or entails a risk of extensive damage to the environment, or, for other reasons, there is justifiable cause to report; or
- there is reasonable cause to assume that reporting internally would entail a risk of retaliation or result in the wrongdoing probably not being effectively addressed.

Alternatively, reporting may be done through **public disclosure**, meaning that information about breaches is made available to the public, for example through traditional media, online platforms, social media, elected representatives, civil society organisations, trade unions, professional organisations or industry associations.

Public disclosure may take place with the protection of the Whistleblower Act if:

- external reporting has not resulted in reasonable measures or a reasonable response within three months;
- external reporting would entail a risk of retaliation or result in the wrongdoing probably not being effectively addressed;
- there is an imminent or obvious danger to life, health or safety, or a risk of extensive damage to the environment; or
- there is justifiable cause for other reasons.

The Whistleblower Directive (and therefore also the Whistleblower Act) is based on the premise that the public disclosure of information should generally be avoided in favour of other reporting channels and that public disclosure should be used as a last resort.

2.6 Appointed recipient of reports

Employers are to appoint one or more independent and autonomous individuals (or units) to:

- receive reports and have contact with the whistleblower;
- investigate what has been reported;
- pass the investigation to the competent internal body for a decision on measures to be taken; and
- provide feedback to the whistleblower about measures that have been planned or taken and the reasons for these.

The report recipient must hold a position that does not entail any conflict of interests. They may be a person who is employed by or associated with the operator (such as a compliance officer, human resources manager or officer, or a member of the board), or employed by someone who has been engaged for the assignment (such as an accountant, lawyer or company providing external reporting platforms).

Only authorised staff are permitted to have access to personal data that is processed in a whistleblower case. Access to personal data is to be limited to what each individual needs in order to complete their tasks. A person dealing with a whistleblower case is not permitted, without authorisation, to divulge information that could reveal the identity of the reporting person or any other individual involved in the case.

Chapters 7 and 8 of the Whistleblower Act state how personal data can be processed and how reports can and should be documented, stored and culled.

2.7 Information to employees

Employers must document their whistleblower channels in writing and make them known internally so that employees are aware how to proceed with whistleblowing. Employees must also be made aware of how they can report to competent authorities.

Employers must also provide information about protection when reporting information – if the activities are covered by these rules. Protection when reporting information means that:

- all citizens have the right to report information: the right to contact the media and disclose information for publication;
- all citizens have the right to anonymity, meaning that a person who receives a media tip-off is not permitted to reveal the source if the source wishes to remain anonymous; and
- public authorities are not permitted to seek to identify who has disclosed information (prohibition on seeking to identify sources) and public authorities are not permitted to punish a person who has disclosed information (retaliation prohibition).

People employed by a private organisation such as UI do not enjoy the protection afforded by the prohibition on seeking to identify sources and the retaliation prohibition; instead, they are bound by a duty of loyalty to their employer.

3. Internal reporting at the Swedish Institute of International Affairs

The following officers are responsible for receiving reports of wrongdoings in accordance with Chapter 5, Section 5 of the Whistleblower Act:

Monica Haglund, Head of Administration. Tel.: +46 851176810. Email: monica.haglund@ui.se
Postal address: Monica Haglund, Utrikespolitiska institutet, Box 27035, 102 51 Stockholm.

Helena Berger, Human Resources Manager. Tel.: +46 765519266. Email: helena.berger@ui.se
Postal address: Helena Berger, Utrikespolitiska institutet, Box 27035, 102 51 Stockholm.

If the officer responsible for receiving reports is directly involved in what is being reported, a report may instead be sent to the most senior operations manager:

Jakob Hallgren, Director. Tel.: +46 851176802 Email: jakob.hallgren@ui.se
Postal address: Jakob Hallgren, Utrikespolitiska institutet, Box 27035, 102 51 Stockholm

Reports can also be sent to the following email address: whistleblower@ui.se

If a whistleblower wishes to remain anonymous when reporting via email, they should create an email address that conceals their identity, such as outlook.com, icloud.com, gmail.com, hotmail.com or similar. UI does not have the technical ability to trace such email senders and will also refrain in other regards from seeking to identify the whistleblower if they wish to remain anonymous (given, of course, that the whistleblower is covered by the protection of the Whistleblower Act).

UI may need to ask the whistleblower additional questions while investigating the case. When reporting, the whistleblower should state whether or not they are available for such questions. The whistleblower should also state whether or not they would like to receive feedback on any measures taken and the reasons for these.

All reports received will be shared with the board.

UI will ensure that the reported wrongdoing is investigated with the necessary level of discretion and the appropriate protection of the personal data involved in the case. If it is considered that the investigation would be better dealt with by an external party – for example, in the event of conflicts of interest, for reasons of credibility or because expert knowledge is required – such a party will be engaged for the task.

UI will decide which measures should be taken on the basis of the investigation results. The whistleblower will receive feedback on the measures taken and the reasons for these if they can be contacted and wish to receive such feedback.

In the event of external reporting, the competent authorities have reporting channels on their websites that can be used. The following authorities are competent authorities for UI's activities:

- The Swedish Work Environment Authority www.av.se/om-oss/visselblasarlagen