Reporting and investigating procedure as part of the whistleblowing system and the complaints procedure at Aurubis

Integrity and compliance are essential components of Aurubis' corporate success. The Aurubis whistleblowing system plays an important role in identifying potential violations of laws and regulations, or misconduct.

The whistleblowing system follows a regulated process for submitting, receiving and processing reports that complies with legal requirements and is set out in these rules of procedure.

1. Area of application

The following issues in particular can be reported via the whistleblowing system:

- Conduct that constitutes a criminal offense against the interests of the company (in particular fraud, corruption, violations of antitrust law, misconduct related to accounting regulations);
- Human rights or environmental risks and violations of human rights or environmental obligations arising from Aurubis' economic activities in its own business area or with direct and indirect suppliers;
- Behavior that violates anti-discrimination regulations;
- Other behavior that violates the Aurubis Code of Conduct for Employees or the Aurubis Business Partner Code of Conduct.

The whistleblowing system may not be used for deliberately or grossly negligent false reports.

2. Complaint channels

Employees, business partners, and other third parties (whistleblowers) can submit information on the risks and violations mentioned under Section 1. via various reporting channels.

Aurubis has set up the digital whistleblowing system as an internal, optionally anonymous reporting channel. It is based on the Integrity Line from the provider EQS Group AG and is therefore a protected, external application. The whistleblowing system can be accessed at

https://aurubis.integrityline.app

The whistleblowing system is available around the clock for all internal and external stakeholders. Reports can be submitted completely anonymously via the system and anonymity is technically ensured. Incoming reports cannot be traced back to the person who submitted them.

The input mask is available in ten languages. The use of the whistleblowing system is free of charge.

In addition, information can also be submitted via the following reporting channels:

- **Email:** compliance@aurubis.com
- **Post**: Aurubis AG, Corporate Compliance, Hovestrasse 50, 20539

In principle, whistleblowers can also request and arrange a personal meeting via the above-mentioned channels.

Complete anonymity of the whistleblower can only be ensured by using the digital whistleblowing system.

2.2 Content of the report

To enable Aurubis to conduct a proper and targeted investigation of the reported risk or incident, the report should be based on facts.

When submitting a report via the digital whistleblowing system (Aurubis Integrity Line), the following questions must be answered at a minimum:

- What country did the incident take place in?
- What are your suspicions?

Information on the following questions is helpful for the comprehensive processing of the report and can speed up report processing. The report need not, however, contain information on the following questions; all reports will be consistently investigated.[1]

- What company did the incident take place in?
- Are you an employee of the company in question?
- Please enter the name of the department concerned.
- What people are involved in the incident?
- What happened where and when?
- Who was involved?
- Is a repetition of the incident to be expected? If so, when and where?
- Who else might have knowledge of the incident or access to the relevant information?
- Is there any documentation or evidence of the incident described?
- Is there any other information that might be relevant and helpful?

3. Procedural principles

3.1 Confidentiality

The confidential treatment of reports is a priority for Aurubis. The whistleblowing system is designed to ensure that unauthorized employees or other unauthorized persons are not able to view the reports at any time. This is the case regardless of whether the whistleblower discloses their identity when submitting the report or not. The provision of contact details or the disclosure of identity is generally not necessary for Aurubis to process the report efficiently.

The Aurubis Compliance department is responsible for processing the report and any further investigations (see also Section 4.). Compliance department employees are specially trained, impartial

[1] These questions are also displayed in the input mask of the whistleblowing system.

with regard to the reporting process and subsequent investigations, independent, not bound by directives, and sworn to secrecy.

3.2 Protection of the whistleblower

Whistleblowers are protected against negative repercussions or punishment after reporting risks and violations. All whistleblowers who report a risk or violation in good faith in accordance with these rules of procedure can rest assured that Aurubis will not initiate or tolerate any reprisals against them.

Persons who intentionally or through gross negligence submit a false report or otherwise misuse the Aurubis whistleblowing system are excluded from whistleblower protection by Aurubis. Aurubis reserves the right to assert claims for damages in such cases.

Aurubis is only interested in the risks and violations reported, and not in the identity of the whistleblower. The sole objective is to clarify grievances.

It may not be possible for Aurubis to maintain the confidentiality of the identity of the whistleblower if Aurubis is required by law to disclose information about the identity of the whistleblower, in particular at the request of law enforcement authorities.

4. Reporting and investigation procedure

The whistleblower will receive confirmation of the receipt of the report within **seven days**.

The Chief Compliance Officer or their deputy will first review the plausibility and validity of the report. For a complaint pursuant to the German Supply Chain Due Diligence Act or of suspected discrimination, the Chief Compliance Officer or their deputy will coordinate any additional investigation and involve the relevant specialist department or the discrimination officer respectively. The Compliance Committee is brought in for all other issues. This interdisciplinary committee consists of the Chief Compliance Officer, the Head of the Legal department, the Head of Group Security, and the Head of Internal Audit, and is responsible for coordinating the review process and defining the investigative responsibilities. The investigation into the facts of the case is initiated. All investigations are conducted objectively and without prejudice while protecting the legitimate interests of the persons involved.

It is also possible to discuss the facts of the case with the whistleblower anonymously via the digital whistleblowing system using a secure inbox. The identity of the whistleblower cannot be identified when the secure inbox is used.

The Aurubis Human Rights Officer is involved in the investigation of the facts for any complaints or information pursuant to the German Supply Chain Due Diligence Act (LkSG).

If, once an investigation is complete, the Compliance department is convinced that violations pursuant to Section 1. have occurred, appropriate countermeasures will be taken. In the event of conduct in the company's own business area and suppliers that violates human rights or environmental obligations or if corresponding risks are identified, preventive and remedial measures will be developed, implemented and monitored, with the involvement of the whistleblower if necessary.

The investigation and findings are documented in accordance with legal requirements. The confidentiality of the identity of the whistleblower is ensured. Aurubis only processes personal data in accordance with the applicable legal provisions, in particular the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG).

The time required to process a report depends on the scope and complexity of the report. Whistleblowers will be appropriately informed in keeping with applicable whistleblower laws of the follow-up measures taken or planned within **three months** of receipt of the report, insofar as this is legally feasible.

Version: 2.0
Status: April 2025