Whistleblowing Policy

Stegra AB and subsidiaries

Content

Stegra encourages employees and other stakeholders to report in good faith suspected or actual criminal conduct, unethical conduct, or other misconduct by or within Stegra.

1. Purpose

Stegra AB as well as its subsidiaries and affiliated companies ("**Stegra**") are committed to upholding ethical conduct, as outlined in the Code of Conduct, Supplier Code of Conduct, and other related policies as well as applicable laws and regulations.

This Whistleblowing Policy (this "**Policy**") and an effective whistleblowing process is of vital importance to:

- protect Stegra' and its stakeholders' integrity and reputation,
- comply with legal obligations,
- prevent financial loss and regulatory sanctions,
- ensure a fair and non-discriminatory work environment,
- safeguard against criminal or unethical behaviour;
- safeguard the privacy of whistleblowers and individuals involved; and
- safeguard whistleblower's right not to be retaliated against.

Stegra encourages a strong speak-up culture and in order to allow individuals to raise concerns, Stegra has established an internal reporting channel (the "**Whistleblowing Channel**") that serves as a contact interface designed specifically for receiving and handling reports on certain serious irregularities.

2. Scope

This Policy applies to Stegra as well as Stegra's employees, consultants, or other contractors and/or persons acting on behalf of Stegra.

3. Policy statement

3.1 What you can report about

When using the Whistleblowing Channel, you may only report information on work-related irregularities or suspected misconduct, in which there is a public interest in them being resolved. The information may also refer to suspected violation of certain EU rules.

In practice, this means that irregularities or suspected misconduct that may be reported in the Whistleblowing Channel includes:

- Serious criminal activity;

- Fraud-related crime (such as misrepresentation, violations of internal control procedures, misappropriation of assets or fraud);
- Briberies and corruption (such as offering or receiving bribes);
- Violations of money laundering or terrorist financing laws;
- Violations of competition law (for example, exchange of price-sensitive information, illegal collusion between competitors) or public procurement law;
- Serious environmental risks or crimes;
- Violations of privacy and personal data protection laws and network and information system security;
- Security and safety vulnerabilities which constitute a risk for employees', customers' or others health or safety;
- Other activities that are considered serious and inappropriate, such as discriminatory work practices and harassment;
- Other serious and/or unethical conduct, such as the use of child labour, other improper exploitation of labour and violations of human rights;
- Serious violations of Stegra's Code of Conduct; and
- Other serious negligence concerning Stegra's essential interests or the life and health of individuals.

You don't need evidence to file a report in the Whistleblowing Channel, but you should have reasonable grounds to believe that the information you report is true.

The circumstance that the information in a report must be of public interest to be investigated means that the following situations should be reported to your manager or People & Organization, not be reported through the Whistleblowing Channel:

- General expressions of dissatisfaction;
- Alcohol and drug related concerns;
- Minor thefts at work; and
- Minor accidents and incidents.

Irregularities that only affect one individual, such as the reporting person themself, should typically not be reported in the Whistleblowing Channel.

If the Whistleblowing Team receives a report that is deemed to fall outside the scope of the Whistleblowing Channel, your report will be handed over to the relevant function or you will be guided to the right means of reporting your concern.

3.2 How to submit a report through the Whistleblowing Channel

The Whistleblowing Channel, which enables anonymous communication, is managed by the external service provider Scutus Solution AB (“**Scutus**”). Scutus is certified by ISO 27001 – the international standard for information security – and meets all requirements for information security.

There are different ways to report misconduct:

- Option 1: Report via this link: https://h2greensteel.system.scutus.se/whistleblower/form
- Option 2: Call Scutus hotline and just say “whistle-blower” and you will be referred to an investigator. Phone number: +46 8 20 40 00
- Option 3: Send an email to whistleblow@scutus.se
- Option 4: Contact a supervisor or manager within the organization for guidance.

Note: You can also schedule a private meeting with an investigator in option 2 and 3. In such a case, you have the right to a meeting no later than one week from your request.

Examples of information to include in your report include the date, time and place of the event; names and positions of persons concerned; a description of what has happened, and other useful information to understand the event and to process your report; and witnesses.

To make it easier for us to investigate your report, we encourage you to be as specific as possible. If the information you provided is too general, you may be asked to provide additional information.

When you file a report, try not to include sensitive personal information, such as information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation, if it is not necessary to describe your concern.

3.3 How your report will be handled

3.3.1 The Whistleblowing Team

All reports logged through the Whistleblowing Channel are handled and investigated by Stegra whistleblowing team comprising of the Chief People Officer, Head of Legal Affairs, Ethics & Compliance Manager and Head of Safety and Security (the “**Whistleblowing Team**”).

The members of the Whistleblowing Team are designated as competent to, on Stegra’s behalf and in an independent and autonomous manner, receive reports,

follow-up on reports (investigate), and maintain contact with the person submitting the report.

All cases received by the Whistleblowing Team are treated in accordance with the following principles:

- No one from the Whistleblowing Team or others involved will attempt to identify an anonymous whistleblower.
- Any member of the Whistleblowing Team or any other individual who assists in an investigation who has an interest in the case will be excluded from the handling of such case.
- All cases are handled strictly confidentially.
- All cases are investigated rigorously and with the assistance of external advisors if necessary.

The Whistleblowing Team will not open an investigation if:

- the alleged conduct falls outside the scope of this Policy,
- the case has a malicious intent or was not made in good faith,
- the information is not sufficient for further investigation,
- the case has already been resolved.

3.3.2 Receiving and assessing the report

You will receive confirmation that the Whistleblowing Team has received your report within **seven days** from submitting it. Confirmation will not be provided if you have declined such confirmation, if there is reason to believe that a confirmation could reveal your identity, or where you have not provided any means to contact you.

Initially, the Whistleblowing Team will assess whether the reported irregularity may be reported in the Whistleblowing Channel. If your report falls outside the scope of the Whistleblowing Channel, you will receive a message within **seven days** of receipt of your report, with further information on where to turn instead. Your report will then be deleted.

3.3.3 Investigating the reported concern

If the report concerns irregularities that may be reported in the Whistleblowing Channel, the Whistleblowing Team will investigate the reported irregularities and, where relevant, address the breaches reported. If you choose to be open with your identity or have provided other contact details, the Whistleblowing Team may contact you to ask further questions.

Investigations may require the involvement of other internal functions or external expertise, such as IT expertise, legal counsel, or forensic investigation firms. Where applicable, the Whistleblowing Team will inform you if information on your identity will be disclosed, unless such information impedes or obstructs the purpose of the measures.

Where appropriate, matters raised may be referred to the police or other law enforcement authorities, an independent auditor, or become the subject of an independent inquiry.

3.3.4 Feedback on the report

The Whistleblowing Team will, within **three months** of the confirmation of the report, give you reasonable feedback on measures taken in the follow-up of your report and on the reasons for those measures.

If the investigation of the report is not completed within the time limit of providing feedback, you will receive information that the investigation is still ongoing and on what actions have been taken and are planned to be taken.

You will also receive a notice when the investigation is complete. The notice will not necessarily contain the outcome of the investigation.

3.4 Your rights and protections when reporting

3.4.1 Anonymity and confidentiality

You can report anonymously through the Whistleblowing Channel, but we encourage you to be open with who you are. It normally makes the investigation easier if you provide your name and contact details.

Your identity and any reported person will be treated with strict confidentiality. The Whistleblowing Team will not disclose information that could reveal your identity, or any other person involved in the case, without being authorized to do so. If information that could reveal your identity is disclosed to an authorized recipient, you will be informed of this, unless it impedes or obstruct the purpose of the measure.

All messages sent through the Whistleblowing Channel are encrypted and no IP-addresses or other data, that can be traced back to the sender, are saved.

3.4.2 Non-retaliation

Stegra has a strict non-retaliation policy for all who in good faith reports about suspected misconduct. Stegra will not tolerate any attempt to penalize or discriminate against anyone who has used the Whistleblowing Channel to report a genuine concern regarding wrongdoing. No reprisals may also be taken against a person who assists you in your reporting (for example, a colleague or a safety representative) or against a company that you own, work for or otherwise have a connection with.

If you believe you have been subjected to restrictive measures or retaliation, you should report this in the Whistleblowing Channel as soon as possible.

3.4.3 Further legal protection under the Swedish Whistleblowing Act

If you are considered a “reporting person” under the Swedish Whistleblowing Act (Sw: *Lag (2021:890) om skydd för personer som rapporterar om missförhållanden*)

and you report in accordance with this Policy, you are further protected against retaliation and restrictive measures according to applicable legislation.

Reporting persons includes employees, volunteers and trainees (including persons who are applying for, or have formerly held, any of these positions), members of the board of directors, consultants or shareholders. You are also considered a reporting person if you previously have belonged to any of the above categories and have received or obtained information during this time.

If you, in gathering information or reporting, commit a crime (for example, theft, illegal intrusion or data breach), you are not protected against reprisals.

If you are a reporting person and report an irregularity in the Whistleblowing Channel you will not be held liable for breach of confidentiality for collecting the reported information, if you had reasonable grounds to believe that it was necessary to file the report to uncover the irregularity. There are some exceptions to this in applicable law. Please note that the protection from liability does not include a right to disclose documents.

3.5 Reporting in external channels and through public disclosure

3.5.1 Reporting to relevant authorities' external reporting channels

In view of the EU Whistleblowing Directive, EU member states, including Sweden, have defined designated authorities that also accepts reports on misconduct as "external reporting channels".

The rights and protections in Section 3.4 above, applies also if you chose to report a concern to the Swedish authorities' external reporting channels. If you want to file a report to an authority, you should contact the authority designated to receive reports on the relevant matter directly.

A list of competent authorities, their areas of responsibility and details on how to report in the external reporting channel can be found at the website of the Swedish Work Environment Authority (Sw: *Arbetsmiljöverket*), accessible here (in Swedish) https://www.av.se/om-oss/visselblasarlagen/extern-rapporteringskanal/lista-over-myndigheter-med-ansvar-enligt-ansvarsomrade-enligt-forordning-2021949/.

3.5.2 Freedom to collect and disclose information

In addition to what is stated above on the possibility to report irregularities through external reporting channels, the Freedom of the Press Act (Sw. *Tryckfrihetsförordningen*) and the Freedom of Expression Act (Sw. *Yttrandefrihetsgrundlagen*) contain provisions on the right to provide information for publication in certain media (freedom of information) and the right to acquire information for the purpose of notifying it for publication in certain media (freedom of acquisition). Since Stegra is a private company, these freedoms are limited by, among other things, contractual obligations of confidentiality (confidentiality obligations) and general principles regarding the duty of loyalty in employment relationships on the private labour market.

4. Roles and responsibility

All persons using the Whistleblowing Channel are responsible for adhering to this Policy when submitting their report.

All employees of Stegra, and managers especially, are responsible for upholding the principles of and ensuring adherence to whistleblower's right to protection against retaliation.

The Whistleblowing Team is responsible for ensuring adherence to the process of receiving and investigating a report.

5. Monitoring of compliance

Document Owner will monitor the compliance of this Policy by annually reviewing the effectiveness of the Whistleblowing Channel, that the Whistleblowing Team follows established processes and that the external provider of the Whistleblowing Channel follows established processes.

6. Definitions

Abbreviation or term	Explanation
Policy	This Whistleblowing policy.
Scutus	Scutus Solution AB, the external service provider of the Whistleblowing Channel.
Stegra	Stegra AB and its subsidiaries.
Swedish Whistleblowing Act	The Swedish law on protection against retaliation for persons reporting misconduct, including requirements on companies with 50 or more employees to implement whistleblowing channels. In Swedish *Lag (2021:890) om skydd för personer som rapporterar om missförhållanden*.
Whistleblowing Channel	Stegra's internal reporting channel for reporting serious misconduct.
Whistleblowing Team	The group of persons designated as competent to, on Stegra's behalf and in an independent and autonomous manner, receive reports, follow-up on reports (investigate), and maintain contact with the person submitting the report.

7. References to associated documents

This policy relates to the following policies:

- Code of Conduct
- Supplier Code of Conduct
- Internal Data Protection Policy

8. Revision history

Revision	Date	Description of revision	Author(s)
1	2022-04-27	Created	Sofia Gellar, Chief People Officer

2	2023-11-01	Rewritten based on set up with external partner Scutus	Sofia Gellar, Chief People Officer
3	2025-02-21	Formatted according to new policy template, inclusion of information about external reporting channels, processing of personal data, non-retaliation, and clarification of what may be reported.	Lisa Ejelöv, Ethics & Compliance Manager

Annex 1 - Information about the processing of your personal data

1. Contact details to the controller

Stegra is the controller of any personal data collected via the Whistleblowing Channel. As controller, Stegra is responsible for ensuring that the personal data collected is processed in accordance with applicable laws and regulations on data protection. The contact details of Stegra for purposes of its role as controller are as follows:

H2GS AB, 559272–3000

Norra Stationsgatan 93A, 113 64 Stockholm

Contact: privacy@stegra.com

2. Categories of personal data and of data subjects

Reports made through the Whistleblowing Channel are likely to contain personal data, that is data which directly or indirectly pertains to an identified or identifiable individual. The personal data may pertain to the person who has made the report, and/or to a person suspected of the alleged wrongdoing.

The types of personal data which may be processed in conjunction with the investigation of a reported irregularity are typically the following:

- The name, position, and contact details (for example, e-mail and telephone number) of the person who submitted the report and the individual to whom the report relates, as well as any witnesses or other individuals affected.
- Details of the misconduct of which the reported person is suspected.

Stegra will only process personal data that is correct and relevant to the investigation. Superfluous personal data will not be processed. Sensitive personal data, such as information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation may not be submitted, unless essential for the reported issue, and will be erased unless legal to process and deemed absolutely necessary for the investigation.

3. The purposes, legal basis and retention period of the processing of personal data

Purpose	Legal basis	Retention period
Any personal data collected via the Whistleblowing Channel or during the investigation of the alleged misconduct	The processing is based on Stegra's legal obligation to establish reporting channels and procedures for reporting and investigating.	The personal data which is compiled and processed will not be retained longer than is necessary for the purpose of carrying out an investigation

will be processed for the purpose of handling and investigating a report.	For processing of special categories of personal data, the processing is necessary for the reasons of substantial public interest, on the basis of Union or Member State law or, where necessary, for the purposes of carrying out obligations and exercising specific rights in the field of employment and social security and social protection. For processing of personal data relating to criminal convictions or offences the processing is necessary to fulfil the legal obligation to establish reporting channels and procedures for reporting.	and to address the breach reported. Complaints, reports, and information regarding misconduct that has been investigated will be deleted at the latest within **two years** of the conclusion of the investigation.
Personal data may also be processed for the purpose of taking action in response to investigated allegations.	The processing is based on Stegra's legitimate interest in processing personal data in order to deal with and take action on discovered misconduct. To the extent such processing includes special categories of personal data or data relating to criminal convictions or offences, we do so on the basis that it is necessary for the establishment, exercise or defense of a legal claim.	See above.

4. Protection of and access to personal data

Stegra is committed to ensure that personal data is handled with a high level of security and confidentiality. Stegra has taken technical and organisational measures to protect the personal data from loss, destruction, damage and unauthorised access or disclosure. Only authorised employees and contractors have access to personal data in reports and follow-up cases.

5. Recipients and transfer of personal data

Personal data in reports and investigations will not be disclosed to others than what is necessary for the purposes of the processing. When necessary, for example, for acting on the findings of a case, personal data may be transferred to the police or other law enforcement authorities, forensic companies, or independent auditors.

The Whistleblowing Channel is managed by the external service provider Scutus Solution AB which processes personal data on Stegra's behalf and only on the documented instructions of Stegra, in the role of a data processor. The arrangement is governed by a data processing agreement.

6. Rights of data subjects

You have the right to request confirmation of and access to the personal data that Stegra processes about you, together with certain more detailed information. If you consider that the personal data relating to you is inaccurate or incomplete, you can request to have the data rectified or completed. In certain cases, you also have the right to have your personal data erased, to restrict Stegra's processing of your personal data, or to object to Stegra's processing of your personal data. Further, you have the possibility in certain cases to be given the personal data relating to you to use it somewhere else, for example, to transfer the data to another data controller (data portability).

When personal data pertaining to an individual is collected via the Whistleblowing Channel, the individual must be informed. If it is not possible to inform the individual

immediately, for example, if such information could jeopardize Stegra's investigation, information will be provided at a point in time where it would no longer constitute a risk to the investigation.

If you have any queries regarding the processing of your personal data or wish to exercise any of the rights stated above, please contact the data controller, Stegra, on the contact details specified in the beginning of this Section.

You have the right to lodge a complaint regarding how we process your personal data to the Swedish Authority for Privacy Protection (Sw: *Integritetsskyddsmyndigheten*).