Whistleblowing Policy

June 2026

Table of Contents

1. Background and purpose of the whistleblowing policy

1.1. About CBTW

Collaboration Betters The World (hereinafter "CBTW") is committed to being a responsible company and promotes ethical business conduct for all its stakeholders.

To support its commitment, CBTW is implementing a Whistleblowing Policy in accordance with the requirements of the European Whistleblowing Directive[1].

1.2. The scope of the Policy within Collaboration Betters The World

For the purposes of this Policy, "CBTW" refers to the following company:

- Collaboration Betters The World GmbH (DE – Company number HRB 106869)

Therefore, the reporting received via the tool (cf. Infra point 5) can only concern this company.

1.3. From who comes this procedure and for whom it is intended ?

The European Directive of October 23, 2019, sets out a legal framework of minimum standards that must be transposed into national law by December 17, 2021. It is intended to provide whistleblowers with greater protection across CBTW entities. Companies with over 50 employees are obliged to set up internal reporting channels and procedures in accordance with this Directive. By setting up such internal reporting channels, CBTW can improve their ability to deal with issues internally and reduce the risk of damaging public disclosure, which could potentially harm our reputation as a company.

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law

1.4. What is a whistleblower? Why this procedure and for what reasons?

A whistleblower is a natural person who reports or discloses information on actual or potential breaches obtained in a work-related context and who has reasonable grounds to believe that the information reported was true at the time of reporting (hereinafter: “The Whistleblower”). Such breaches may include, without limitation, bribery and corruption, competition law violations, conflicts of interest, fraud, financial crimes, harassment, discrimination or workplace violence This whistleblowing procedure allows witnesses or victims of serious incidents within the company to report facts or suspicions, while protecting them from any negative repercussions. The procedure is accessible via NAVEX digital Whistleblowing tool (WhistleB, Whistleblowing Centre) on CBTW’s websites for people outside the organization and on the Positiveapp in the "useful links" section for employees (cf. Infra point 5). This tool is available in all the languages of the entities covered by this policy.

In order to ensure the fairness, effectiveness, and universality of the whistleblowing system, CBTW commits to provide clear, continuous, and accessible information about the existence and procedure of this mechanism to all employees.

1.5. Internal reporting vs. External reporting

This whistleblowing procedure is designed to provide a channel for people who have witnessed or been victims of serious incidents within the company to express their views, while ensuring protection against any negative repercussions against them.

The purpose is to offer a safety channel to report breaches, facts or reasonable suspicions that occurred or might have occurred in the company in order to resolve the incident internally without having to go through an external reporting system. The Whistleblower can also choose to make an external reporting to the competent authorities, but this internal tool provides the Whistleblower an opportunity to resolve the issue internally. CBTW encourages the Whistleblower to do the reporting first internally, without having to go to external authorities first.

2. To whom does this Policy apply?

This Policy applies to the CBTW’s employees within the scope of this Policy as per section 1.

But also, all persons who are part of the life of CBTW without being employees, i.e., interns (paid or unpaid)or volunteers.

This Policy is also intended to apply to all CBTW stakeholders, including suppliers, contractors and subcontractors and anyone working under their supervision and direction, the Clients, facilitators / intermediaries, in the context of their contractual relationship with CBTW; Shareholders and members of the administrative, management or supervisory body, including non- executive members.

But also, anyone who is not yet or no longer part of the corporate life of CBTW, such as:

- Ex-employees who disclose information about breaches during the work-based relationship that has since ended.
- Future employees whose employment relationship has not yet begun in cases where information about breaches was acquired during the recruitment process or other precontractual negotiations.

Finally, third parties who are related to someone who works for the company and who could suffer retaliation in a work-related context, such as colleagues or relatives of the affected party. This can also be legal entities that the Whistleblower owns, works for or is otherwise connected with in a business context.

3. Whistleblower protection

3.1. Protection of the Whistleblower against retaliation

When a reporting is made in good faith, based on reasonable grounds that the information on a breach reported was true at the time of reporting and that such information fall within the scope of this Policy; the Whistleblower will be protected from any retaliation within CBTW.

By retaliation we refer to:
- Suspension, lay-off, dismissal or equivalent measures.
- Demotion or withholding of promotion.
- Transfer of duties, change of location, reduction in wages, change in working hours.

- Negative performance assessments only when the Whistleblower did not actually perform poorly.
- Intimidation.
- Discrimination or unfair treatment.
- Failure to convert a temporary employment contract into a permanent one only when the Whistleblower had legitimate expectations.
- Early termination or cancellation of the contract (or license/permit).
- Psychiatric and medical referrals.

Any such retaliation by anyone will be considered a serious breach of this Policy. Members of the Ethics Committee, case managers, and any person involved in receiving, assessing, investigating or following up on a report under this Policy shall also be protected against retaliation, threats, intimidation, discrimination, or any adverse treatment resulting from the performance of their duties under this Policy.
In jurisdictions where applicable law so provides, any detrimental measure taken against a reporting person following a report may be presumed to constitute retaliation, unless CBTW can demonstrate that such measure was based on duly justified grounds unrelated to the report.

This may result in disciplinary action against the offender, including the issuance of a formal warning or reprimand, suspension or termination of employment or service with CBTW.

Please be aware that this protection under this Policy applies solely to the act of reporting. This will however not prevent CBTW from taking actions against an employee or any other person, outside the scope of the Policy. Accordingly, where a Whistleblower is subject to measures arising from independently established performance issues or unmet promotion criteria, such measures shall not be considered retaliatory and fall outside the scope of this Policy's protections.

3.2. Data protection and confidentiality of the Whistleblower

The Whistleblower is also protected in terms of non-disclosure of his/her identity.

The identity of the Whistleblower will not be disclosed to anyone beyond CBTW's Ethics Committee (cf. Infra point 6). Information can only be disclosed when there is a necessary and proportionate obligation imposed by the law.

Reporting will be stored for no longer than it is necessary and proportionate in order to comply with the requirements of the EU Directive concerning the Protection of Whistleblowers.

3.3. Right of the alleged wrongdoer in the report

The alleged wrongdoer (about whom the reporting will be) may not be prejudiced prior to the deliberation of the Ethics Committee.

The alleged wrongdoer has the legal right to enjoy an effective remedy and a fair trial, the presumption of innocence and the right of defense (which entails the right to be heard and the right to access their file).

4. What incidents/breaches can be reported?

In accordance with the European Whistleblower Directive, a range of breaches can be reported via our Whistleblower reporting tool. These are the standards of the Directive, which can be adapted by the member states where CBTW operates. For reporting concerning Germany, the scope of reportable breaches shall also include all matters falling within the material scope of the German Whistleblower Protection Act (Hinweisgeberschutzgesetz), including criminal offences, certain administrative offences, violations of legal provisions protecting employees, and other breaches covered by applicable German and European legislation.
CBTW has voluntarily expanded the list of eligible reporting based on its CSR policies, including anti- harassment and anti-discrimination policies.

The scope of breaches that can be reported :

- Actual or potential breaches.
- Breaches which have already taken place, or which have not yet materialized, but are very likely to take place.
- Acts or omissions which the Whistleblower has reasonable grounds to consider as breaches.
- Attempts to conceal breaches.

Type of incidents/breaches that can be reported :

- Bribery & corruption: Any type of corruption (active or passive) is strictly prohibited within CBTW. Active corruption is the act of offering advantages without right (offers, promises, gifts, donations) to a person so that he/she accomplishes or abstains from accomplishing an act of his/her function, mission or mandate. Passive corruption is the fact of taking advantage of your position to solicit or accept these advantages in order to accomplish or abstain from accomplishing an act of your position, mission or mandate.

- Breaches of competition law: This entails illegal contacts and agreements, also known as cartels. Some examples are price fixing, market sharing, agreements on customer allocation or distribution agreements between supplier and re-seller where the price charged to customers is imposed by the supplier. This breach can also be the abuse of a dominant position like charging unreasonably high prices which would exploit customers or charge unrealistically low prices which would drive competitors out of the market.
- Conflict of interests: Conflict of interests is a situation where an employee's private interest influences and competes with his or her job-related decisions.
- Fraud: Deception or evasion of the law in order to obtain a benefit or consent that would not have been obtained if the rules of law had been followed. There are different types of fraud such as fraud against the law or tax fraud.
- Financial crimes: This entails not only bribery, corruption and fraud (cfr. Supra), but also terrorist financing, market abuse and insider dealing.
- Harassment (moral or sexual): Any unwanted conduct related to the sex of a person of any form of unwanted verbal, non-verbal or physical conduct with a sexual connotation, with the purpose or effect that the dignity of the person is being violated, especially when a threatening, hostile, insulting, humiliating or offensive situation is being created. This can also include unwanted sexual acts and requests to carry out sexual acts, physical contact of a sexual nature, comments of a sexual nature, as well as the unwanted showing or public exhibition of pornographic images, which takes place with the purpose or effect of violating the dignity of the person concerned, in particular where it creates an intimidating, hostile, degrading, humiliating or offensive environment. Moral harassment can be defined as when you are treated in a manner that is hostile, either in words or in writing, and if this affects your dignity, your physical or psychological well-being, jeopardizing your employment and damaging your physical or mental health.
- Discrimination: This is defined as the unequal and unfavorable treatment of persons on the basis of unfounded criteria such as ethnicity, culture, gender, sex, religion, beliefs, nationality, age, sexual orientation, physical or mental disability, family status, political opinion, union activity, etc.

- Physical violence in the workplace: This is an act with the intent or consequence of physical pain and/or injury. Physical violence includes the following acts, but is not limited to: beating, burning, kicking, punching, biting, maiming or killing, using objects or weapons.
- Violation of Human Rights (e.g, forced labour, child labour) and Fundamental Freedoms (e.g, freedom of association, freedom of

expression) or any situation arising from an employment relationship, under applicable local laws, that could constitute a criminal offense.
- Serious or intentional breaches that compromise the confidentiality, integrity, or availability of personal data, particularly where such breaches may result in significant harm to individuals or violate applicable data protection laws (e.g., GDPR).

For all the above types of breaches that are part of our Whistleblowing Policy, the breaches do not necessarily have to be proven and verified. However, the reported cases cannot be simple assumptions without reasonable basis. Any person who is aware of a breach described in this section is encouraged to report it to the Ethics Committee (cfr. Infra point 6), which will be in charge of handling the reporting. Therefore, if the breach is identified by the Whistleblower as one of the type of breaches set out in this section and falls within the scope of a valid breach, then it can and should result in a reporting.

5. How to report an incident/breach

CBTW has set up a tool dedicated to whistleblowing (WhistleB, Whistleblowing Centre) and encourages Whistleblowers to use it by submitting internal reporting. For people outside the organization, the link is available on the different CBTW ecosystem websites at the following addresses CBTW.

For employees, the link is available on the Positiveapp at the following address in the "useful links" section.

CBTW encourages the Whistleblower to do an internal reporting via the Whistleblowing tool. This tool is designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the Whistleblower and any third party mentioned in the reporting is protected, and prevents access thereto by non-authorised staff members.

- As soon as the Whistleblower becomes aware and has reasonable grounds to believe that there is a breach or that a breach is likely to occur, CBTW encourages the Whistleblower to do a reporting through the internal Whistleblowing tool.
- When the Whistleblower reports a breach, he/she must make sure that its findings are true and accurate with a description that is as precise as possible. The breach must be clearly identified and if possible, with the appropriate documentary evidence. The tool provides a possibility to add documents, recordings and even voice notes. However, if the Whistleblower does not have substantial evidence, but knows for a matter

of fact that there are reasonable grounds of suspicion, those genuine concerns are also encouraged to be reported.
- The reporting will be received by CBTW's Ethics Committee (cf. Point 6). This Ethics Committee will be held at Group Level. The Whistleblower will get an acknowledgement of receipt in 7 days after the reporting. Every communication will be done via the Whistleblowing tool.

6. Who is in charge of the treatment of the reporting ?

CBTW has designed an Ethics Committee to handle all the received reporting. This Ethics Committee consists of permanent case managers who are in charge of collecting all the alerts on the tool and of ad-hoc case managers who are mobilized for the resolution of specific cases.

If the alleged wrongdoer is someone from the Ethics committee, that person will be suspended from its task until there has been made a decision on the case by the other members of the Ethics committee and the ad-hoc case managers.

Permanent case managers

The permanent case managers are the central body of the Ethics Committee. They are two members of the legal and the CSR officer at group level. They will collect all the reporting made via the tool and send out an acknowledgement of receipt to the Whistleblower. They are also in charge of identifying the ad-hoc case managers who will ensure the local follow-up of the case, and make sure that the procedure is done in time.

Ad-hoc case managers

Ad-hoc case managers are people attached to the Ethics Committee and who will be in charge of the investigation of particular cases. They are appointed on 3 main criteria :

- Their location: where the breach took place.
- Their impartiality regarding the case and persons involved in the breach.
- Their competence to deal with the case.

They oversee all investigations related to the breach and are supported by the Ethics Committee. They are the privileged intermediaries of the Whistleblower. They only have access to cases to which they were appointed to.

7. Investigation of the reporting

Once the reporting is well received via the tool, the Ethics Committee will assess it to determine whether the reporting falls within the scope of this Policy.

7.1. Out of the scope of this policy

If the reported breach does not fall within the scope of this Policy, the Whistleblower will get a notification saying that this case will not be handled internally.

7.2. Within the scope of this Policy

- If it concerns a breach falling inside the scope if this Policy, the permanent case managers of the Ethics Committee will designate an impartial person or department as ad-hoc case manager for each specific case, who will do the follow-up of the reporting, or in some cases an external attorney to the company. This impartial person or department will not be a person mentioned in the reporting. These people or department will maintain communication with the Whistleblower through a secure inbox via the Whistleblowing tool and can ask for further information from and provide feedback to the Whistleblower. Per specific case or breach, another person or department can be appointed as ad-hoc case managers to do the investigation and follow-up.

- The investigation will be initiated if there is sufficient evidence to indicate that a breach has occurred. The investigation will consist out of the evaluation of documents (including the information and evidence received by the Whistleblower), as well as interviews with employees and potential further discussions with the Whistleblower and possibly with the alleged wrongdoer. While conducting the investigation, the Ethics Committee will make sure this is always compliant with labour law, confidentiality and data protection requirements.

- All reports shall be documented in a complete and accurate manner. Reports made orally shall be recorded through a written transcript or summary. Where required by applicable law, the reporting person shall be given the opportunity to review, correct and confirm the record of the report. Such documentation shall be retained only for as long as necessary in accordance with applicable legal and data protection requirements.

- Once the investigation is completed, the ad-hoc case manager will revert back to the Ethics Committee. A decision will be made together, and if necessary, with the Management, and can include but will not be limited to, any of the following:

    - the rejection of the reporting;
    - directing the concerns or any part thereof for consideration under other internal procedures or disciplinary procedures, if appropriate and applicable;
    - resolution without recourse to an investigation;
    - directing investigations on the reporting and any persons involved or implicated;
    - suspending the alleged wrongdoer or any other implicated person from work to facilitate any fact finding or to avoid any employee's exposure to threat or harm;
    - obtaining any other assistance (for instance, external auditors or legal advice); and
    - referral to the police or any other appropriate enforcement authority.

• The Whistleblower will get feedback in a timeframe of maximum 3 months starting from the acknowledgement of receipt.

8. Anonymity

Alerts have the possibility to be reported anonymously in countries that have allowed this option in their national legislation.

The anonymous option is directly set in the tool according to which country the Whistleblower is located in, to make sure there can be no confusion for the user of the tool.

9. Amendments of the Policy

This policy is adopted by the Board of Directors of each entity and shall be formally approved by the competent body of each entity listed in Section 1. Each entity is responsible for its local implementation, including, where applicable, the prior consultation of employee representative bodies and the adaptation to national legal requirements. Any substantial amendments shall follow the same validation procedure.