Whistleblower Policy

Versions

Number	Version	Date of publication
1	Release	31.07.2024.

Responsible for the subject	Surveyor(s)	Approver(s)
dr. Máté Smelka Compliance Officer International	Christoph Palausch Geschäftsführer (COO)	Prof. Dr. Robert Gröning Geschäftsführer (CFO)

Related guidelines	
Title	ID Number
CPO Procedural Directive	
Code of Conduct	

Overview

I. Definitions

- **Policy** refers to this Whistleblower Policy.

- **OBO-Group:** The list of companies belonging to the OBO Group can be found here. This Policy does not apply to the Swedish company OBO BETTERMANN AB.

- **Breaches** are actions or omissions that violate the values or rules set out in the OBO-Group's Code of Conduct, as well as acts and omissions that are considered violations under the applicable law of the respective country.

- **Information on breaches** are justified suspicions or knowledge of actual or possible violations that have already been committed or are highly likely to be committed within the OBO-Group or in connection with the activities of the OBO-Group, as well as attempts to conceal such violations.

- **Data and information processing** are actions and measures aimed at collecting, storing, changing, supplementing, using, disseminating, anonymising, blocking and deleting data.

- **Reports** are the oral or written communications of information about violations to internal or external reporting offices (competent authorities of the respective country).

- **Reporting person or whistleblower** means the natural person who reports or publicly discloses information on breaches to the competent offices listed in Annex 1 of this Policy (hereinafter referred to as: competent offices), or to external reporting offices.

- **Suspected breach** means a reporting person's suspicion of a breach in the organisation at which he works or has worked or in another organisation if he has come into contact with that organisation through his work, in so far as the suspicion is based on reasonable grounds resulting from the knowledge gained by the employee in the service of his employer or from the knowledge obtained by the employee through his work at another business or organisation.

- **Internal reporting** is the oral or written communication of information on breaches within the OBO-Group to the competent offices.

- **External reporting** is the oral or written communication of information on breaches to the competent authorities of the respective countries.

- **Disclosure** refers to making information about breaches available to the public.

- **Retaliation** is any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person (e.g. suspension, dismissal, etc.).

- **Follow-up action** is the action taken by an internal or external reporting office to verify the validity and accuracy of a report, to take further action on the reported violation, to restore the legal status or to close the case.

- **Employee(s)** refer(s) to all employees, officers, directors, managers, shareholders, non-executive members, temporary staff, volunteers, paid or unpaid trainees of any of the OBO-Group companies.

"Gender clause"

For reasons of readability, the generic masculine form is used. It should be noted that the exclusive use of the masculine form is to be understood independently of gender. This is in no way intended to imply gender discrimination or a violation of the principle of equality.

II. Scope of application

1. Material scope

The OBO-Group is committed to conducting its business in accordance with the highest ethical and legal standards. For this reason, any violation of the OBO Code of Conduct will be treated with the utmost seriousness.

The following regulations are intended to support the employees, management, business partners, customers and suppliers etc. of the OBO-Group as well as all potentially affected individuals (all natural persons) in recognising, reporting and eliminating possible misconduct within the OBO-Group and to provide a secure channel for reporting without fear of retaliation, with the aim of strengthening the compliance and information culture within the OBO-Group.

Illegal, immoral or unlawful behaviour, or behaviour which violates the OBO Code of Conduct and which the employee or person concerned cannot stop on their own should be reported to a contact person appointed by the OBO-Group. However, the whistleblower system is not intended to be used to complain about or denounce other employees in general.

Facts / information / documents, regardless of their form or medium, the disclosure of which is prohibited because they are covered by national security, the protection of classified information, the protection of legal and medical professional privilege, the secrecy of judicial deliberations and rules of criminal procedure are excluded from the scope of this Policy.

2. Personnel scope (target group)

This Policy applies to all companies of the OBO-Group and to all persons named in section II. 1 and III. 4. This Policy does not apply to the Swedish company OBO BETTERMANN AB.

3. Temporal scope

This Policy shall apply for an unlimited period from the date of its publication until its repeal.

4. Territorial scope

This Policy applies to all countries where an OBO-Group company is located. This Policy does not apply to the Swedish company OBO BETTERMANN AB.

5. Hierarchy

To the extent that stricter rules, statutory provisions, conflict-of-law rules, etc. exist in the applicable national legal systems for individual areas covered by this Policy, such rules shall prevail over the provisions of this Policy (e.g., criminal offenses, misdemeanours, etc.).

III. Whistleblower system

1. Whistleblower

(1) The OBO-Group encourages all natural persons to make a report via the OBO-Group's whistleblower system if they become aware of a violation of the OBO-Group's Code of Conduct and if local legislation permits such a report.

(2) This Policy shall not oblige anyone to submit reports. However, insofar as legal, contractual or other duties or obligations exist to submit reports, these shall remain unaffected by sentence 1.

(3) The whistleblower system serves to receive and process reports and to protect the persons named in point 1 as well as the persons referred to under section III. 4 “Whistleblower protection” below from retaliation related to reports. However, the whistleblower system is not available for general complaints or general enquiries in particular. In this case, please contact our customer service:

Contact

For Germany, complaints under the German Act on Corporate Due Diligence Obligations for the Prevention of Human Rights Violations in Supply Chains (LKSG) should be submitted through the contact provided in Annex 1.

(4) Reports should only be made if the whistleblower acts in good faith that the information reported is true and the whistleblower has reasonable grounds to believe that the information reported is true. The whistleblower is not acting in good faith if he knows that a reported information is untrue. In case of doubt, the information shall not be presented as facts but as assumptions, estimates or assertions of other persons. Labour law sanctions shall also not be imposed in the event of good faith reports.

(5) It should be noted that whistleblowers who, against their better judgement, report untrue information about other persons may be liable to prosecution or a fine under national law.

2. Reports

(1) Reports may be submitted by whistleblowers to one of the competent offices using the contact details specified in Annex 1. The submission of information on breaches is not bound to any particular form, or language. Information on violations may be submitted by the whistleblower in the native language of the country of origin; the competent office shall ensure translation and communication in the native language of the whistleblower. In particular, the reports may be submitted in person, by telephone, in writing or in text form (e.g. by letter or e-mail). For reasons of procedural simplification, we recommend submission by e-mail. In order to ensure confidential processing of postal notices, we request that the address suffix "CONFIDENTIAL - OBO Notices" be used. National legislation may lay down specific formal requirements for reporting which may go beyond those laid down in this Policy.

(2) The competent offices will, of course, give all natural persons the opportunity of prior consultation before making a report. The use of the consultation does not imply an obligation to make a report, and the competent offices are obliged to treat the information provided during the consultation in the same confidential manner as the reports.

(3) In addition to the responsible competent offices listed in Annex 1, the whistleblower has the option of contacting external reporting offices in accordance with the legal provisions of the respective country, as listed in Annex 3. However, the OBO-Group recommends first taking the route via its own internal reporting office (competent offices). The whistleblower shall be informed that some local laws may make the protection of the whistleblower dependent on the whistleblower first contacting the competent offices.

(4) The report may also be made anonymously. As a general rule, the whistleblower is however encouraged to disclose his identity rather than proceed with an anonymous report. The reason is that it is more difficult to follow up on a report and to conduct a thorough and complete investigation if it is impossible or difficult to contact the source for further information. If the whistleblower identifies himself, it may be easier to protect him against retaliation.

(5) The competent office shall acknowledge receipt of the report to the whistleblower within 2 working days at the latest. Following this acknowledgement, the competent office shall assess whether the reported infringement falls within the material scope of this Policy and shall inform the whistleblower within 7 days of receipt of the report (or within 3 days of the relevant decision being taken) how the report is classified and whether it will be investigated by the competent office or referred to the competent department or authority.

(6) In case that national legislation requires that follow-up actions be carried out by an organizational unit or a person within company's organizational structure, the competent office listed in Annex 1 will forward the matter to such internal unit or person within the relevant company to carry out follow-up activities. In the above-mentioned case, such internal organizational unit or person within the relevant company will be deemed as the competent office within the meaning of this Policy, in the scope of carrying out the follow-up actions.

(7) The competent office shall (if possible and permissible) maintain contact with the whistleblower, verify the validity of the report received, request further information from the whistleblower if necessary, and take appropriate follow-up action.

(8) The competent office shall provide feedback to the whistleblower in writing within 30 days of acknowledging receipt of the report. The competent office may, after informing the whistleblower, extend the deadline for providing feedback by 30 days if justified by the circumstances of the investigation. Notwithstanding the above, the competent office shall be obliged to provide feedback to the whistleblower within 2 working days of the end of the investigation.

(9) The feedback shall include an indication of any follow-up action planned, as well as any follow-up action already taken and the reasons for such action. Feedback provided to the whistleblower shall not interfere with internal inquiries or investigations and will not prejudice the rights of the persons who are the subject of, or named in, the report.

(10) The competent office shall be granted by the OBO-Group the powers necessary for the performance of its tasks, in particular to examine the notifications, to obtain information and to carry out follow-up actions. The competent office shall be provided with the resources required to fulfil its tasks. The competent office shall be independent in the fulfilment of its tasks and may also carry out other activities within the OBO-Group, provided that this does not conflict with the tasks in accordance with this Policy or jeopardise the fulfilment of these tasks.

(11) The whistleblowers maintain at all times the right not to incriminate themselves when making a report.

(12) During the investigation, confidentiality will be maintained to the fullest extent possible, consistent with a thorough investigation and the needs of the OBO-Group.

3. Documentation of the reports

(1) The competent office shall document all incoming reports in a permanently available form in compliance with the confidentiality obligation and the provisions of the respective national law.

(2) In the case of reports by telephone, reports by means of another form of voice transmission or reports in the context of a meeting, a complete and accurate transcript (verbatim record) of the conversation may only be made with the consent of the whistleblower. In the absence of such consent, the competent office shall document the report in a summary of its content (content protocol). A copy of the document containing the report is kept by the whistleblower. The competent office shall not make audio recordings of reports.

(3) The whistleblower shall be given the opportunity to review and, if necessary, correct the transcript or protocol and confirm it by signature or in electronic form.

(4) The competent office shall document in each case whether the whistleblower has chosen to remain anonymous and where the whistleblower's consent is required pursuant to applicable data protection legislation, that the whistleblower has expressly consented to the processing of his personal data, in accordance with Annex 2.

(5) The competent office shall also comply with any additional requirements for the documentation of reports set out in the applicable laws of the relevant country.

4. Whistleblower protection

(1) The OBO-Group is obliged to keep the identity of the following persons confidential:

- the whistleblower and their supporters (e.g. witnesses, close relatives or colleagues who provide information to the whistleblower, or who may be retaliated against in a professional context but do not act as whistleblowers, facilitators i.e. natural persons who help a whistleblower during the whistleblowing process and whose help should be confidential, in the context of whistleblower protection hereinafter collectively referred to as: whistleblower), insofar as the reported information relates to violations that fall within the scope of the Policy, or the whistleblower had reasonable grounds to believe that this was the case at the time of the report,
- the persons who are the subject of the report,
- the other persons mentioned in the report, and
- legal entities belonging to the whistleblowers, or for which they work, or to which they are related in a professional context.

(2) Except for the purpose of complying with the legal obligations in force in the country concerned, including those stemming from EU law, or with the explicit and free consent of the persons referred to in the section 1, the identity of the persons referred to in the section 1 or any information from which their identity may be directly or indirectly deduced may be disclosed only to the persons responsible for the competent office or the persons carrying out follow-up activities and to the persons assisting them in the performance of these tasks, and only to the extent necessary for the performance of these tasks.

(3) When the identity of the persons referred to in the section 1 and any information from which this identity may be directly or indirectly deduced are disclosed pursuant to specific legislation in the context of investigations by national authorities or judicial proceedings, the persons concerned will be informed thereof beforehand, unless such information would risk jeopardising the investigations or judicial proceedings concerned.

(4) The requirement of confidentiality of identity shall apply regardless of whether the competent office is responsible for the incoming report.

(5) Whistleblowers shall enjoy protection under this Policy only if they can reasonably believe, on the basis of the factual circumstances and the information available to them at the time of reporting, that their information is true and falls within the scope of this Policy. Otherwise (especially if the whistleblower knowingly provides false information), the identity of a whistleblower is not protected by this Policy, unless otherwise provided by the applicable national law.

(6) The competent office shall reject obviously false information by informing the whistleblower that such information may make the whistleblower liable for damages or, depending on the provisions of the applicable national legal system, may expose the whistleblower to the risk of legal or administrative prosecution.

(7) The protection of whistleblowers requires that
- the whistleblower is acting in good faith, and
- the information relates to an infringement within the scope of this Policy, or the whistleblower had reasonable grounds to believe that this was the case at the time of the report, and
- the protection of the whistleblower is not excluded by the legal provisions of the respective country.

(8) The whistleblower cannot be held legally responsible for obtaining or accessing the information he has reported, unless the obtaining or accessing in itself constitutes a separate criminal or administrative offence under the rules of the applicable national legal system.

(9) Retaliation against the whistleblower, who had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and fell within the scope of this Policy, the other persons referred to in section 1 and the Employer are prohibited. This also applies to the threat and attempt of retaliation.

(10) If, in the context of proceedings before competent courts or competent authorities, the whistleblower demonstrates that he suffers from any detriment in connection with his professional activities and that he made a report under this Policy, such detriment shall be presumed to be a retaliation for making such report. In this case, the person (natural person or legal entity) who retaliated against the whistleblower must prove that the detriment was based on sufficiently justified reasons or that it was not based on the report.

(11) In the event of a breach of the prohibition of retaliation, the person concerned shall be entitled to claim compensation for the resulting damage in accordance with the provisions of the applicable national legal system.

(12) If the whistleblower has nevertheless been the victim of retaliation, this shall not constitute a claim to employment, a vocational training relationship or any other contractual relationship or to career advancement.

(13) Further sanctions for violations of the whistleblower protection provisions may be provided for in the whistleblower protection laws of the respective country.

IV. Data protection

1. Processing data

(1) The OBO-Group fulfils its obligations under the applicable data protection laws, including Regulation (EU) 2016/679 (GDPR) and the national laws implementing it, and treats all information about violations, regardless of their truthfulness, with particular confidentiality and in accordance with the applicable statutory data protection regulations. More generally, any processing of personal data, including the collection, exchange, transmission or storage of personal data as part of the collection and handling of reports and their investigation, will be carried out in accordance with applicable data protection laws, as further detailed in Annex 2 "Data Protection Notice", as amended from time to time.

(2) In addition to the processing directory, which is to be kept correctly and updated at all times, the persons who have access to the information and the associated data, as well as their rights with regard to the processing, are to be recorded in writing. The employees of the OBO-Group who are involved in the processing of information are obliged to treat the personal data of which they become aware in connection with the reports as confidential, in accordance with Annex 2 “Data Protection Notice” to this Policy.

(3) If a privacy policy is published in the relevant country in accordance with local law, it will automatically become part of this Policy. In the event of a conflict between the privacy policy under local law and the Data Protection Notice attached in Annex 2, the privacy policy under local law shall prevail.

2. IT- and data security

(1) IT solutions for receiving and processing information on breaches must be checked and approved by the ombudsperson (DR. WEHBERG UND PARTNER mbB) and - if available - by the data protection officer of an OBO-Group company before they are used.

(2) The OBO-Group fulfils its security obligations for data processing by means of an IT security system in accordance with Art. 32 GDPR.

3. Deletion concept

(1) As a matter of principle, the personal data shall be retained for as long as is necessary and proportionate for the investigation of the reported compliance incident. After completion of all work in connection with the compliance report, the competent office shall delete the personal data with the exception of the data that must be retained and processed in order to exercise and defend the rights of the OBO-Group.

(2) The date of deletion of the personal data stored and processed by the OBO-Group for the exercise and defence of its rights shall be determined by the expiry of the maximum limitation periods for administrative offences and criminal offences or for the assertion of civil claims in accordance with the applicable local law.

(3) Data relating to a report which has not led, or could not lead, to disciplinary or judicial proceedings shall be destroyed right after the closure of the investigation.

(4) The above is without prejudice to specific data retention periods set forth in the applicable national law of the relevant country, referred to in Annex 3, which shall prevail in the event of a conflict with section 3.

V. Miscellaneous

1. Review of the whistleblower system

The OBO-Group is obliged to review the whistleblower system annually and to make any necessary changes.

2. Country-specific information

The references to national legislation, the list of national external reporting offices and the contact details of the national data protection authorities are set out in Annex 3 to this Policy.

VI. List of Annexes

Annex 1 Competent offices
Annex 2 Data Protection Notice
Annex 3 Country-specific information