ETHICAL WHISTLE-BLOWING SYSTEM

PROCEDURAL RULES AND POLICIES RELATING TO THE BUSINESS CODE OF CONDUCT

DECEMBER 2021

Reference : #104

Document version : 1

econocom

Contents

Please note:

The content of this memorandum may not correspond exactly to the laws of certain countries. Wherever legislation in force stipulates provisions that are stricter than the content of this memorandum, such legislation takes precedence. In the opposite case, the rules set forth in this memorandum apply, unless this results in unlawful activity.

1 Context and Purpose

This memorandum explains Econocom's ethical whistle-blowing system and the terms under which alerts received are processed.

Econocom introduced a whistle-blowing platform to strengthen its policy of vigilance in the face of ethical risks. This system is used to collect and process alerts about incidents that breach the group's Business Code of Conduct and/or regulations that apply to the group.

The system is based on EU directive 2019/1937 of 23 October 2019 on protection of whistle-blowers. For France, it upholds the provisions designed to better protect whistle-blowers' rights, laid down by French law 2016-1691 of 9 December 2016 on transparency, anti-corruption efforts and modernisation of business life, known as the Sapin II law. In countries with legal provisions that are more protective, the provisions stipulated in local law take precedence over those set forth in this memorandum.

2 General Principles

2.1 Who can trigger an alert?

The whistle-blowing system is available to anyone who works in the Econocom group (directors, employees, temporary workers, interns, etc.) and to any external third-party who has business relations with the group.

No-one is obliged to trigger an alert. No employee can be penalised for not reporting a breach.

2.2 What incidents does the whistle-blowing system concern?

The ethical whistle-blowing system has been introduced to receive alerts about incidents that constitute a:

- crime or offence;
- serious, obvious breach of a law or rule, or of an international pledge regularly ratified or approved by the country or countries concerned by the incident the alert reports;
- serious violation, or risk of serious violation, of human rights and fundamental freedoms;
- breach of the group's Business Code of Conduct or procedures and policies relating to the latter;
- threat, or serious detriment to, public interest (e.g. detriment to public health, to public security, to the environment, etc.).

Incidents or information kept secret by national military confidentiality, by medical confidentiality or by confidentiality between a lawyer and their client may not be the subject of an alert.

2.3 Who should you contact and how can you contact them?

The whistle-blowing system complements other existing channels for triggering alerts in the Econocom group (line manager, human resources, etc.).

Anyone wishing to report an incident that breaches the group's Business Code of Conduct and/or regulations that apply to the group can report it to:

- Their direct or indirect line manager
- Their contact person in HR or legal affairs if need be
- The group's Ethics Committee if need be

Any admissible alert brought to the attention of a line manager, human resources or the legal affairs department should be immediately sent to the Ethics Committee.

The whistle-blowing platform through which alerts can be triggered is available at the following URL address:

https://report.whistleb.com/fr/econocom

If you have any doubts or questions, you can e-mail the Ethics Committee at: ethical.committee@econocom.com

2.4 How does the whistle-blowing system work?

The platform is secure and the process for triggering alerts is encrypted and password-protected.

When an alert is triggered, the platform automatically generates a username and password. The person who triggered the alert should keep this information to sign back into the platform to edit or complete their alert or track its progress.

The whistle-blowing system is available twenty-four hours a day, seven days a week, in several languages, including French, English, Spanish and Italian. It can be accessed from a computer, tablet or smartphone.

2.5 What information should be sent?

For an alert to be admissible, the incident reported should be explained clearly, objectively and as exhaustively as possible. Any document backing up the alert can be sent via the platform.

Anonymous alerts are possible but not recommended. Anonymous alerts shall only be considered admissible if they help determine with certainty the seriousness of the incident reported and provide facts that are sufficiently detailed. If anonymity makes it impossible to process the alert, the person who triggered the alert is informed of this.

The form to fill in on the platform is as follows:

- Would you like to state your identity?
  yes/no
- If yes:
  first name, surname, e-mail address, telephone number, date of birth
- What is your status?
  victim, direct witness, neither of these
- In which country are you based?
- What is the topic of your alert?
  fraud, corruption, conflict of interest, discrimination, harassment, ill treatment, other

- When did the incident occur?
- Where did the incident occur? (country/town)
- Case details (obligatory)

When you trigger an alert, it is recommended that you:

- use a personal device rather than a professional device and do so in a safe place;
- delete the internet browser's history after sending the alert.

2.6 What protection is provided when an alert is triggered?

Legal protection of whistle-blowers covers anyone who triggers an alert, even if the incident reported turns out to be unfounded, provided that the person is eligible for whistle-blower status (see below).

They are then guaranteed:

- no retaliation from the Econocom group, whether direct or indirect: no retaliatory measure (e.g. reduction in salary, disciplinary measure, dismissal, etc.) relating to the alert can or will be taken against them – if the whistle-blower believes the Econocom group is retaliating in some way, the former will enjoy dispensation from the burden of proof of retaliation;
- confidentiality of their identity and of the incident reported.

Anyone who believes they have been the subject of retaliation for having triggered an alert or for having helped process it can report such retaliation to the Ethics Committee.

The identity of the person who triggered the alert cannot be shared with the person who the alert accuses, unless the person who triggered the alert has given their approval for it to be shared with them.

It is forbidden to obstruct an alert. Anyone who prevents a whistle-blower from triggering their alert risks being the subject of disciplinary and penal measures. However, **abuse of the system or the triggering of a libellous alert, can expose the perpetrator of such abuse or libel to disciplinary measures and legal proceedings.**

<u>Eligibility for whistle-blower status</u>

Pursuant to EU directive 2019/1937 of 23 October 2019, anyone who triggers an alert enjoys protection covering whistle-blowers, provided that:

- they have reasonable grounds to believe, in light of the circumstances and the information they have when triggering the alert, that the incident they report truly occurred;
- they triggered their alert in line with the provisions the directive stipulates.

Pursuant to French law no. 2016-1691, known as the Sapin II law, a whistle-blower should meet the five following cumulative criteria:

They should:

- **be a natural person**: a legal entity (e.g. an association, a trade union, etc.) cannot be considered a whistle-blower;

- **act in good faith**: they should not be driven by malice;
- **act with disinterest**: they should not enjoy any advantage and not be paid in return for their alert;
- **have first-hand knowledge of the incident** they denounce: they should have directly observed the incident they report – they should not just deduce or surmise that the incident they reveal took place, they should not act as an intermediary for an employee who refuses to trigger an alert, and they should not simply repeat information already revealed;
- **reveal a serious incident**: the incident they denounce should be one that breaches the Business Code of Conduct and/or regulations that apply to the Econocom group.

2.7 What happens when an alert is triggered?

When an alert is triggered, it is instantly sent to the ethics officers. Within seven working days from receipt, these ethics officers confirm they have received the alert, and within a month they decide on its admissibility.

To help decide on the alert's admissibility, the ethics officers may ask the person who triggered the alert for clarifications via the whistle-blowing system.

Only objective information covered by the whistle-blowing system's scope[1] will be considered in assessing alerts received.

Scenario 1: The alert is deemed inadmissible:

- the person who triggered the alert is told their alert is inadmissible;
- the procedure is terminated, the data anonymised and archived.

Scenario 2: The alert is deemed admissible:

- the alert is sent to the Ethics Committee who determines how to follow it up;
- the person who triggered the alert is told their alert is admissible; they are also told the alert procedure has been brought to a conclusion;
- the person accused is told about the accusations against them, but not in the whistle-blower's name, once Econocom has completed its investigation and taken measures to prevent destruction of proof; they are also told the alert procedure has been brought to a conclusion;
- if the alert is not followed up with a disciplinary procedure or legal proceedings, the data relating to that alert is anonymised then archived within two months from the checks ending;
- if a disciplinary procedure begins or legal proceedings are set in motion against the person accused or the perpetrator of an improper alert, the investigator keeps the data relating to the alert until the procedure has been brought to a conclusion.

If the Ethics Committee deems the alert should be followed up with an enquiry, it defines the framework of the investigation and its terms (documents that could be used, expert in charge of processing, etc.).

If someone involved in processing an alert encounters a difficulty, this difficulty is reported to the Ethics Committee, who makes a decision about it.

[1] As specified in § 2.2 What incidents does the whistle-blowing system concern?

Access to alerts triggered via the platform is limited to people accredited to receive or process alerts.

The receipt, processing and consequences of alerts are reported to the Audit Committee at least once a year.

3 Confidentiality and Protection of Personal Data

3.1 Confidentiality

The Econocom group undertakes to strictly respect the confidentiality of any whistle-blower's identity and any incident an alert reports and any person it accuses.

Only with a whistle-blower's consent may aspects that identify that whistle-blower be revealed, except in the case of revealing them to legal authorities. If a whistle-blower's refusal to allow such aspects to be shared makes it impossible for the alert to be processed, the whistle-blower is informed of this.

Only once the soundness of an alert has been confirmed may aspects that identify the person the alert accuses be revealed to people outside the processing of the alert, except in the case of revealing them to legal authorities.

These provisions in confidentiality apply to all people who are aware of an alert triggered, including when the processing of the alert requires communication with third parties.

Particular measures are taken to ensure confidentiality while an alert is being processed (written reminder of confidentiality rules and penalties in the event of these rules being breached).

3.2 Protection of personal data

Data collected as part of the Econocom group's whistle-blowing system is the subject of processing that seeks to receive and track work-related alerts in line with EU directive 2019/1937 of 23 October 2019 on protection of whistle-blowers and in line with locally applicable provisions, including French law 2016-1691 of 9 December 2016 on transparency, anti-corruption efforts and modernisation of business life, known as the Sapin II law. The lawfulness of the processing is therefore the legal basis.

From the moment when the alert is triggered, access to personal data is strictly limited to people working in alert management in the Econocom group, to needs in checks and in processing alerts, and to legal authorities.

The following conditions determine the duration for which personal data is kept:

- if the alert is not followed up on, the personal data involved is destroyed within two months from when the alert procedure is brought to an end
- if the alert is followed up on, the personal data involved is kept until the end of the procedure then archived in line with legal provisions in force

The person responsible for processing is the company representative.

Pursuant to France's data protection law of 6 January 1978, as amended, and to the General Data Protection Regulation (EU regulation no. 2016/679 of 27 April 2016), the whistle-blower – if they have not remained anonymous – or the person accused by the alert have the right to gain access to data about them and may ask for this data to be modified or deleted if it is incorrect, incomplete, ambiguous or outdated. This right cannot be exercised to prevent Econocom from fulfilling its legal obligations in processing alerts and protecting whistle-blowers.

The Data Protection Officer can be contacted at the Econocom group's head office: DPO – 40 quai de Dion Bouton, 92800 Puteaux, FRANCE.