

Grievance and Whistleblowing Procedure

Aurum Chemicals Sp. z o.o.

Confidential reporting and impartial follow-up in chemical raw material distribution

Document ID	AC-ESG-WB-002
Revision date	30 September 2026
Document owner	Management Board
Effective date	Date of approval
Next review	Within 12 months of entry into force, or earlier after a material change

1 Purpose and scope

Aurum Chemicals Sp. z o.o. distributes chemical raw materials and provides advice on their selection. This Procedure describes how to raise concerns about the Company's purchasing, sales, technical advice, office activities and supply chain, including storage, handling and deliveries performed by service providers.

Company details: ul. Kępowa 44, 40-583 Katowice, Poland; NIP 6342660122; KRS 0000906538; REGON 240798549; www.aurumchemicals.eu.

Employees, former employees, candidates, B2B contractors, trainees, shareholders and members of Company bodies may report concerns. The mechanism also welcomes individuals working for manufacturers, suppliers, warehouse operators, logistics providers and customers, as well as other stakeholders. Statutory whistleblower protection depends on the applicable legal conditions, including a work-related context; being a customer or supplier alone does not establish eligibility.

This public document is a draft description of the reporting mechanism. The Company's formally adopted internal reporting procedure and mandatory law govern statutory reports. Ordinary workplace grievances and commercial complaints may be handled through an appropriate separate process, with the safeguards stated here.

2 Principles

We encourage reporting of suspected misconduct, protect confidentiality and prohibit retaliation. Reports are assessed impartially and followed up with due care. A reporter does not need to prove a breach. Provide information reasonably believed to be true; an unsubstantiated concern or honest mistake alone is not a reason for adverse treatment.

3 Matters that may be reported

- Product safety and chemical compliance concerns, including inaccurate safety data sheets, labelling or packaging, concealment of hazards, and suspected failures to meet applicable REACH or CLP obligations.
- Unsafe chemical storage, handling or delivery; damaged packaging; leaks and spills; improper waste management; or other risks to people or the environment.
- Bribery, fraud, conflicts of interest in procurement or sales, unfair competition, suspected trade-restriction breaches, financial misconduct or falsification of product or transaction records.
- Discrimination, harassment, bullying, employment or human-rights concerns, and other workplace misconduct.
- Misuse of personal data, confidential information or Company assets, cybersecurity incidents, concealment of evidence, obstruction of reporting or retaliation.

These examples describe the Company's broader reporting mechanism. Not every grievance falls within the statutory whistleblowing regime. The authorised reviewer identifies the appropriate route and explains any referral where a contact address is available. Reports must not be rejected solely because the reporter chose an incorrect category.

4 Reporting channels

Channel	How to use it
Written report	Send a sealed envelope to Aurum Chemicals Sp. z o.o., ul. Kępowa 44, 40-583 Katowice, Poland, marked "Confidential — Whistleblowing — authorised recipient only". Before activation, the Company must establish delivery directly to the authorised recipient without opening by other staff.
Direct meeting	Request a confidential meeting with the designated authorised recipient. Where the statutory procedure applies, arrange the meeting within 14 days of the request. Record the report with the reporter's consent and allow review, correction and signature of the minutes.
Electronic reporting	Use the restricted reporting address or system communicated by the Company after verification of its access controls. Complete the activation record on page 4 before publishing this channel.
General contact	office@aurumchemicals.eu is the published general contact address. Use it to request secure reporting instructions without including sensitive allegations or identifying details. It is not confirmed as a restricted whistleblowing mailbox.
Conflict route	Use the alternative authorised recipient identified on page 4 if the usual recipient or a Board member is implicated. The implicated person must not receive, assign or investigate that report. External statutory reporting remains available.

5 Making a report

Describe what happened, when and where, the persons or entities involved and any immediate risk. For product or delivery concerns, include available product, batch, order or shipment references. Provide relevant evidence lawfully available to you and a safe contact address if you wish to receive acknowledgement and feedback. Do not obtain evidence through unlawful access or include unrelated personal data.

Anonymous reports are accepted under this proposed mechanism and assessed on the information available. Lack of contact details may prevent clarification, acknowledgement and feedback. If an anonymous reporter is later identified, statutory protection applies where the legal conditions are met.

For an immediate threat to life, health or the environment, contact the emergency services and follow applicable emergency instructions. This reporting mechanism does not replace urgent incident response.

6 Handling and follow up

Receipt and acknowledgement

The authorised recipient registers the report securely, checks immediate risks and preserves relevant evidence. Acknowledge receipt within 7 days where a contact address is provided. Any unintended recipient must safeguard the information and transfer it promptly to the authorised person without unnecessary copying or further disclosure.

Assessment and impartial review

Assess whether the matter concerns a statutory report, a grievance or another complaint; identify urgency, conflicts and the competent reviewer. The reviewer may examine records, interview relevant persons and obtain chemical safety, environmental, HR, legal or data-protection expertise as needed. Access is limited to authorised persons. Treat persons affected by allegations fairly and preserve their confidentiality.

Feedback and closure

Provide feedback on planned or completed follow-up and the reasons for it within 3 months of acknowledgement. If acknowledgement was not sent, the statutory deadline runs from the expiry of 7 days after the report was made. Feedback is provided where a contact address exists and respects lawful confidentiality limits. An investigation may continue after feedback; document its outcome and track corrective, preventive, disciplinary or contractual measures to completion.

7 Confidentiality data protection and records

Protect the identity of the reporter, the person concerned and third parties, including details that could identify them indirectly. Disclosure outside authorised handling is permitted only with the reporter's explicit consent or where law requires it. Apply appropriate access controls and GDPR safeguards; provide the applicable privacy information.

The secure register records the report number, subject, receipt date, necessary identification and contact details, follow-up actions and closure date. Retain statutory internal-report records for 3 years after the end of the calendar year in which follow-up or proceedings initiated by that follow-up were completed. Delete records after the lawful period, subject to statutory exceptions for case files. Remove irrelevant personal data within 14 days of identifying their irrelevance. Keep ordinary grievance records under a separately justified retention schedule.

8 Protection against retaliation

Dismissal, demotion, intimidation, harassment, discrimination, adverse scheduling, unjustified contractual disadvantage and other retaliatory actions, attempts or threats are prohibited. Protect reporters and people assisting or connected with them as required by law and under the Company's reporting commitments. Statutory protection requires reasonable grounds to believe the reported information was true and concerned a breach of law when reported.

Report suspected retaliation through an authorised, non-conflicted route; assess it as a separate serious concern. Knowingly reporting false information is not protected. A finding that a report could not be substantiated does not itself establish deliberate false reporting.

9 External reporting

Eligible persons may report a breach of law to the Polish Ombudsman or the competent public authority without first using the internal channel. Current information and reporting instructions are available at <https://www.gov.pl/web/sygnalisci>. Relevant EU institutions may also receive reports where applicable. Public disclosure has separate statutory conditions; internal reporting is not a prerequisite for external reporting.

10 Responsibility and implementation

The Management Board appoints authorised recipients and an impartial follow-up owner, arranges substitutes and an independent conflict route, and provides resources. Purchasing, sales, technical and logistics personnel support reviews within their competence and authorisation. External specialists may assist under confidentiality and data-protection arrangements; accountability remains with the Company.

Review effectiveness at least annually using aggregated case categories, response times, completed actions and retaliation risks. Protect identities in management reporting. Before activation, confirm channel security, issue authorisations and communicate the approved arrangements. For a statutory internal procedure, consult the relevant trade unions or elected worker representatives, as applicable, for 5 to 10 days and bring it into force after 7 days from communication to persons performing work, as required by law.

Activation and approval record

Complete these fields before issuing the procedure as operational. The published contact details must permit direct access to an authorised person without routing through an implicated person.

Primary authorised recipient and secure contact: Magdalena Wiśnicka mwi@aurumchemicals.eu

Signature: _____ Approval date: _____

Signature Not Verified
Dokument podpisany przez
Grzegorz Szczepanik
Data: 2026.09.30 13:21:48 CEST

Sources

Company profile and details: aurumchemicals.eu/en/p/about-us-en and aurumchemicals.eu/en/contact. Legal reference: Polish Act of 14 June 2024 on the Protection of Whistleblowers, Dz. U. 2024 item 928 — eli.gov.pl/api/acts/DU/2024/928/text.html. Verified on 30 September 2026.