Sproud™

Whistleblower policy

Sproud corporate values promote a transparent business environment in which the company's activities are run with the highest possible level of responsibility, openness, and honesty. Sproud is committed to running a healthy business and high ethical standards, which implies that every one of us must act in accordance with these principles, and have a common duty to prevent, correct and, if necessary, report any issues out of code.

At Sproud whistleblowers can report inappropriate conduct without fear of consequence. By making it easy to report, we work together to promote the trust of employees, customers, and the general public. Hence, any suspicion of fraudulent conduct, bribes or other similar issues witnessed must be reported without delay. This Policy shall apply to Sproud International AB, Sproud Ltd or Sproud SP. Z O.O. (any of the aforesaid Sproud companies are hereafter individually referred to as "Sproud".

Definitions

GDPR: General Data Protection Regulation, which is a European regulation governing the processing of personal data and the free movement of such data within the European Union.
The Whistleblower Directive: EU Directive 2019/1936 on the protection of persons reporting irregularities in Union law.
Whistleblower Act: National implementation of the Whistleblower Directive in EU Member States.
Visslan: The Whistle Compliance Solutions AB's service Visslan, which enables digital reporting of misconduct: https://visslan.com/
Misconduct: Acting or omissions that have emerged in a work-related context that there is a public interest in it occurring.
Reporting: Written or verbal submission of information about misconduct.
Internal reporting: Written or verbal provision of information about misconduct within a company in the private sector.
External reporting: Written or verbal provision of information about misconduct to the competent authorities.
Publication or to make public: To make information about misconduct available to the public.
Reporting person: A person who reports or publishes information about misconduct acquired in connection with his work-related activities.
Retaliation: Any direct or indirect act or omission which occurs in a work-related context and which is caused by internal or external reporting or by a publication, and which gives rise to or may give rise to unjustified injury to the reporting person.
Follow-up: Any action taken by the Case Manager(s) of a report to assess the accuracy of the allegations made in the report and, where appropriate, to deal with the reported infringement, including through measures such as internal investigations, investigations, prosecutions, actions to recover funds and to close the procedure.
Feedback: providing reporters ("whistleblowers") with information on the actions planned or taken as a follow-up and on the grounds for such follow-up.

Sproud™

1. Who can report?

You can report and receive protection from the Whistleblower Act if you are an employee, volunteer, trainee, active shareholder, person who is otherwise available for work under our control and management or is part of our administrative, management or supervisory body. External stakeholders such as contractors, subcontractors, and suppliers can also report. The fact that you have ended your work-related relationship with us, or that it has not yet begun, is not an obstacle to reporting malpractice or receiving protection for reporting malpractice externally.

2. What can I report?

In case of suspicion of possible misconduct, law and/or regulation violation, we urge you to report this to us as a whistleblowing case. When reporting, it is important that at the time of reporting, you had reasonable grounds to believe that the information about the misconduct being reported was true.

2.1 Malpractice in the public interest

You can report information about misconduct that has emerged in a work-related context where there is a public interest in it coming to light. In the event of other types of personal complaints that do not have a public interest, such as disputes or complaints regarding the workplace or the work environment, we encourage you to contact your immediate manager, CEO or other suitable person instead. This is to ensure that these matters are handled in the best possible way.

Examples of malpractices of a serious nature that should be reported:

- Deliberately incorrect accounting, internal accounting control or other financial crime.
- Incidence of theft, corruption, vandalism, fraud, embezzlement, or hacking.
- Serious environmental crimes or major deficiencies in workplace safety.
- If someone is exposed to very serious forms of discrimination or harassment.
- Other serious misconduct affecting the life or health of individuals.

Special rules concerning bribery

- Employees, the management, and board of Sproud International AB shall always discharge their duties professionally and impartially. In other words, in a manner that cannot raise suspicion of them being influenced by external considerations or interests in their work, e.g., by accepting inappropriate gifts or favors from companies or individuals related to their job.
- Such an attitude must be observed in every situation to avoid the risk of an employee and representatives being guilty of giving or accepting bribes.
- All hospitality must be kept within reasonable and justifiable cost limits. In the event of the slightest doubt, the cost must always be approved by your immediate superior.

At Sproud, we have chosen to consider all unethical or illegal behaviors as irregularities worth reporting. We therefore treat all reports received equally, based on the law's intention, and provide protection against retaliation for all. In these cases, we first and foremost encourage you to contact your immediate manager or safety representative.

If the reporting does not meet the Whistleblower Act's criteria and the law itself cannot provide protection, Sproud will still provide the same level of confidentiality and protection as reporting according to the Whistleblower Act, provided that the reporting is true and/or made in good faith.

The following are examples of unethical or illegal behaviors that could be reported:
- Actions and omissions that go against our culture, policies, vision and values.
- Actions that run counter to good practice and standards in the labour market.
- Drug and alcohol abuse during working hours.
- Dangerous acts that could cause physical damage to a person or property.
- Discrimination of any kind.
- Exploitation of position and/or abuse of power.

2.2 Misconduct contrary to EU law
In addition, there is the possibility to report information about misconduct that emerged in a work-related context that is contrary to EU laws or regulations. If you suspect that this occurs, then please read the scope of the Whistleblower Directive (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937) in Article 2 and Annex Part 1 for applicable laws.

3. How do I report?
3.1 Written reporting
For written reporting, we use Visslan, a digital whistleblowing channel. It is always available through https://sproud.visslan-report.se or through our website: https://sproudglobal.com

Please describe what happened as thoroughly as possible so that we can ensure that adequate measures can be applied. It is also possible to attach additional evidence that can help further investigation, for example, written documents, pictures or audio files.

3.1.1 Sensitive personal data
Please do not include sensitive personal information about people mentioned in your report unless it is necessary to be able to describe your case. Sensitive personal data is information about; ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, a person's sexual life or sexual orientation, genetic data, biometric data used to uniquely identify a person.

3.1.2 Anonymity
You can be anonymous throughout the process without affecting your legal protection, but you also have the opportunity to reveal your identity under strict confidentiality. Anonymity can occasionally complicate the follow-up possibilities and the measures we can take, but in such a circumstance we can also ask you to reveal your identity later to the Case Manager, again in strict confidentiality.

3.1.3 Follow-up & login
After you have reported, you will receive a sixteen-digit code. It is very important that you save the code to access your report again via logging into Visslan https://sproud.visslan-report.se.

Within seven days, you will receive confirmation that the Case Manager has received your report. The Case Manager is the independent and autonomous party that receives reports in the reporting channel, whose contact information is attached in “6.1 Contact information for Case Manager”. In case of questions or concerns, you and the Case Manager can communicate through the platform's built-in and anonymous chat function. You will receive feedback within three months on any measures planned or implemented due to the reporting.

It is important that you, with your sixteen-digit code, log in regularly to answer any follow-up questions that Case Manager may have. In some cases, the report cannot be taken forward without answers to such follow-up questions from you as the reporting person.

3.2 Verbal reporting

In addition, it is also possible to conduct a verbal report by uploading an audio file as an attachment when creating a report at https://sproud.visslan-report.se. In the audio file, you should describe the same facts and details as you would have done via a written submission.

In addition, a physical meeting with the Case Manager can be requested via Visslan. This is most easily done by either requesting it in an existing report or creating a new report asking for a physical meeting.

3.3 External reporting

We urge you to always report malpractice internally first, but in the event of difficulties or it is considered inappropriate, it is possible to conduct external reporting instead (or after internal reporting without results). We then refer you to contact the relevant authorities or, where applicable, EU institutions, bodies, or agencies.

4. What are my rights?

4.1 Right to confidentiality

During the handling of the report, your identity as a reporting person is treated confidentially and access to the case is prevented for unauthorized personnel. We will not disclose your identity without your consent unless compelled to by law, and we will ensure that you are not subjected to retaliation.

4.2 Protection against reprisals or retaliation

In the event of a report, there is protection against negative consequences from having reported misconduct in the form of a ban on reprisals and retaliation. The protection against this also applies in relevant cases to persons in the workplace who assist the reporting person, your colleagues and relatives in the workplace, and legal entities that you own, work for or are otherwise related to.

This means that threats of retaliation and attempts at retaliation are not permitted. Examples of such are if you were to be fired, have been forced to change tasks, imposed disciplinary measures, threatened, discriminated against, blacklisted in your industry due to reporting.

Even if you were to be identified and subjected to reprisals, you would still be covered by the protection if you had reasonable grounds to believe that the misconduct reported was true and within the scope of the Whistleblower Act. However, it should be noted that protection is not given if it is a crime itself to acquire or have access to the information reported.

The protection against retaliation also applies in legal proceedings, including defamation, copyright infringement, breach of confidentiality, breach of data protection rules, disclosure of trade secrets or claims for damages based on private law, public law or collective labor law, and you shall not be held liable in any way a consequence of reports or disclosures provided that you had reasonable grounds to believe that it was necessary to report or publish such information in order to expose a misconduct.

4.3 Publication of information

The protection also applies to the publication of information. It is then assumed that you have reported internally within the company and externally to a government authority, or directly externally, and no appropriate action has been taken within three months (in justified cases six months). Protection is also obtained when you have had reasonable grounds to believe that there may be an obvious danger to the public interest if it is not made public, for example in an emergency. The same applies when there is a risk of retaliation in the case of external reporting or that it is unlikely that the misconduct will be remedied in an effective manner, for example if there is a risk that evidence may be concealed or destroyed.

4.4 The right to review documentation at meetings with Case Manager

If you have requested a meeting with the Case Manager, they will, with your consent, ensure that complete and correct documentation of the meeting is preserved in a lasting and accessible form. This can be done, for example, by recording the conversation or by keeping minutes. Afterwards, you will have the opportunity to check, correct and approve the record by signing it.

We recommend that this documentation is kept in Visslan's platform by the whistleblower creating a case where the information can be collected in a secure way, with the option to communicate securely.

5. GDPR and handling of personal data

We always do our utmost to protect you and your personal information. We therefore ensure that our handling of these is always in accordance with the General Data Protection Regulation ("GDPR").

In addition to this, all personal data without relevance to the case will be deleted and the case will only be saved for as long as it is necessary and proportionate to do so. The longest a case will be held is two years after its conclusion. For more information about our handling of personal data, see the Company's policy on personal data (GDPR).

6. Additional contact

If you have further questions regarding how we handle whistleblower cases, you are always welcome to contact the Case Manager.

For technical questions about Visslan's platform, feel free to create a case at https://sproud.visslan-report.se. Contact information is found below.

6.1 Contact information for Case Manager
Name: Malin Göransson
Position: Quality & Sustainability Manager
Email: malin.goransson@sproud.se
Phone number: +46 76-645 33 47

6.2 Contact information for Visslan (The Whistle Compliance Solutions AB)
Email: clientsupport@visslan.com
Number: +46 10-750 08 10
Direct number (Daniel Vaknine): +46 73 540 10 19

Policy review & Document updates

This policy will be reviewed annually and revised when necessary.

Doc: Whistleblower policy	Updates & changes
Version: 001, 2021-01-12	Establishing Whistleblower policy
Version: 002, 2022-09-02	Adding the Whistle Compliance Solutions AB's service Visslan, which enables digital reporting of misconduct.
Version: 003, 2023-11-01	Policy revised and updated
Version: 004, 2025-11-20	Clarification of which companies this policy applies to

CEO signature and date
2025-12-05

Sara Berger
CEO Sproud International AB