WHISTLEBLOWING – REPORTING UNLAWFUL CONDUCT

(Directive (EU) 2019/1937 on the protection of whistleblowers, Act No. 171/2023 Coll. on the protection of whistleblowers)

What is Whistleblowing?

Whistleblowing is defined as the disclosure or reporting of information about possible unlawful conduct.

Who Can Report?

The whistleblower must be a person who performs work or a similar activity for the obligated entity (ELLA-CS) according to Act No. 171/2023 Coll., §2, (3). However, not only the whistleblower is protected, but also a significantly wider circle of people, such as close people, including the whistleblower's family.

A report must be submitted by a natural person and must contain information about possible unlawful conduct:

a) that has the characteristics of a crime or an administrative offense,

b) or violates a law or another legal regulation or an EU regulation governing areas defined by the law,

c) and of which the whistleblower became aware in connection with work or another similar activity.

Reports submitted anonymously may not be considered (see Act No. 171/2023 Coll. §2, paragraph 2). Anonymous reports will be handled outside the framework of the Whistleblower Protection Act.

What Can Be Reported?

Possible unlawful act that has occurred or is about to occur at the entity for which the whistleblower, even indirectly, performed or performs work or a similar activity, or at an entity with which the whistleblower has been or is in contact in connection with performing work or a similar activity.

The reporting person should have a valid reason, based on the circumstances and information available at the time of the report, to believe that the disclosed or published facts are authentic and truthful. **Knowingly reporting false information is not permitted** and may be subject to penalties. The whistleblower should act in public interest and in good faith that the submitted report is based on credible facts and evidence.

The report contains information about possible unlawful conduct that:

1. has the characteristics of a criminal offense,
2. has the characteristics of an administrative offense for which the law stipulates a fine of at least CZK 100,000,
3. violates the Whistleblower Protection Act, or

4. violates another legal regulation or EU regulation in the areas of:
    - financial services, statutory audit and other verification services, financial products, and financial markets,
    - corporate income tax,
    - prevention of money laundering and terrorist financing,
    - consumer protection,
    - compliance with product requirements, including safety,
    - transport safety, road transport, and traffic regulations,
    - environmental protection,
    - food and feed safety and animal welfare and health,
    - radiation protection and nuclear safety,
    - competition, public auctions, and public procurement,
    - internal order and security, protection of life and health,
    - protection of personal data, privacy, and security of electronic communications networks and information systems,
    - protection of the EU's financial interests, or
    - the functioning of the internal market, including competition protection and state aid under EU law.

How to Report?

Reports should be submitted via a communication channel that ensures the confidentiality of the information provided, the protection of the whistleblower, the reported person, and their personal data.

The person authorized to receive and process reports is Mgr., PharmDr. Jan Honegr, Ph.D. (hereinafter referred to as the "competent person").

If a report concerns an impending violation, including suspicions of a possible violation, it should always be a case that can be properly substantiated. However, this does not mean that the violation or impending violation must be proven by the whistleblower. It is sufficient for the whistleblower to be able to reasonably justify, based on available information, why they believe the situation requires reporting.

The reporting system is not intended for submitting inquiries, general suggestions, or complaints about individuals that would lead exclusively to a private dispute with no involvement of the company.

Methods of notification

Possible unlawful conduct within ELLA-CS, s.r.o. can be reported in the following ways:

- **Electronically:**
    - Email: whistleblowing@ellacs.eu
- **In Writing:**
    - By sending a letter marked “DO NOT OPEN – Whistleblower Protection – To the Attention of the Designated Person” to: ELLA-CS, s.r.o. Milady Horákové 504/45, Třebeš 500 06, Hradec Králové Czech Republic
- **By Telephone:**
    - Tel.: +420 702 055 834
    - Calls will be recorded. If you do not consent to a voice recording, ELLA-CS will prepare a written summary of the conversation. You will have the opportunity to review, amend, and approve the written record with your signature.
- **In Person:**
    - You can arrange a personal meeting with the designated person by calling **+420 702 055 834** or emailing **whistleblowing@ellacs.eu**.
    - A voice recording of the meeting will be made. If you do not consent, ELLA-CS will prepare a written summary, which you can review, amend, and approve with your signature.

Alternatively, reports can be submitted to the Ministry of Justice if there are doubts about whether the identified facts constitute possible unlawful conduct. More information is available at: https://oznamovatel.justice.cz/chci-podat-oznameni/.

Investigation of Reports

The company will confirm receipt of a written protected report via the electronic or postal address provided by the whistleblower unless they request a different confirmation method. However, this does not apply if confirming receipt would endanger the confidentiality of the whistleblower’s identity or the protection of their personal data.

During the investigation of reported violations or potential violations, the company will act with the highest possible confidentiality and ensure the protection of the whistleblower and their personal data. The content of reports will be handled confidentially, unless the circumstances require immediate action to protect individuals’ safety.

Deadlines for Notifying the Whistleblower of Actions Taken

If the designated person is aware of the whistleblower’s identity and contact details, the whistleblower will be notified within 7 days of receipt of the report (unless another deadline is agreed). The whistleblower will also be informed of the results of the assessment of the report’s validity within 30 days from the date of the report (unless another deadline is agreed).

The competent person will subsequently notify the whistleblower of the investigation outcome and planned or implemented measures within 3 months of notifying the whistleblower of receipt of the report or, if no confirmation was sent, from the date of receipt.

If the investigation takes longer than 3 months, the whistleblower will be informed of the reasons for the delay.

Whistleblower Protection

The identity of the whistleblower will always be kept strictly confidential. The company is committed to protecting the whistleblower and, depending on the circumstances, the identity of the reported person.

The reporting system is technically and organizationally set up to prevent the disclosure of the whistleblower's identity. Only the designated person, who is bound by confidentiality, has the right to access the whistleblower's identity and the content of the report.

The company commits to not taking any retaliatory actions against individuals who submit reports in accordance with this policy. Individuals who believe they have been subjected to retaliation may contact the company's management at any time.

Handling of Personal Data

The company ensures the protection of personal data in accordance with applicable legal regulations, including the General Data Protection Regulation (GDPR) No. 2016/679. This also applies to the personal data of the notified person who is allegedly responsible for the breach or threatened breach.

The company maintains records, minutes or transcripts of notifications made in person in a confidential and secure system, with access to the data from this system restricted to appropriate persons who are authorized to investigate a breach or threatened breach.

Reports and related documents are stored securely for 5 years from the date of receipt.