

WHISTLEBLOWER'S GUIDE

I. Context

In line with its CSR policy to promote respect for human rights and business ethics, the CONDAT Group has set up a whistleblowing system, enabling group's employees, customers, suppliers, and partners to report criminal behaviour that has not been dealt with in the usual way, either at CONDAT (and its subsidiaries) or at its partners.

The aim of the system is to encourage everyone to report situations and behaviour that are contrary to the charter of respect for human rights, the group's code of ethics and the applicable laws and regulations.

Bad behaviour in business threatens the foundations of the business. So reporting a problem can minimise the potentially negative impact it could have on the company, its working environment, its employees and its customers.

II. Who can submit an alert?

The system is open to all employees of the group as well as to third parties (whether natural or legal persons such as subcontractors, suppliers, agents, customers, etc.) with whom the group has an established relationship.

The whistleblower may decide not to disclose his/her identity and to report anonymously, provided that this does not prevent the report from being processed.

III. What are the relevant facts?

The following facts are likely to be the subject of an alert

- A crime (e.g., aggravated robbery, attack, rape, torture, ...).
- An offence (e.g., fraud, corruption, misuse of company assets, unlawful conflict of interest, moral or sexual harassment, discrimination, sexual assault, etc.).
- A serious and manifest violation of an international commitment, such as the Universal Declaration of Human Rights (e.g., forced labour or child labour).
- A serious and manifest violation of the law or regulations.
- A threat or serious damage to the general interest.
- Conduct or situation contrary to the Group's code of ethics.
- Any serious infringement of human rights and fundamental freedoms, human health and safety or the environment, resulting from the activities of the group as well as from the activities of subcontractors or suppliers with whom there is an established business relationship, where these activities are related to that relationship.

Definitions and examples are given on the platform for each of these categories to best guide you in your alert.

The events reported may have already occurred or may be about to occur (e.g., environmental risk due to non-compliance with safety rules). The person reporting may be directly involved in the incident or may simply be a witness to it.

Exclusion:

Cases covered by national defence secrecy, medical secrecy or attorney-client privilege are excluded from the whistleblowing process.

IV. How to raise an alert

If reporting through the usual channels (chain of command, commercial contact) is inappropriate or has not been dealt with, or if the whistleblower is under pressure, the alert can be submitted to this address:

<https://www.signal.condat.fr>

This link is accessible 24/7 from any connection (computer or smartphone). It is unique for all employees of the group and for all third parties.

All information, including personal information, is encrypted, and stored in an independent secured environment.

The whistleblower is advised to give his or her identity to be able to benefit from the protection afforded to him or her (see point VI). However, he/she can choose to remain anonymous (anonymous reporting is preferable to keeping information to itself), in which case he/she can always exchange information with the person handling the alert via an anonymized and secured exchange space. This information system does not rely on a standard messaging system, the information communicated is encrypted and does not leave the secured system.

In his or her report, the author must describe as objectively as possible and in detail the situation of which he or she has **personal** knowledge.

To enable the alert to be dealt with effectively, the author should indicate as precisely as possible:

- What is the nature of the event(s) reported and where did they occur.
- When and how he became aware of the situation reported.
- The facts, information, or documents, whatever their form or medium, which may support the alert.
- Which persons or third parties are concerned.
- The possible impacts that the event could have.

The author is guided on the platform, throughout his report, via a questionnaire allowing him to complete and detail all these elements.

V. How the alert is handled

All alerts received will be acknowledged within 7 days at the latest.

All alerts received are subject to an admissibility review. This allows us to check that the alert corresponds to the criteria defined by this guide and that the elements provided allow us to investigate and confirm or deny the facts reported. During this phase, additional information may be requested from the author of the alert.

It should be noted that no report will be accepted if the facts are already the subject of legal proceedings.

If the alert is not admissible, the author is informed via the "dialog box" at the latest two months after receiving the alert.

The author of the alert will also be informed within two months if his or her alert is considered admissible and is therefore investigated further. He or she will then be regularly informed of the follow-up of his or her case, unless legal obligations or the need for confidentiality or protection of individuals prevent precise details of the alert, its processing, or its author from being given.

VI. What are the guarantees for the whistleblower?

The identity of the whistleblower and of the persons concerned by the alert, as well as the information collected by all the recipients of the alert, shall be treated in strict confidence.

The whistleblower is not criminally liable if he/she has acted in a disinterested manner (without consideration) and in good faith (truthfulness, absence of defamation) concerning the facts of which he/she has personal knowledge and which he/she has reported in compliance with the reporting procedure.

The whistleblower may not be sanctioned, dismissed or be the subject of any reprisals or discriminatory measures, whether direct or indirect, particularly regarding remuneration or professional promotion.

Any person who believes that he or she has been subject to retaliation for reporting or participating in the processing of a report under this scheme may report it to the Group's Human Resources Department.

VII. Sanctions

Misuse of the device may result in possible sanctions or prosecution.

The following facts may give rise to a sanction which may go as far as the termination of the employment contract and/or an action for compensation, depending on the case:

- Making a slanderous or bad faith report with malicious intent.
- Making an alert in violation of national defence secrecy, medical secrecy, and lawyer-client privilege.
- Obstructing by action or inaction a report or its treatment.
- Violating the obligation of strict confidentiality when receiving or processing an alert.
- Retaliating against or threatening to retaliate against the person who reported the incident, a person involved in the handling of the incident or their relatives.

No employee may be sanctioned for not using the system.