ATRIA

Good food – better mood.

Whistleblowing Policy

Purpose and Scope

This Policy describes the purpose and content of Atria's whistleblowing channel and the principles that are followed in managing the channel.

The purpose of Atria's whistleblowing channel is to meet the requirements on reporting channels of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and the applicable national laws concerning Atria Group companies on the protection of persons who report breaches.

Whistleblowing channel offers a possibility to alert suspected misconduct related to Atria's operations in confidence without any subsequent threat of retaliation. It is an important tool for reducing risks and maintaining trust, as it enables Atria to address any misconduct identified in its operations at an early stage and to develop its operations in accordance with its ethical values.

Approval:

Whistleblowing Policy is approved by the CEO. It is reviewed annually by the team responsible for managing the whistleblowing channel.

Target audience: Public, all employees

Approval date: 26 November 2021

Content

Reporting suspected misconduct

Situations when to blow the whistle

It is of utmost importance to Atria that any serious misconduct detected or suspected is reported to Atria without delay. The procedures described in this Policy relate in particular to severe breaches falling within the scope of EU Directive 2019/1937 in the following areas of legislation:

- public procurement;
- financial services, products and markets, and the prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- protection of the environment;
- 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;
- breaches affecting the financial interests of the Union;
- breaches relating to the internal market, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
- in addition, under the national legislations, protection may also be granted in other areas.

The whistleblower does not need to have firm evidence for expressing a suspicion. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service is a serious disciplinary offence.

Whistleblowing channel

Suspected misconduct can be reported in alternative ways:

1. Secure reporting through the whistleblowing channel
    - Atria Group http://report.whistleb.com/atria
    - Atria Sweden http://report.whistleb.com/atriasverige
2. If you wish to give the notice orally or face to face, request an appointment by e-mail compliance@atria.com. The e-mail is managed by Atria Group's Legal Department.

All whistleblowing notifications received are treated confidentially in accordance with Atria's standard processing procedure described below. To ensure the anonymity of the whistleblower, the whistleblowing service is managed by an external partner, WhistleB Whistleblowing Center.

The notification procedure made through the whistleblowing channel is encrypted and password protected. The whistleblowing service enables the whistleblower and Atria to discuss the matter while maintaining anonymity. The source of the notification cannot be identified, unless the whistleblower wishes to provide his or her name and/or contact information. No metadata is stored in relation to the notifications and the IP address of the whistleblower cannot be identified.

Prior to the introduction of the whistleblowing channel, the channel has been subject to an impact assessment approved by Atria's Data Protection Team 24 November 2021. In addition, the necessary discussions on the whistleblowing channel and its introduction have taken place with employee representatives in Atria's operating countries during autumn 2021.

Matters that do not fall within the scope of this policy

Standard customer feedback does not belong to the whistleblowing channel and procedures described in this policy. Instead, they should be provided through Atria's consumer and customer feedback channels.

Similarly, normal business-related complaints should be handled through Atria's representatives designated for business relationship in matter.

If the matter concerns dissatisfaction in the workplace, it is recommended to contact one's supervisor or supervisor's supervisor or HR in the first instance, as these matters cannot be investigated in the context of the whistleblowing process.

The investigation process

The whistleblowing team

All notifications will be treated confidentially in accordance with Atria's standard processing procedure by the persons assigned to this task. Atria Group's Legal Department assembles the team responsible for managing the notification channel and takes care of the proper training of the team members in the task (hereinafter “Processors”).

If necessary, other external experts may also be used in the study to ensure proper handling.

Confidentiality

Only Processors have access to notifications made through the whistleblowing channel. Each Processor is bound by an obligation secrecy which guarantees the confidentiality of the processing. During the processing of the whistleblowing case, the Processors may request information and expertise from other persons. This is also done in confidence. In addition, the Processors report the whistleblowing cases reported anonymously to Atria's senior management.

Processing and investigation

Receiving a message

All notifications are taken seriously. Upon receipt of a notification, the Processors shall decide whether to accept or reject it. If the notification is accepted, appropriate measures will be taken for the investigation. An acknowledgment of receipt shall be sent to the whistleblower no later than seven (7) days after receipt of the notification.

Processing and investigation

All wb-notifications of suspected misconduct accepted for investigation will be thoroughly investigated. Processors shall determine the appropriate method of investigation, and the following principles are applied in processing:

- All whistleblowing notifications are processed confidentially.
- A person whom the suspicion concerns or who has an interest in the matter will not participate in investigating a reported misconduct.
- If necessary, Processors will ask further questions through the anonymous whistleblowing channel.
- Processors or other persons participating in the investigation process will make no attempt to identify the whistleblower unless this person is willing to provide their contact details.
- If the whistleblower has voluntarily provided their name and/or contact details, the person's name and/or contact details will be stored only by Processors.

Rejection of the notification

Processors may reject a notification if it is evident that:

- the deviation reported is not included in the matters to be reported under this policy;
- the whistleblowing notification was not made in good faith, or it was made with intent to cause harm;
- insufficient information is available to allow further investigation; or
- the matter referred to in the report has already been resolved.

Termination of the investigation

Processors will provide feedback to the whistleblower on what actions have been taken or will be taken on the basis of the report no later than within three (3) months of the notification of receipt

of the whistleblowing notification. At the same time, however, taking into account the privacy of the persons against whom the allegations have been made, as well as other issues related to confidentiality.

Whistleblower protection

The protection enabled by the Directive applied in this policy shall apply to reporting persons who acquired information on breaches, violations or neglects in a work-related context.

Anyone who, in good faith, expresses his or her suspicions and participates in the investigation of suspected violations within the scope of this policy will not be subject to negative consequences. The whistleblower and his or her close associates will be protected from direct and indirect countermeasures. Any discrimination or other disadvantage resulting from the whistleblow notification is prohibited.

When charged with a criminal offense, the whistleblower is informed that his or her identity may need to be revealed in the course of a preliminary investigation and trial by the authority, unless the information jeopardizes the pre-trial investigation or trial.

Protection of persons identified in a notification and information to be disclosed to them

The appropriate data protection legislation will be applied to the rights of the persons whom the notification concern. The interested parties have the right to access the data concerning them and demand that any data that is incorrect, incomplete, or outdated be corrected.

These rights shall be subject to any precautionary measures necessary to prevent the destruction of evidence and any other prejudice to the processing and investigation of the whistleblowing case.

Processing of personal data

The Whistleblowing service may collect personal data about the person specified in the report, the person who submitted the report (if not sent anonymously), and any third parties involved, to investigate the reported misconduct and inappropriate behavior. This processing is based on the legitimate interest in preventing reputational risks and promoting ethical business.

The provided description and facts under this processing are only reserved to the competent and authorized persons who will treat the information in confidence. The parties have the right to access the data concerning them and to request revisions or deletions if the data is incorrect, incomplete or out of date, in accordance with local data protection law. These rights may be revoked by more important precautionary measures aimed at preventing the destruction of evidence or other obstruction of the investigation and handling of the case. Any questions or complaints regarding the processing of personal data can be addressed to the Data Protection Team at tietosuoja@atria.com.

Deletion of data

Personal data included in whistleblowing reports and investigation documents is deleted upon completion of the investigation, unless the personal data must be maintained according to other applicable laws. Data will be permanently deleted 30 days after completion of the investigation. Archived investigation documents and whistleblowing reports must be anonymized in accordance with the GDPR: they must not contain personal data through which persons can be identified, directly or indirectly.

Personal data controller

Atria Plc, General Counsel Merja Harju merja.harju@atria.com, is responsible for the personal data processed within the whistleblowing service.

Personal data processor

WhistleB Whistleblowing Center Ab (World Trade Center, Klarabergsviadukten 70, SE-107 24 Stockholm) is responsible for the Whistleblowing application, including the processing of encrypted information such as whistleblowing reports. Neither WhistleB nor any sub-suppliers can decrypt and read messages. As such, neither WhistleB nor its sub-processors have access to readable content.

1. Legal Basis for Whistleblowing practices

This practice is based on the EU General Data Protection Regulation, EU directive on whistleblower protection and national legislation on whistleblowing.

2. Transfer of personal data outside the EEA

The data is stored within the EU. The transfer of personal data outside the European Economic Area (EEA) is generally prohibited unless specific measures are taken to protect the data.