Whistleblower Policy

Aumann Group

As of 2023

This is a translation of the original German version and is provided for convenience only. Only the German version shall be binding.

Table of contents

Summary

The Aumann Group's whistleblower system is designed to enable employees and other individuals to submit reports anonymously. The whistleblower system is designed to capture such reports in a transparent process that best protects the legitimate interests of those involved. The whistleblower system is designed to prevent both financial damage to the company and damage to its reputation. Reports are only intended for the following categories of criminal or quasi-criminal violations:

- Conflicts of interest,
- Capital markets law,
- Corruption and bribery,
- Public procurement,
- Financial services, financial products and financial markets,
- Prevention of money laundering and terrorist financing,
- Product safety and compliance,
- Road 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,
- Security of network and information systems, and
- Competition law.

This Whistleblower Policy also aims to ensure, from a technical and organizational perspective, that reports of violations of laws, the Code of Conduct, or policies can be received and processed, stored, and archived with the necessary confidentiality in accordance with the requirements of the Code of Conduct, as well as data protection and data security. If local regulations are stricter than the minimum standards established in this Policy, the stricter rules apply. If there is a conflict between relevant laws and this Policy, the affected company must inform the Chief Compliance Officer to resolve the conflict.

I. Scope

This policy applies worldwide to all officers, directors, employees, contract workers and temporary workers in all locations and to all Company officials, including consultants and representatives.

II. Come into effect

This directive comes into force on 1 September 2023.

III. Content of the directive

1. Reporting obligation

Any employee of the Aumann Group and other individuals are authorized to submit information. It is particularly irrelevant whether they are employees of the Aumann Group or a subsidiary of the Aumann Group.

To the extent permitted by law and consistent with conducting a sufficient investigation, the company will protect the confidentiality and anonymity of the reporting individual.

This policy does not obligate anyone to submit information. However, if legal, contractual, or other obligations or duties to submit information exist, these remain unaffected by the above paragraph.

2. No retaliation

Employees and other persons who report an incident will not be subjected to harassment, retaliation, or other adverse employment consequences, including dismissal, demotion, suspension, or discrimination regarding the terms and conditions of employment.

Employees and associated persons who retaliate against a person who has reported an incident in good faith will be subject to disciplinary action, up to and including termination.

3. Submitting information

The submission of reports regarding actual or suspected violations should be facilitated as follows:

- Reports can be reported confidentially to the immediate supervisor;
- Reports can be reported directly and confidentially to the Compliance Department;
- Reports can be reported directly via the digital whistleblower system.

The types of reports are technically predefined in the digital whistleblower system. Otherwise, however, the submission of reports is not tied to any specific format. A current overview of the reporting channels can be found at: Corporate Governance | Aumann AG

4. Relevant information

The whistleblower system is solely for receiving and processing reports of actual or alleged violations of laws, guidelines, or the Code of Conduct. It is not available for general complaints or product and warranty inquiries. Reports should only be submitted if the whistleblower has a good faith belief that the facts reported are correct. A whistleblower is not considered to be acting in good faith if he or she knows that a reported fact is untrue. In cases of doubt, such facts should not be presented as facts, but rather as assumptions, evaluations, or statements made by other persons. Please note that a whistleblower may be liable to prosecution if he or she asserts untrue facts about others despite knowing better.

5. Protection of the whistleblower

All information, including references to the whistleblower, will be processed confidentially and in accordance with applicable laws.

6. Legal restrictions

Laws in some countries impose certain restrictions on reporting, such as what can be reported, whether personal data about an individual can be retained, or whether reports can be made anonymously. These guidelines are integrated into the digital whistleblower system. Concerns that cannot be reported using the aforementioned reporting procedures due to such restrictions should be addressed to the employee's line manager. If an employee believes it is not possible to raise the matter locally, they should escalate it within the business unit to the local HR representative or the Compliance Department.

IV. Confidentiality and data protection

Regardless of their veracity, all information is likely to cause significant damage to the reputation of those affected, the whistleblower, and / or third parties, as well as the company. We will therefore treat it with the utmost confidentiality, going beyond the obligations arising from data protection laws. In addition to maintaining a properly updated record of processing activities, it is necessary to document in writing which individuals are authorized to access the information and the associated data, and what rights they have within the scope of data processing. These individuals must be bound to strict confidentiality beyond any legal requirements.

V. IT and data security

IT solutions for receiving and processing whistleblowers must be reviewed and approved by the Information Security Officer (ISO), the Compliance Officers, and the Corporate Data Protection Officer before deployment.

The minimum requirements for the scope of the General Data Protection Regulation are derived from Article 32 GDPR and the corporate guidelines on IT security and data protection. The particular sensitivity of whistleblowers and the risks to individuals and the company if whistleblower-related data becomes known must be taken into account in a special way.

VI. Extinguishing concept

The deletion of data in the digital whistleblower system must only take place in accordance with the respective time specifications of the deletion concept or after deletion approval by two separate users (four-eyes principle).

Aumann AG
Dieselstraße 6
48361 Beelen
Germany
Tel +49 2586 888 7800
Fax +49 2586 888 7805
info@aumann.com
www.aumann.com