

Whistleblowing policy

1 Table of acronyms 3

2 Background..... 4

3 Content..... 4

4 Reporting channel and public disclosure 4

 4.1 Internal reporting channel 4

 4.2 External reporting channel..... 5

 4.3 Public disclosure..... 5

5 Confidentiality and protection 5

6 Administrative Fine 6

7 Retaliation 6

8 Conclusion 6

1 Table of acronyms

AVEGA	AVEGA S.à r.l.
AVEGA Management	AVEGA S.à r.l. Management
Designated case managers	Human Resources Team (two people) and Compliance Team (two people)
HR	Human Resources
Law	Law of 16 May 2023 transposing into the DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report reporting violations of Union law
Whistleblower	A whistleblower is a person who comes forward and shares his/her knowledge on any wrongdoing which he/she thinks is happening in the whole organisation or in a specific department. A whistleblower could be an employee, contractor, or a supplier who becomes aware of any illegal activities.

2 Background

The law of 16 May 2023 (the “Law”) implements Directive (EU) 2019/1937 of the Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the “Directive”) into Luxembourg law. However, the Law has a wider scope than the Directive.

The Luxembourg government has decided to extend the material scope of the directive to all national law. Whistleblowers shall be protected against any form of retaliation when they report acts or omissions that are unlawful or defeat the object or purpose of directly applicable provisions of national or European law.

The key aim of the new law is to guarantee effective and balanced protection for Whistleblowers through clearly defined rights and obligations, to reduce the current legal insecurities to which Whistleblowers are exposed and, in so doing, to help increase respect for the rule of law.

The law applies to Whistleblowers working in the private or public sector who have obtained information on breaches in a professional setting. This includes, for example, self-employed or employed workers, shareholders and members of administrative bodies, paid or unpaid volunteers and interns, persons working under the supervision and direction of contractors, subcontractors and suppliers, Whistleblowers whose employment relationship has not yet begun in cases where information on breaches has been obtained during the recruitment process or other pre-contractual negotiations, as well as third parties who are related to Whistleblowers, such as colleagues or relatives.

3 Content

No approvals or authorisations shall be needed to report alleged misconduct. It is not necessary for Whistleblowers to present evidence of an alleged misconduct. However, the level of completeness of the whistleblowing report may affect the ability to assess the case properly and in a timely manner. Whistleblowers have the assurance that their reporting will be assessed in the appropriate manner and that it may lead to an investigation. If the allegations are confirmed, AVEGA shall take all necessary steps to identify appropriate actions. AVEGA has put in place this policy and as well as a Whistleblowing procedure. Here we refer to the Whistleblowing procedure available in the AVEGA intranet (<https://intranet.avega.local/knowledge-base-category/procedures/>). The policy and the procedure are getting reviewed on an ongoing basis in order to ensure compliance with the Whistleblowing law (at least annually).

4 Reporting channel and public disclosure

The Law provides for three reporting channels:

1. internal reporting channel
2. external reporting channel
3. public disclosure

4.1 Internal reporting channel

Public and private-sector legal entities are required to set up channels and procedures for internal reporting and follow-up. Private-sector legal entities are only subject to the requirement if they have at least 50 employees.

Reporting channels may be managed internally by a designated person or department or provided externally by a third party.

Whistleblowing channels shall be designed, set up and managed so as to guarantee the confidentiality of the Whistleblower's identity and that of any third party mentioned in the report and to prevent access to said channels by unauthorised personnel.

Once a report has been made, an acknowledgement of receipt is sent to the Whistleblower within seven days.

The person responsible for receiving reports shall be a designated person/s competent to ensure follow-up. The Whistleblower shall be guaranteed feedback within three months.

Reports via internal channels can be made in writing, or verbally, or both.

4.2 External reporting channel

Whistleblowers are free to choose whether to report internally or externally, i.e. to a competent authority. The law lists the competent authorities in article 18.

4.3 Public disclosure

Any person making a public disclosure is protected by law if one of the following conditions is met:

- The person first made an internal and external report, or made a direct external report, but no appropriate action has been taken in response to the report within the specified timeframe.
- The person has reasonable grounds to believe that:
 - o the breach may represent an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible harm;
 - o in the case of external reporting, there is a risk of retaliation or there is little likelihood that the breach will actually be remedied, due to the particular circumstances of the case, such as where evidence may be concealed or destroyed or where an authority may be colluding with the perpetrator of the breach or may be involved in the breach.

5 Confidentiality and protection

Internal and external channels shall strictly guarantee the confidentiality of the Whistleblower's identity, except in the event of a necessary and proportionate obligation imposed by directly applicable national, or European, law during investigations, in particular, with a view to safeguarding the rights of defence of the person concerned. Internal and external channels shall comply with legislation on personal data processing. Reports are only kept for as long as is legally necessary and proportionate.

The law establishes the status of the "Whistleblower", who enjoys protection under the following conditions:

- the Whistleblower shall have reasonable grounds for believing that information on breaches was true at the time of reporting and that this information falls within the scope of application of this law, and

- the report has already been made internally or externally via the channels provided for this purpose or a public disclosure has been made in accordance with the applicable provisions.

Persons who have reported or disclosed information on breaches anonymously but who are subsequently identified and subjected to retaliation shall enjoy the protection provided by this law. The same applies to persons reporting breaches to competent European Union institutions, bodies, offices or agencies.

The case information needs to be completely removed from the system unless required for evidence purposes. Reports are only kept for as long as is legally necessary and proportionate.

The designated case managers is responsible for the deletion of the case information, as the deletion is not automated. Once deleted, no data is retained in the system.

6 Administrative Fine

In the event of failure to comply with these provisions, the competent authorities may impose an administrative fine of between €1,500 and €250,000 on private-sector legal entities, the maximum fine being doubled in the event of a repeat offence within 5 years.

7 Retaliation

A Whistleblower who knowingly reports or publicly discloses false information can be punished with a prison sentence of 3 days to 3 months and a fine of 1,500 euros to 50,000 euros (article 27(5)).

8 Conclusion

This policy is adopted by the AVEGA Management and enters into force following its publication on the intranet site/AVEGA website.