WHISTLEBLOWER CHANNEL FOR LU-VE SWEDEN AB

1. INTRODUCTION

"REPORTING PROCEDURE FOR THE APPLICATION OF RULES AND CODES OF CONDUCT AT THE LU-VE GROUP" (hereinafter referred to as the "procedure") contains the principles and general provisions that apply to all companies in the LU-VE Group and thus also to LU-VE Sweden AB in connection with the "Reports of conduct contrary to legal rules and/or procedural and regulatory provisions and/or to the LU-VE Group's Code of Ethics". Exceptions to this approach are described in point 6 of this proceeding.

This policy has been developed specifically for LU-VE Sweden AB (hereinafter referred to as the "Company"). The policy includes the company's internal process regarding whistleblowing (hereinafter referred to as the "process") and aims to implement the requirements of the Act (2021:890) on the protection of persons who report misconduct (the "Whistleblower Act"). Through this policy, the company has, among other things, established an internal reporting channel that provides reporting persons, so-called whistleblowers, with protection in accordance with the Whistleblower Act.

All processing of personal data is carried out in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR"), Legislative Decree No. 196 of 30 June 2003 and Legislative Decree No. 51 of 18 May 2018, which you can read about in the Company's Privacy Policy available at https://whistleblowing.luvegroup.com/ .

2. DEFINITIONS

Without prejudice to the meaning of the terms and expressions set out in the 'REPORTING PROCEDURE FOR THE APPLICATION OF RULES AND CODES OF CONDUCT AT LU-VE GROUP', the following terms and expressions have the meanings set out below, with the same meaning applicable in both singular and plural.

"Publication" means making information about wrongdoing available to the public, for example through printed, electronic or otherwise disseminated media that is likely to reach a large number of people.

"Assistant person": a person who assists the reporting person in the reporting process, such as an elected representative or a safety representative, or who is connected to the reporting person, such as a relative or colleague.

"Internal report" means written or oral communication of information about misconduct provided through the internal reporting channel established by the Company in accordance with this Policy.

"External report" means written or oral communication of information about breaches submitted to an external reporting channel in accordance with the Whistleblower Act and as set out in section 4.10 of this policy.4.10

3. PURPOSE AND SCOPE

The report shall relate to irregularities and/or violations of national or EU regulations or irregularities affecting the company's integrity and/or of procedural and regulatory provisions and/or the LU-VE Group's Code of Ethics, of which it has become aware. In order to be covered by the protection of the Whistleblower Act, the misconduct must be of public interest, i.e. that the misconduct concerns a circle of people who can be classified as the public.

The Whistleblower Act does not apply to:

1. Shortcomings that only concern the whistleblower's own working or employment conditions. This means, for example, that disputes, claims or demands that are linked to a personal interest of the whistleblower or the person submitting a complaint, and which relate exclusively to his/her individual working relationships, fall outside the scope of the law. In such cases, you are encouraged to contact your immediate manager or the company's HR department.
2. When reporting classified information in accordance with the Protective Security Act (2018:585), or information relating to national security in the activities of an authority in the field of defence and security.

The misconduct covered is that which consists of acts and omissions, regardless of whether it concerns intentional or negligent conduct or whether the misconduct is based on circumstances for which no particular person can be blamed. It can be any form of negligence or impropriety that may occur in a business. Below are examples of misconduct that is typically covered by the Whistleblower Act.

a) infringements of national and EU rules consisting of criminal offences in the following areas: public procurement; services, products and financial markets, as well as the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data and security of network and information systems;
b) infringements of national and EU rules consisting of: (i) acts or omissions detrimental to the financial interests of the Union, (ii) acts and omissions relating to the internal market, (iii) acts and conduct which defeat the object or purpose of the provisions of Union acts in the areas referred to in point (a) above;
c) breach of the Code of Conduct and Procedure of the Company and/or the LU-VE Group and/or the LU-VE Group's Code of Ethics, resulting in a breach of points a) and b);
d) breaches of national rules consisting of unlawful conduct or breaches of organisational and management models such as *: 1. Organization of production and product development. 2. Product design, research and development. 3. Procurement of goods and services. 4. Procurement of goods and services for the business. 5. Receipt of materials and quantity and quality control of the same. 6. Sale of goods and services. 7. Sales Network Management. Sec. 8. Sales management: assessment of customer reliability. 9. Purchase of transport services and management of transport. 10. Handling of customs formalities. 11. Management of intra-group relationships. 12. Selection, recruitment and management of staff. 13. Management of mandatory recruitment. 14. Bonus System. 15. Raising Funding/Public Contributions. 16. Management of corporate communications and marketing activities. 17. Share capital transactions and extraordinary financial transactions. 18. Planning and management of financial flows. 19. Cash Management. 20. Preparation of financial statements, reports and corporate communications. 21. Tax Compliance Management. 22. Management of inspections/audits/assessments. 23. Relations with public authorities for the purpose of obtaining/renewing permits, concessions and licences, including in the fields of environment*

and safety. 24. Handling of Legal Proceedings and Disputes. 25. Credit Management. 26. Management of Corporate Agent Relations. 27. Management of disclosure of inside information. 29. Competition. 30. Occupational safety compliance management. 31. Protection of the moral and physical integrity and rights of workers. 32. Management of compliance with environmental requirements. 33. Use of the Company's IT Equipment.

The process also applies to anonymous reports, provided that they contain information about misconduct that is sufficiently detailed and specific to enable it to be investigated.

Actions and omissions that have not occurred but are highly likely to occur may also constitute misconduct. An attempt to conceal wrongdoing may in itself be an act that constitutes misconduct. It is not required that the misconduct must be ongoing.

The conditions for the whistleblower to be covered by the protection provided by the Whistleblower Act are as follows:

i. that it is a person who is, has been or will be active within the company as an employee, intern, volunteer, self-employed, shareholder or other person specified in Chapter 1. Section 8, second paragraph of the Whistleblower Act,
ii. that there is a public interest in the disclosure of information about the misconduct;
iii. that the whistleblower, at the time of reporting, had reasonable grounds to believe that the information about the misconduct was true;
iv. that the reporting is done internally or externally in accordance with the Whistleblower Act and this policy, or
v. through disclosure in accordance with the conditions set out in the Whistleblower Act and as described in this policy (section 4.11)4.11

The reasons that lead a person to report or publish information about misconduct are irrelevant to the protection that the whistleblower receives under the Whistleblower Act.

However, a person who is guilty of a crime by reporting or gathering information is not protected against reprisals. Furthermore, it does not apply to the discharge in the event of a breach of confidentiality if the reporting person is guilty of a crime through the collection.

Discharge from liability in the event of breach of confidentiality

The whistleblower may not be held liable for a breach of confidentiality, provided that the person at the time of reporting had reasonable grounds to believe that the reporting of the information was necessary to reveal the reported misconduct.

The exemption does not apply to:

1. intentional breach of such duty of confidentiality which, according to the Public Access to Information and Secrecy Act (2009:400), restricts the right to communicate and publish information under the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, or
2. breach of professional secrecy in accordance with the Defence Inventions Act (1971:1078).

Furthermore, the discharge does not entail any right to disclose documents.

The whistleblower may also not be held liable for a violation of the provisions concerning the collection of information, if the person at the time of obtaining information had reasonable grounds to believe that the collection was necessary to reveal a misconduct. Thus, the whistleblower is not covered by this protection if he obtains superfluous information for other reasons (e.g. gossip, vindictiveness, opportunistic or scandalous purposes).

4. PROCESS DESCRIPTION

4.1 Internal reporting channel

To report misconduct through the company's internal reporting channel, the report can be made via the IT portal available at the address https://whistleblowing.luvegroup.com/se/. In order to report, you must have read and accepted the company's "Privacy Policy".

You can also choose to report by:

- Request a physical meeting by contacting Katja Karlsson, katja.karlsson@luvegroup.com +358407751245
- send a written report to the following address whistleblowing.se@luvegroup.com or "Whistleblowing", LU-VE Sweden AB, Södra Industrivägen 2-4. SE-374 50 Asarum

If you report in any way other than through the internal reporting channels described in this policy, you must clearly state that it is a report for which you wish to keep your identity confidential and thus covered by the protection of the Whistleblower Act.

Anyone who receives a report, by external and/or internal mail, e-mail or fax or by any other means, must notify the competent person of this within seven days of receipt via the IT portal. The recipient of the report shall, if possible, also notify the whistleblower that he or she has forwarded the report to an competent person. Any paper originals of the report shall be sent together with the other documents at the request of the competent person.

The recipient of the report may not keep a copy of the report, nor may he or she carry out his or her own independent analysis and/or investigation. Failure to forward or notify an authorized person of a report received may constitute a violation of this policy.

4.2 Confidentiality when handling the report

When handling reports submitted through the company's internal reporting channel, the confidentiality of the content and related documentation is guaranteed, as well as the identity of the whistleblower and/or the person concerned and the person named in the report, as well as of any assisting persons.

The identity of the whistleblower or any other information that may directly or indirectly reveal the identity of the whistleblower will not be disclosed to persons other than the authorised persons appointed by the company and will therefore remain confidential.

The addressees of the report shall not have access to the identity of the whistleblower unless the whistleblower has expressly consented to this.

Personal data that are clearly not necessary for the processing of a particular report shall not be processed and shall be deleted immediately.

4.3 Prohibition of obstruction and retaliation

Provided that the whistleblower has reported misconduct that is covered by the protection of the Whistleblower Act, he or she is protected against the operator taking obstructive measures or reprisals against the whistleblower. Retaliation is a direct or indirect action or omission taken or not taken because the reporting person has reported that causes or may cause harm or harm to the reporting person.

It should also be noted that the prohibition of obstruction and retaliation also applies to:

a) persons who assist the reporting person in the reporting process at the responsible party, such as an elected representative or a safety representative;

b) persons who are connected to the reporting person by the responsible party, such as a relative or colleague, or

c) A legal entity that the reporting person owns, works for or is otherwise associated with.

4.4 Authorized person

The authorized persons who receive and investigate reports and provide feedback to the whistleblower are independent and autonomous persons or entities. The competent persons may be employed by the company or a person appointed by the company to manage the reporting channels and procedures on behalf of the company.

4.5 Registration

All reports, regardless of the method of receipt, are registered in the Company's Portal in the Register of Reports in the section that exists within the scope of the Company's competence. The database summarizes the essential details of the reports and their management, as well as archives all attached documentation and the documentation created during the processing of the case. After registration of the report, it will only be available to an authorized person at the company.

A personal code is assigned for each report, allowing each whistleblower to verify their treatment status. This Code will also be stated in the minutes of reports within the company's area of competence.

Once the authorized person has received the report on the Portal, an acknowledgement of receipt will be issued to the reporting person within 7 days of receipt of the report.

In the case of verbal reports (meeting request and/or use of the telephone line) and/or written reports on paper, an acknowledgement of receipt will be issued within seven days of the reporting (only if the reporting person has

provided an email address), together with a personal code linked to the report, which allows him/her to monitor the status of the report on the portal; by entering the personal code in the designated field on the home page of the portal.

4.6 Preliminary analysis of the report

The authorized person for the report carries out a preliminary assessment to ensure that the necessary conditions are in place to initiate the subsequent investigation phase, as well as to dismiss general reports or those that lack sufficient information.

If necessary, the authorized person may request further clarification and/or information from the whistleblower.

If the whistleblower has submitted the report through the portal and provided an email address, he/she will receive a notification to the provided email address of the request for clarification and/or information from the competent person. If the whistleblower has not provided an email address or other contact details, no messages can be sent and the whistleblower must therefore log in to the portal on an ongoing basis to access the information and communication in the case.

The competent person shall assess, on the basis of the documents and also taking into account the results of the preliminary analyses carried out, the initiation of the preliminary investigation phase as well as non-compliance with company rules and/or corporate rules and procedures.

The following types of reports will not be processed:

- general where it is not possible to initiate an investigation;
- manifestly unfounded;
- those containing facts which have previously been the subject of special investigations which have been closed, where the preliminary checks carried out have not revealed new information requiring further verification;
- reports where the initial investigation shows that it is not possible to verify the accuracy and/or grounds of the report.

4.7 Special investigations

a. Purpose and characteristics of the study

The purpose of the investigative activities is to follow up the report closely, within the framework of the tools available to the competent person, by means of specific assessments, analyses and specific consideration of the reasonable grounds for the reported facts, and to make an initial assessment of any action necessary to take into account the report.

b. Conduct of the investigation

The competent person shall carry out a diligent investigation and obtain the necessary information and, where deemed appropriate, have recourse to external and independent parties or experts. External parties engaged by the company are subject to the confidentiality of authorized persons

within the company.

The investigation will be carried out, among other things, with the help of:
- company details and/or documents useful for the investigation;
- external databases;
- unsealed sources;
- Documentation obtained from the company's departments
- where appropriate, statements by persons who may have been informed of the facts.

For the purpose of obtaining information, the authorised person may carry out so-called random checks on the reported facts, including directly, by means of a formal convener and interview of the whistleblower (if not anonymous), the reported person and/or other persons involved, and request these persons to produce informative reports and/or documents.

Upon completion of the investigation, the competent person prepares a report setting out the following: the activities carried out, the respective results and the results of any previous investigations carried out based on the same facts and/or facts similar to those to which the report relates, as well as an assessment on reasonable grounds or otherwise of the reported circumstances with an indication of the adoption of necessary corrective actions in the business areas and processes concerned by the report.

If the investigation results in circumstances that may be relevant to the taking of labour law measures, the final report can be sent to the appropriate person within the company, such as the company's HR department. Similarly, a final report showing criminal conduct can be shared with the company's legal department.

When the investigation is completed, the competent person decides whether to close the case or whether to take action in response to the reported misconduct.

c. Monitoring of corrective actions

If the investigation phase shows that there is a need to take action, the areas of enterprise under investigation will be responsible for establishing an action plan to eliminate the critical factors identified.

d. Time period for completion of the procedure

The evaluation process for the report will be completed within a maximum of three months from the date of notification of receipt of the report or, in the absence of such notification, within three months from the end of seven days from the date of submission of the report.

4.8 Information to the Board of Directors

The Human Resources Department provides quarterly information to the company's Board of Directors on measures taken as a result of reports made to the company.

4.9 Preservation of documentation

The information and other personal data collected is processed - also within the framework of the portal - in accordance with the company's Privacy Policy https://whistleblowing.luvegroup.com/

In order to ensure the management and traceability of the reports and the resulting activities, the Company has, whenever possible, worked to prepare and update all information relating to the reports and guarantees, by means of the Portal and its functionalities, the archiving of all related supporting documentation for the time necessary for the processing of the report, but in any event no longer than five years from the date of communication of the final outcome of the reporting procedure; in accordance with confidentiality requirements.

The originals of reports received in paper form and/or via the hotline and/or by means of hearing requests and/or other means are stored by the authorised person not only by uploading them to the portal of the relevant department, but also in a dedicated protected environment.

4.10 External reporting channel

In accordance with the principles of openness, loyalty, trust and cooperation that characterize your relationship with the company, you are encouraged to use the internal reporting channel established by the company. As a whistleblower, you may also have the right to report misconduct externally, via reporting channels administered by authorities responsible for external reporting. You can find more information about such external reporting here (https://www.av.se/om-oss/visselblasarlagen/extern-rapporteringskanal/lista-over-myndigheter-med-ansvar-enligt-ansvarsomrade-enligt-forordning-2021949/).

4.11 Publication

There is also a possibility for a whistleblower to obtain protection in the disclosure of information, provided that the reporting person:

1. has reported externally as set out in paragraph 4 and that the recipient has taken reasonable follow-up action on the reporting, or the recipient has provided reasonable feedback on the follow-up within three months of receipt of the report or, if there are special reasons, six months and the reporting person has been informed of the reasons for extending the deadline;
1. has reasonable grounds to believe that the misconduct constitutes an imminent or obvious danger to life, health, safety or the risk of extensive damage to the environment or for any other reason has a legitimate reason to make the information public, or
1. have reasonable grounds to believe that external reporting would entail a risk of retaliation or lead to the misconduct being unlikely to be effectively remedied.

5. Violation of the Whistleblower Act and this policy

This policy aims to ensure the effectiveness of the reporting process and the internal assessment process, as well as to facilitate the protection of the whistleblower, while ensuring a climate of open and constructive cooperation, also to avoid the use of reports in a way that could threaten their credibility.

An operator who violates any of the prohibitions on obstructive measures or reprisals in the Whistleblower Act may be liable to pay damages for the loss that arises and for the violation that the violation entails.

The Company takes violations of this policy very seriously and will take action in response to them. Examples of violations of this policy include:

- behaviour that hinders or attempts to impede reporting;
- failure to transmit a report of another person who has come to his knowledge and/or to take independent steps of analysis and/or investigation, including by withholding a copy of the report;
- direct or indirect retaliation and/or discrimination against the whistleblower for reasons directly or indirectly linked to the report itself;
- infringements of the measures put in place to protect the whistleblower with regard to the right to confidentiality;
- failure to establish reporting channels as well as failure to adopt procedures for preparing and managing reports, or non-compliance with them;
- failure to carry out verification and analysis of the reports received;
- the determination, including by a judgment of the first instance, of the liability of the whistleblower for defamation or slander or, in any case, for the same offence committed with the report to the judicial or accounting authorities, or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence.

If you as an employee violate this policy, the company may take employment law action against you. As a rule, this will mean that the company will inform you of this and, depending on the circumstances, give you a written warning. The appropriate measures will be determined on a case-by-case basis and depending on the circumstances of the individual case. In case of serious violations of this policy, the termination or dismissal may be relevant.

6. EXCEPTIONS

By way of derogation from what is stated in the general procedure, the Company shall comply with the following:

- According to the policy, the policy refers to all reports of conduct (including negligence) that violate the law and/or procedural and regulatory regulations and/or the LU-VE Group's Code of Ethics. Nevertheless, LU-VE Sweden's Internal Report Assessment Process only deals with whistleblowing that is covered by the Swedish Act on the Protection of Persons Reporting Irregularities (2021:890) (Whistleblowing Act).

- Section 4.1 of the operating model states that the reporting channel portal is available at: https://whistleblowing.luvegroup.com/it/. By way of derogation, LU-VE Sweden AB´s portal is available at: https://whistleblowing.luvegroup.com/se/

- Section 4.1 of the operating model describes the fields to be filled in for notifications made through the portal. For the sake of clarity, it is not necessary for the notifier to answer every question in the field in order for the notification to be processed.

- In addition to section 4.1 of the operating model, it is stated for the sake of clarity that the

processing of personal data is not based on consent but on the controller's legal obligation, as stated in the relevant data protection notice.

- By way of derogation from section 4.1 of the general procedure, the notification will not be rejected if the notifier does not respond to the request for further information after 15 days. Instead, notifications can be processed on the basis of current information if the request for further information is not answered within the time limit.

REFERENCES

- Act (2021:890) on the Protection of Persons Who Report Misconduct (Whistleblower Act)
- Regulation (EU) 2016/679 on the protection of personal data (GDPR)
- The LU-VE Group's Code of Ethics