Protection of Whistleblowers

1. Scope

This Policy applies to all group companies of Assenagon and implements Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and its national implementation in Germany and Luxembourg and comprises all full- and part-time employees hired by Assenagon, including interns, trainees, working students and volunteer employees and also shareholders, members of the Board of Directors and Conducting Officers, self-employed persons, freelance workers, civil servants and employees of a contractual partner, a subcontractor or a supplier (together **"Workers"**). This Policy even applies to reporting persons where they report information on breaches acquired in a work-based relationship which has since ended.

2. Introduction

Persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in that context. By reporting breaches of Union and national law that are harmful to the public interest, such persons act as 'whistleblowers' and thereby play a key role in exposing and preventing such breaches and in safeguarding the welfare of society. However, potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of retaliation. In this context, the importance of providing balanced and effective whistleblower protection is increasingly acknowledged at both Union and international level.

Assenagon encourages all its Workers to report actual or potential breaches of law, which comprises administrative, criminal or other types of breaches, and are linked to work-related activities, either internally or externally without fearing any retaliation; however, in order to enjoy protection under this Policy, reporting persons should have reasonable grounds to believe, in light of the circumstances and the information available to them at the time of reporting, that the matters reported by them are true. That requirement is an essential safeguard against malicious and frivolous or abusive reports as it ensures that those who, at the time of the reporting, deliberately and knowingly reported wrong or misleading information do not enjoy protection. At the same time, the requirement ensures that protection is not lost where the reporting person reported inaccurate information on breaches by honest mistake. Similarly, reporting persons should be entitled to protection under this Policy if they have reasonable grounds to believe that the information reported falls within its scope. The motives of the reporting persons in reporting should be irrelevant in deciding whether they should receive protection.

3. Breaches

The following list of breaches is not complete and only gives examples of the possible offences:

fraud and corruption and money laundering;
breaches of tax laws and;
data protection laws;
employment laws;
occupational safety and health provisions;
moral harassment and workplace violence[1].

[1] Therefore implementing the Luxemburg law of 29 March 2023 on moral harassment.

4. Channels of Internal Reporting

Breaches can be reported internally via the following means:

in writing by physical post;

email;

telephone;

physical meetings;

via the homepage under Contact.

The reporting can either be done by name or on an anonymous basis; in the latter case, it is best to use a dummy account from e.g. Hotmail.

5. Recipient of the Internal Report

All reports should be directed to the Head of Legal & Compliance, although an employee can also directly address its report to the Conducting Officers or Board of Directors. When using the MCO platform, only the Head of Legal & Compliance has access and, depending on the case, tries to resolve the issue either on its own or, if needed, with other departments including Conducting Officers and Board of Directors. The identity of the reporting person is not disclosed to anyone beyond the Head of Legal & Compliance, the Conducting Officers and the Board of Directors without the explicit consent of that person. The receipt of the report will be acknowledged to the reporting person within seven days of that receipt.

The reporting person should be informed within a reasonable timeframe (maximum three months) about the action envisaged or taken as follow-up to the report and the grounds for the choice of that follow-up. It should be possible to ask the reporting person to provide further information, during the course of the investigation, albeit without there being an obligation to provide such information. The Head of Legal & Compliance is obliged to diligently follow-up on the reporting.

6. External Reporting

Workers do not need to report internally but can choose to report breaches directly externally, i.e. to communicate orally or in writing information on breaches to the competent authorities (for example CSSF, State Prosecutor, Luxembourg Labour Inspectorate (*Inspection du Travail et des Mines*, ITM), Luxembourg Direct Tax Authority *(Administration des Contributions Directes)*.

7. Data Protection

The treatment of each report requires the processing of personal data, which is carried out in strict compliance with national data protection legislation. Such data will be collected exclusively for the purpose of reviewing and answering the submission and will not be disclosed, internally or externally, to any person not involved in the treatment of submissions. In case of anonymous reports, the processing of personal data is restricted and accessibility reduced to a minimum. Any personal data gathered will generally be stored for a period of 5 years starting from the year-end of the submission. The legal basis for the processing operations described above is Article 6 para. 1 sent. 1 lit. c of GDPR (EU General Data Protection Regulation, 2016/679).