

# ETHICAL WHISTLEBLOWING SYSTEM

PROCEDURES AND POLICIES RELATING TO  
THE CODE OF BUSINESS CONDUCT

APRIL 2025

APPENDIX NO. 2 TO THE INTERNAL

Reference: #104  
Document version: 1

econocom

# Contents

1	Background and objectives	3
2	Glossary	3
3	Internal whistleblowing system	4
3.1	Who can file a whistleblowing report?	4
3.2	What incidents are covered by the whistleblowing system?	4
3.3	Who to contact and how?	5
3.3.1	Internal whistleblowing system	5
3.3.1.1	Reporting via the internal whistleblowing platform	5
3.3.1.2	Reporting by post or e-mail	6
3.3.1.3	Oral reporting	6
3.3.1.4	Anonymous reporting	7
3.3.2	Other internal reporting channels	7
3.3.3	External reporting channels	7
3.4	Who handles whistleblowing reports?	7
3.5	What information should you provide?	8
3.6	What happens after a whistleblowing report has been filed?	9
3.6.1	Confirmation of receipt	9
3.6.2	Examination of admissibility of the whistleblowing report	9
3.6.3	Handling the merits of whistleblowing reports	10
3.7	What protection is granted following a whistleblowing report?	11
4	Protection of personal data and confidentiality	11
4.1	Confidentiality	11
4.2	Protection of personal data	12
5	Measures and sanctions	13
6	Scope of Application	13
6.1	Annex 1: Spanish Law specificities added to the “Ethical Whistleblowing system”	14
6.2	Annex 2: Italian Law specificities added to the “Ethical Whistleblowing system”	15
6.3	Annex 3: Dutch Law specificities added to the “Ethical Whistleblowing system”	20
6.4	Annex 4: German Law specificities added to the “Ethical Whistleblowing system”	21

# 1 Background and objectives

In the scope of its ethical risk prevention policy, Econocom has implemented an internal whistleblowing system to enable its employees and any person fulfilling the criteria set out in this procedure to report or disclose information concerning situations that are contrary to the Group's Code of Business Conduct and/or the rules applicable to the Group. To this end, Econocom has implemented a secure whistleblowing platform for all Group entities to guarantee the confidentiality of the information disclosed.

The internal whistleblowing system is based on 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, Act no. 2016-1691 of 9 December 2016 on transparency, combatting corruption and modernising economic life, referred to as "Sapin II Act", amended by Act no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers and Decree no. 2022-1284 of 3 October 2022 and Act no. 2017-399 of 27 March 2017 on the duty of care of parent companies and ordering companies (1). In countries with more protective provisions, the provisions of local law take precedence over the provisions under this system.

This procedure applies to all divisions, departments, services, entities, agencies, directly or indirectly controlled subsidiaries, representative offices and branches of Econocom Group, hereinafter referred to as "Econocom Group".

It applies to all employees, whether casual or permanent, all persons acting in the name of or on behalf of Econocom Group, regardless their status or position in the organisation (corporate officers, agents, etc.), and all of its external stakeholders (service providers, partners, suppliers, subcontractors, etc.).

## 2 Glossary

**Ethics Committee:** the body responsible for compliance within Econocom Group. It has general remits for all issues relating to ethics and compliance, as well as handling and monitoring of whistleblowing reports submitted in the scope of the whistleblowing system, conflicts of interest, and the proper appropriation and understanding of ethical and compliance principles by Econocom Representatives and all stakeholders (customers, suppliers, partners, agents, etc.).

**Ethics Correspondent:** an ethics correspondent is appointed in each entity/region. He/she acts as an intermediary for the Ethics Committee and ensures that the rules, principles and procedures implemented by Econocom Group are applied and complied with.

**Recipient of the whistleblowing report:** the Whistleblowing Officer (via the internal whistleblowing platform), the direct or indirect line manager, the whistleblower's HR contact person, the Group Compliance Officer, the Group General Counsel and the Ethics Committee.

**Personal data:** means any information relating to an identified or identifiable natural person.

**Facilitator:** means any natural person or any private non-profit-making legal entity providing assistance and support to the whistleblower in the process.

**Econocom Group:** all companies controlled directly or indirectly by Econocom Group.

**Whistleblower:** means any person belonging to a category referred to in §3.1 below who reports or discloses, in good faith and without any direct financial compensation, information relating to an incident set out in §3.2.

**Whistleblowing platform:** means the whistleblowing platform set up by Econocom Group to collect and handle all reports. This platform can be accessed at the following address: <https://report.whistleb.com/fr/econocom>.

**Whistleblowing Officer:** persons appointed by the Ethics Committee for their expertise and experience in compliance issues and who are involved in the whistleblowing process. The Whistleblowing Officer has access to the whistleblowing platform. In this capacity, he/she is responsible for receiving the whistleblowing report and analysing the admissibility of the report in view of legal requirements. The Whistleblowing Officer may liaise with the whistleblower and, where appropriate, the person who is the subject of the whistleblowing report, in accordance with the Ethics Committee's instructions, in addition to the whistleblowing platform provider. The Whistleblowing Officer may contribute to the investigation further to a decision by the Ethics Committee.

## 3 Internal whistleblowing system

### 3.1 Who can file a whistleblowing report?

The whistleblowing report collection and handling system is available to all Econocom Group stakeholders:

- Internal: casual employees (Econocom Group trainees, temporary workers, work-study students), permanent employees, former employees or job applicants).
- External: external collaborators, service providers, partners, suppliers, subcontractors, etc.

Whistleblowing is not compulsory - no employee can be penalised for failing to report misconduct - but it is strongly recommended.

Whistleblowers may be assisted by a facilitator in filing their report or disclosure. The facilitator will be eligible for similar protection as afforded to whistleblowers. A facilitator is a natural person (e.g. a relative or colleague) or any private non-profit-making legal entity (e.g. an association or trade union) providing help to the whistleblower in filing a report or making a disclosure. The facilitator must be able to demonstrate that he/she provided assistance to the whistleblower in compliance with the reporting rules laid down by law.

### 3.2 What incidents are covered by the whistleblowing system?

Cumulative conditions relating to the whistleblower and the alleged incidents in the whistleblowing report must be fulfilled in order to grant whistleblower status to the person filing the report and consequently enabling him/her to be eligible for the legal protection connected thereto.

The whistleblowing report must relate to incidents that have occurred or are likely to occur within Econocom Group in connection with its operations and operations of subcontractors, partners, service providers or suppliers and relating to:

- Crime or misdemeanour (e.g. probity breach, moral harassment, sexual harassment, or any other offence that could be classed as a crime or misdemeanour).
- Threat or harm to the general interest.
- Breach or attempted concealment of a breach of an international commitment duly ratified or approved by France, a unilateral act by an international organisation taken on the basis of such a commitment, or European Union law.
- Breach or attempted concealment of a breach of the law or regulations.
- Non-compliance with the rules of the Group's Code of Business Conduct and/or the procedures and policies relating to it.
- Breach of human rights and fundamental freedoms, health and safety of individuals and the environment.

The whistleblowing system does not apply to incidents, information and documents, in any format or on any medium, whose revelation or disclosure is prohibited by provisions on:

- National defence secrecy,
- Medical confidentiality,
- Judicial secrecy,
- Confidentiality of the judicial investigation or inquiry,
- Solicitor-client privilege.

Whistleblowers must be natural persons, who act in good faith and receive no direct financial compensation for their disclosure. It is not necessary to have had personal knowledge of the information reported in the whistleblowing report if it was obtained in the scope of the professional activity. Nevertheless, personal knowledge is required if the alleged incidents were discovered outside the professional activity.

If the whistleblowing report fulfils the admissibility requirements relating to its scope and the person filing it, whistleblower status can be granted to the person filing the report, which means that he/she is eligible for the legal protection connected to this status. This legal protection prevents any reprisals against the whistleblower in relation to the reported incidents.

However, misuse of the internal whistleblowing system, in particular when the whistleblower knows that the alleged incidents are inaccurate or to denigrate or defame colleagues or management, exposes the whistleblower to disciplinary sanctions and, where appropriate, legal action.

### **3.3 Who to contact and how?**

Whistleblowers can file reports through a number of channels described below.

#### **3.3.1 Internal whistleblowing system**

##### **3.3.1.1 Reporting via the internal whistleblowing platform**

Whistleblowers should use the confidential and secure whistleblowing platform as their preferred method of reporting.

The whistleblowing platform is available at the following URL address:

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

Or via the following QR code:



This Platform is hosted and managed by an external service provider specialising in handling whistleblowing reports and subject to strict confidentiality and security obligations, WhistleB Whistleblowing Centre AB located at World Trade Center, Klarabergsviadukten, 70 or PO Box 70396 SE 107 24 Stockholm, Sweden.

The platform is secure, and the reporting process is encrypted and password protected.

When a whistleblowing report is filed, the platform automatically generates a login and password. This information must be kept by the person who filed the whistleblowing report, so that they can reconnect to the platform to change, add to or monitor the progress of the report.

The whistleblowing platform is available in several languages, including French, English, Spanish and Italian, 24 hours a day, 7 days a week. It can be accessed from a computer, tablet or smartphone.

When creating a whistleblowing report via the platform, we recommend:

- using a personal terminal rather than a professional terminal, and in a safe place,
- clearing the browser history after sending the whistleblowing report.

Access to whistleblowing reports filed via the platform is restricted to persons authorised to collect or handle reports.

#### [3.3.1.2 Reporting by post or e-mail](#)

Reports can also be submitted by post or e-mail, preferably secure (encrypted).

The letter or e-mail must clearly state that it is a whistleblowing report in the subject line or the content.

#### [3.3.1.3 Oral reporting](#)

Reports can be filed:

- By telephone.
- During a private meeting with the recipient of the whistleblowing report, organised no later than 20 working days after receipt of the request from the person filing the report.

The whistleblowing report is confirmed in writing, if there is no reason to preclude this.

In addition, the whistleblowing report may be transferred to the aforementioned platform, with the whistleblower's prior consent.

#### 3.3.1.4 Anonymous reporting

Anonymous reporting is possible but not encouraged. An anonymous whistleblowing report will only be considered admissible if it establishes with certainty the seriousness of the incidents and provides sufficiently detailed factual information. In all cases, whistleblowers who wish to remain anonymous are asked to provide the recipient of the whistleblowing report with the means to exchange information with them so that the incidents giving rise to the report can be investigated.

If the anonymity makes it impossible to handle the whistleblowing report, the person filing the report will be informed.

By using the whistleblowing platform, he/she can remain anonymous.

#### 3.3.2 Other internal reporting channels

The whistleblowing report may also be sent to the following contact persons, except if it relates to the perpetrator of the offending conduct:

- his/her direct or indirect line manager,
- where appropriate, his/her HR contact person,
- the Group Compliance Officer,
- the Group General Counsel,
- the Group Ethics Committee.

Any admissible report made to a line manager, the Human Resources Department, the Group Compliance Officer or the Group General Director must be immediately disclosed to the Ethics Committee via the whistleblowing platform.

If in doubt or you have questions before filing a whistleblowing report, the Legal Department in charge of Compliance can be contacted by e-mail: [ethical.committee@econocom.com](mailto:ethical.committee@econocom.com).

#### 3.3.3 External reporting channels

The whistleblower may also submit an external report, after filing an internal report in accordance with this procedure, or directly to:

- Competent authority among those designated by Decree no. 2022-1284 of 3 October 2022.
- Defender of Rights, who will forward the whistleblowing report to the authority(ies) best placed to handle it.
- Judicial authorities.
- A European Union institution, body, office or agency competent to collect information on breaches falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

Nevertheless, Econocom Group encourages use of the whistleblowing platform as a preferred channel.

### 3.4 Who handles whistleblowing reports?

Whistleblowing Officers have access (logins) to the whistleblowing platform. They receive whistleblowing reports via the platform. They examine the admissibility of the whistleblowing report in view of legal requirements and inform the Ethics Committee.

If the whistleblowing report is admissible, the Ethics Committee will launch and conduct an investigation in accordance with the procedure for investigating and dealing with misconduct applicable within Econocom Group.

The Ethics Committee may transfer the handling of the whistleblowing report to the Country Ethics Correspondent, depending on the nature and/or sensitivity of the report.

Whistleblowing Officers, members of the Ethics Committee and Ethics Correspondents are selected for their experience and expertise. They have the necessary expertise, authority and resources to carry out their duties.

They are subject to a strict confidentiality obligation.

If in doubt regarding the impartiality of a Whistleblowing Officer, a member of the Ethics Committee, an Ethics Correspondent or any other person involved in the handling of a whistleblowing report, due to their relationship with the whistleblower or the person who is the subject of the whistleblowing report, they must inform the Ethics Committee and be removed from the handling of the whistleblowing report. Similarly, this person may ask not to take part in the handling of the whistleblowing report if he/she considers that he/she is not in a position to carry out his/her duties due to his/her closeness or for any other reason relating to the whistleblower or the person concerned or the incidents set out in the report.

### **3.5 What information should you provide?**

The whistleblower must set out the incidents and information that are covered by his/her report in a precise and detailed manner.

Only evidence that directly relates to the areas covered by the whistleblowing system and which is strictly necessary for examining the merits of the whistleblowing report and verification operations is taken into account.

The whistleblowing platform makes it possible to send any information, in any format or on any medium, to substantiate the report, when the whistleblower has such information.

The whistleblower may provide any information enabling him/her to be identified (last name, first name, reporting entity, position, e-mail address, telephone numbers, etc.).

The form to be completed on the Platform is presented as follows:

- Would you like to share your identity?  
yes/no
- If yes:  
first name, last name, e-mail address, telephone number, date of birth
- What is your status?  
victim, direct witness, indirect witness, other situation
- Use the "Add an attachment" tab to send any evidence demonstrating that the whistleblowing report falls in a category for which the Platform is available, unless the report is anonymous.
- Which country are you in?
- Which Econocom Group entity is concerned?
- What is the subject of your whistleblowing report?  
*fraud, corruption, conflict of interest, discrimination, harassment, abuse, breach of human rights and fundamental freedoms, environmental damage, health damage, safety damage, other*
- When did this happen?
- Where did this happen (country/town)

- Details of the incidents, subject of the whistleblowing report (mandatory)

Any document, information or data shared as part of implementing the whistleblowing system but not falling within the scope of the whistleblowing report, is destroyed.

The whistleblower must respect the confidentiality of the whistleblowing report and the person(s) who may be the subject of the report in all circumstances.

## 3.6 What happens after a whistleblowing report has been filed?

### 3.6.1 Confirmation of receipt

The person filing the whistleblowing report will be informed in writing within **seven working days** of receipt of the report by the Whistleblowing Officer. Confirmation of receipt does not mean that the whistleblowing report is admissible.

This confirmation of receipt:

- Is date and time stamped,
- Summarises all of the information and, where applicable, any attachments sent in the scope of the whistleblowing report.
- Specifies the reasonable and foreseeable time frame for giving notice of the admissibility of the whistleblowing report, which may not exceed **ten working days** from the date of confirmation of receipt of the report.
- Specifies how he/she will be informed regarding the action taken further to his/her report (via the Platform, by post or secure e-mail).

### 3.6.2 Examination of admissibility of the whistleblowing report

The Whistleblowing Officer examines the admissibility of the whistleblowing report by checking that the report meets the admissibility requirements set out in this procedure (criteria relating to §3.1 and §3.2).

He/she may request any additional information from the person filing the whistleblowing report before examining the merits of the report, where applicable. He/she acts on the Ethics Committee's instructions in all circumstances. All whistleblowing reports submitted, and the examination of admissibility are forwarded to the Ethics Committee.

Only objective information falling within the scope of the<sup>1</sup> whistleblowing system will be taken into account when assessing the admissibility of the whistleblowing report submitted.

Case 1: the whistleblowing report is deemed inadmissible:

- The person filing the whistleblowing report will be informed regarding the reasons why the Ethics Committee considers that the report is inadmissible and the closure of the report. This information will be provided within a reasonable time frame, which may not exceed **ten working days** from confirmation of receipt of the whistleblowing report.
- The procedure is closed, and the data is archived after anonymisation.

This procedure also applies when the whistleblowing report is anonymous.

Case 2: the whistleblowing report is deemed admissible:

<sup>1</sup> As specified in § 3.2 What incidents are covered by the whistleblowing system?

- The person filing the whistleblowing report will be informed regarding the admissibility of his/her report within a reasonable time frame, which may not exceed **ten working days** from the date of confirmation of receipt of the report.
- The Ethics Committee handles them.

### 3.6.3 Handling the merits of whistleblowing reports

The Ethics Committee will launch and conduct an investigation in accordance with the procedure for investigating and dealing with misconduct applicable within Econocom Group.

In order to assess the accuracy of the allegations made, the Ethics Committee may request any additional information from the person filing the whistleblowing report.

The person filing the whistleblowing report will be informed in writing by the Ethics Committee of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy the matter set out in the report, as well as the reasons for these measures, within a reasonable period of time not exceeding **three months** from confirmation of receipt of the report.

When the allegations appear to be substantiated, the Ethics Committee will use the resources at its disposal to remedy the matter.

When handling the merits of a whistleblowing report, the Ethics Committee may carry out any investigation it deems necessary to verify whether or not the report is well-founded. In particular, it may involve the line manager (if this person is not the subject of the report) or any employee whose involvement it deems necessary in the scope of verifying or handling the whistleblowing report, in strict compliance with confidentiality obligations. In the course of its investigations, it may, if it deems necessary, appoint any external service provider, who must comply with the strictest confidentiality requirements.

The Ethics Committee will close the whistleblowing report if the allegations are inaccurate or unfounded, or if the report has become irrelevant. The person filing the whistleblowing report is informed in writing regarding the closure of the file by the Ethics Committee or the Whistleblowing Officer, acting further to a delegation.

The Ethics Committee informs the person who is the subject of a whistleblowing report (witness, victim, alleged perpetrator, etc.) within a reasonable period of time, which may not exceed **one month**, except in duly justified exceptional cases, following the filing of the whistleblowing report. This notice may be deferred where it is likely to seriously compromise fulfilment of the objectives of handling the whistleblowing report, in particular where there is a risk of evidence being destroyed. The notice is subsequently passed on as soon as the risk has been ruled out. It must not contain any information concerning the identity of the person filing the whistleblowing report or third parties. He/she will also be notified regarding the closure of the whistleblowing procedure.

This procedure also applies when the whistleblowing report is anonymous.

If anyone involved in the handling of the whistleblowing report encounters a problem, it will be referred to the Ethics Committee, which will take a decision.

Econocom Group General Management is informed regarding the receipt, handling and follow-up action taken further to whistleblowing reports submitted at least once annually.

### 3.7 What protection is granted following a whistleblowing report?

The legal protection of whistleblowers applies to any person who has been recognised as having whistleblower status under the requirements set out above, even if the reported incidents prove to be unfounded. Facilitators are also eligible for legal protection, particularly against reprisals.

Recognised whistleblowers are consequently guaranteed:

- No reprisals by Econocom Group, or threats or attempts to take disciplinary sanctions such as suspension, dismissal, demotion or refused promotion, etc.
- Confidentiality of his/her identity and the reported incidents.

Any person who considers that they are being retaliated against for filing a report or participating in its handling may report the matter to the Ethics Committee.

**However, misuse of the whistleblowing system or use of the system in bad faith exposes the whistleblower to disciplinary sanctions and legal action.**

It is forbidden to obstruct the filing of a whistleblowing report. Any person who prevents a whistleblower from filing a report is liable to disciplinary and criminal sanctions.

Using the whistleblowing system in good faith will not expose the person filing a report to any disciplinary sanctions, even if the incidents subsequently prove to be inaccurate or do not give rise to any follow-up action.

## 4 Protection of personal data and confidentiality

### 4.1 Confidentiality

This procedure guarantees the integrity and confidentiality of the information collected in the scope of a whistleblowing report, in particular the identity of the person filing the whistleblowing report, the persons who are the subject of this report and any third party referred to in the report, and documents, information or data collected in the scope of the report. Only the Recipients of the whistleblowing report, who are bound by a reinforced confidentiality obligation, will have access to this information, except if a particular requirement applies for the sole purpose of verifying or handling the report, in accordance with legal requirements in force.

The information collected may only be disclosed to third parties if such disclosure is necessary to handle the whistleblowing report and in compliance with the provisions of I of Article 9 of the Act of 9 December 2016 as amended by Act no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers, namely:

Information identifying the whistleblower may only be disclosed with the whistleblower's consent. However, information may be disclosed to the judicial authorities if the persons responsible for collecting or handling whistleblowing reports are obliged to report the incidents to the judicial authorities. The whistleblower is then notified, unless there is a risk that such notice could compromise legal proceedings. Written explanations are attached to this notice.

Information identifying the person who is the subject of a whistleblowing report may only be disclosed, with the exception of the judicial authorities, after it has been established that the report is well-founded.

Breach of the aforementioned confidentiality rules may result in disciplinary sanctions or legal action, depending on applicable laws.

Disclosure of confidential information, such as the identity of the person filing the whistleblowing report, the persons who are the subject of this report and any third party referred to in the report, or the incidents set out in the report, is punishable by two years' imprisonment and a fine of €30,000.

## 4.2 Protection of personal data

Econocom and the legal entity, where the incidents giving rise to the whistleblowing report occurred, in the capacity as joint data controllers, ensure that personal data is processed in accordance with Econocom Personal Data Protection Policy.

### **Purpose of processing:**

Data processing in the scope of the whistleblowing system is carried out by Econocom and all of its subsidiaries in the capacity as joint data controllers for the following purposes:

1/ Collecting and handling whistleblowing reports to meet the requirements of Act 2016-1691 of 9 December 2016 on transparency, combatting corruption and modernising economic life, as amended by Act 2022-401 of 21 March 2022, referred to as the “**amended Sapin 2 Act**”,

2/ Collecting whistleblowing reports to meet the requirements of Article 17.II.2 of the **amended Sapin 2 Act** relating to the existence of conduct and situations contrary to the company's Code of Business Conduct and likely to constitute corruption or influence peddling.

3/ Collecting whistleblowing reports provided for in Article L225-102-4 of the French Commercial Code, deriving from Act no. 2017-399 on the "duty of care", relating to the existence or realisation of risks of serious breaches of human rights and fundamental freedoms, health and safety of individuals and the environment, resulting from the company's operations and operations of companies it directly or indirectly controls, and operations of subcontractors or suppliers with which it has established commercial relationship when these operations are connected to this relationship.

**The legal basis** for processing data to achieve the purposes set out above is a legal obligation applicable to Econocom Group.

**Recipients of the data:** the recipient of the whistleblowing report and any other person who may be involved in handling the report.

### **Duration of storage of personal data:**

Unless otherwise stipulated by law or regulation, personal data is stored and archived for the following periods:

- Data relating to a whistleblowing report is kept in the active database until a final decision is taken on the follow-up action to be taken.
- If no follow-up action is taken further to the whistleblowing report, the personal data is destroyed within two months of the closure of the report.

- In the event of follow-up action, personal data will be kept until the end of the procedure or the time limit for appeals against the decision taken and then archived in accordance with applicable legal provisions.

In countries with more protective provisions, the provisions of local law take precedence over the provisions under this system.

### **Rights of data subjects:**

In accordance with the amended French Data Protection Act of 6 January 1978 and the General Data Protection Regulation (EU Regulation No. 2016/679 of 27 April 2016), all data subjects have the right to access, correct and amend their personal data. This right may not be exercised to prevent Econocom from fulfilling its legal obligations with regard to the handling of whistleblowing reports and protection of the person filing a report.

If a data subject wishes to exercise any of their rights under the GDPR, they may contact the Data Protection Officer (DPO) at [dpo@econocom.com](mailto:dpo@econocom.com).

The data subject may also submit a complaint online to the French Data Protection Authority (CNIL) by post.

## **5 Measures and sanctions**

Proven breaches identified through an internal investigation will be subject to disciplinary sanctions or legal action depending on the seriousness, on a case-by-case basis.

These sanctions are decided by the Ethics Committee, taking into account the incidents and circumstances, in conjunction with Econocom Group General Management and the Human Resources Department. Some functions and/or managers may be consulted for this purpose.

Sanctions applicable to Econocom Group employees are decided and implemented in accordance with applicable disciplinary procedures (and in particular, in France, the procedures set out in the Internal Company Rules).

In the event of a proven breach, Econocom Group may also decide to take legal action before the competent courts.

Proven misconduct and the corresponding sanctions will be reported to the Group General Management.

## **6 Scope of Application**

To ensure better understanding and to respond to local specificities, country-specific annexes have been drawn up.

These annexes consider the legal and regulatory requirements specific to each jurisdiction in which the Group operates. Each country may implement its local policy provided that it complies with the group's policy and the specific requirements described in the annexes.

- Annex 1: Spanish entities
- Annex 2: Italian entities
- Annex 3: Dutch entities
- Annex 4: German entities

## **6.1 Annex 1: Spanish Law specificities added to the “Ethical Whistleblowing system”**

### **3.3.3 External reporting channels**

In the case of Spain, in addition to judicial authorities, the Ombudsman or other competent authorities, the whistleblower may also report to the Independent Authority for Whistleblower Protection, as provided for in Article 14 of Spanish Law 2/2023.”

### **3.4 Who handles alerts?**

For the purposes of Law 2/2023, the Ethics Committee of the Econocom Group is formally appointed as the Internal Reporting System Manager, acting with independence and functional autonomy, in accordance with the provisions of Article 8 of the Spanish Law.

### **4.2 Personal data protection**

In Spain, the data subject may lodge a complaint with the Spanish Data Protection Agency (AEPD) if they believe their rights have been infringed.

## **6. Periodic review and audit of the system**

The internal reporting system shall be reviewed at least every two years, or following significant regulatory changes, to ensure its effectiveness and compliance with all applicable laws. Internal or external audits may be conducted to verify its operation.”

## **7. Regulatory**

Internal reporting channel of Econocom in Spain has been duly registered with the Independent Authority for Whistleblower Protection in accordance with Article 5.2 of Law 2/2023.

## 6.2 Annex 2: Italian Law specificities added to the “Ethical Whistleblowing system”

### 1. Background and objectives

The internal whistleblowing system is based on 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, Italian Legislative Decree 24/2023 (implementing the EU Whistleblowing Directive), Italian Legislative Decree 231/2001, and the Italian National Anti-Corruption Authority (ANAC).

### 2. Glossary

**Ethics Correspondent:** the Legal & Compliance Office of the entity/region acts as the ethics correspondent. It acts as an intermediary for the Ethics Committee and ensures that the rules, principles and procedures implemented by Econocom Group are applied and complied with.

**Whistleblowing Officer:** persons appointed by the Ethics Committee for their expertise and experience in compliance issues and who are involved in the whistleblowing process and designated as authorized to process personal data. The Whistleblowing Officer has access to the whistleblowing platform. In this capacity, he/she is responsible for receiving the whistleblowing report and analyzing the admissibility of the report in view of legal requirements. The Whistleblowing Officer may liaise with the whistleblower and, where appropriate, the person who is the subject of the whistleblowing report, in accordance with the Ethics Committee's instructions, in addition to the whistleblowing platform provider. The Whistleblowing Officer may contribute to the investigation further to a decision by the Ethics Committee.

#### 3.1 Who can file a whistleblowing report?

Whistleblowers may be assisted by a facilitator in filing their report or disclosure. The facilitator will be eligible for similar protection as afforded to whistleblowers. A facilitator is a natural person (e.g. colleague from the same office as the Whistleblower, or from another office - including a colleague who also holds the role of trade union representative - may act as a facilitator, provided that the trade union affiliation is not used in this context) providing help to the whistleblower in filing a report or making a disclosure. The facilitator must be able to demonstrate that he/she provided assistance to the whistleblower in compliance with the reporting rules laid down by law.

#### 3.2 What incidents are covered by the whistleblowing system?

The whistleblowing report must relate to incidents that have occurred or are likely to occur within Econocom Group in connection with its operations and operations of subcontractors, partners, service providers or suppliers and relating to:

- Crime or misdemeanor (e.g. probity breach, moral harassment, sexual harassment, or any other offence that could be classed as a crime or misdemeanor).

- Threat or harm to the general interest.
- Unlawful conduct relevant under Legislative Decree no. 231/2001 and violations of the organization, management and control model (Model 232) pursuant to the same Decree.
- Violations of European Union law (as already listed in the previous version of the Whistleblowing Procedure).
- Breach or attempted concealment of a breach of the law or regulations.
- Non-compliance with the rules of the Group's Code of Business Conduct and/or the procedures and policies relating to it.
- Breach of human rights and fundamental freedoms, health and safety of individuals and the environment.

### **3.3.1.2: Oral reporting**

Reports can be filed:

- During a private meeting with the recipient of the whistleblowing report, organized no later than 10-15 working days after receipt of the request from the person filing the report. The private meeting must take place in a location suitable for ensuring the confidentiality of the Whistleblower. It is always advisable - subject to the Whistleblower's consent - to record the meeting using appropriate devices capable of storing and replaying the recording. If it is not possible to proceed with the recording (e.g. because the Whistleblower has not given consent or appropriate recording devices are not available), a written report must be drafted. This report must be signed by both the Whistleblower and the person who received the report. A copy of the report must be provided to the Whistleblower.

In addition, the whistleblowing report may be transferred to the aforementioned platform, with the whistleblower's prior consent.

### **3.3.1.3: Anonymous reporting**

Anonymous reporting is possible but not encouraged. An anonymous whistleblowing report will only be considered admissible if it establishes with certainty the seriousness of the incidents and provides sufficiently detailed factual information, supported by appropriate documentation. In all cases, whistleblowers who wish to remain anonymous are asked to provide the recipient of the whistleblowing report with the means to exchange information with them so that the incidents giving rise to the report can be investigated.

If the anonymity makes it impossible to handle the whistleblowing report, the person filing the report will be informed.

By using the whistleblowing platform, he/she can remain anonymous.

Anonymous reports must be registered by the recipient of the whistleblowing report for handling the whistleblowing process, and all documentation received must be duly preserved.

Indeed, if the anonymous whistleblower is later identified and has suffered reprisals, he/she must be granted the same legal protections provided for whistleblowers under the applicable framework.

### **3.3.2 Other internal reporting channels**

The whistleblowing report may also be sent to the following contact persons, except if it relates to the perpetrator of the offending conduct:

- his/her direct or indirect line manager,
- where appropriate, his/her HR contact person,
- the local Legal & Compliance Department,
- the Group Compliance Officer,
- the Group General Counsel,
- the Group Ethics Committee.

Any admissible report made to a line manager, the Human Resources Department, the Legal & Compliance Department, the Group Compliance Officer or the Group General Director must be immediately disclosed to the Ethics Committee via the whistleblowing platform.

If in doubt or you have questions before filing a whistleblowing report, the Legal Department in charge of Compliance can be contacted by e-mail: [ethical.committee@econocom.com](mailto:ethical.committee@econocom.com).

### **3.3.3 External reporting channels**

The whistleblower may also submit an external report, after filing an internal report in accordance with this procedure, or directly to:

- the external reporting channel with ANAC (Italian National Anti-Corruption Authority).
- public disclosure.
- report to the judicial authorities.

Nevertheless, Econocom Group encourages use of the whistleblowing platform as a preferred channel.

### **3.6.2 Examination of admissibility of the whistleblowing report**

He/she may request any additional information from the person filing the whistleblowing report before examining the merits of the report, where applicable. He/she acts on the Ethics Committee's instructions in all circumstances. All whistleblowing reports submitted, and the examination of admissibility are forwarded to the Ethics Committee. The Ethics Committee shall promptly inform the Supervisory Body (in Italian "Organismo di Vigilanza") of the legal entity about the report received.

## **4.1 Confidentiality**

This procedure guarantees the integrity and confidentiality of the information collected in the scope of a whistleblowing report, in particular the identity of the person filing the whistleblowing report, the persons who are the subject of this report and any third party referred to in the report, and documents, information or data collected in the scope of the report. Only the Recipients of the whistleblowing report, who are bound by a reinforced confidentiality obligation, will have access to this information, except if a particular requirement applies for the sole purpose of verifying or handling the report, in accordance with legal requirements in force.

The information collected may only be disclosed to third parties if such disclosure is necessary to handle the whistleblowing report.

Information identifying the whistleblower may only be disclosed with the whistleblower's consent. However, information may be disclosed to the judicial authorities if the persons responsible for collecting or handling whistleblowing reports are obliged to report the incidents to the judicial authorities. The whistleblower is then notified, unless there is a risk that such notice could compromise legal proceedings. Written explanations are attached to this notice.

Information identifying the person who is the subject of a whistleblowing report may only be disclosed, with the exception of the judicial authorities, after it has been established that the report is well-founded.

Breach of the aforementioned confidentiality rules may result in disciplinary sanctions or legal action, depending on applicable laws.

## **4.2 Protection of personal data**

Econocom and the legal entity, where the incidents giving rise to the whistleblowing report occurred, in the capacity as joint data controllers, ensure that personal data is processed in accordance with Econocom Personal Data Protection Policy, the joint controllership agreement (DPA) of Econocom Group for the Whistleblowing Platform and the provisions of this procedure.

### **Purpose of processing:**

Data processing in the scope of the whistleblowing system is carried out by Econocom and all of its subsidiaries in the capacity as joint data controllers for the following purposes:

The data collected within the whistleblowing system of Group Econocom is processed for the purpose of receiving and tracking reports, in line with EU Directive 2019/1937 of 23 October 2019 on the protection of whistleblowers and with Legislative Decree no. 24 of 10 March 2023 (Decree').

**The legal basis** for processing data to achieve the purposes set out above is a legal obligation applicable to Econocom Group.

**Recipients of the data:** the recipient of the whistleblowing report and any other person who may be involved in handling the report.

**Duration of storage of personal data:**

Unless otherwise stipulated by law or regulation, personal data is stored and archived for the following periods:

- Data relating to a whistleblowing report is kept in the active database until a final decision is taken on the follow-up action to be taken.
- If no follow-up action is taken further to the whistleblowing report, the personal data is destroyed within two months of the closure of the report.
- In the event of follow-up action, personal data will be kept until the end of the procedure or the time limit for appeals against the decision taken and then archived in accordance with applicable legal provisions.

In countries with more protective provisions, the provisions of local law take precedence over the provisions under this system. In particular, in Italy, it is provided that the whistleblowing report and related documentation shall be retained for no more than (5) five years from the date of communication of the final outcome of the reporting procedure.

**Rights of data subjects:**

In accordance with the General Data Protection Regulation (EU Regulation No. 2016/679 of 27 April 2016 - “**GDPR**”) and Italian Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003), all data subjects have the right to access, correct and amend their personal data. This right may not be exercised to prevent Econocom from fulfilling its legal obligations with regard to the handling of whistleblowing reports and protection of the person filing a report. In particular, the person involved or the person mentioned in the report, with reference to their personal data processed in the context of the report, may not exercise - for the time and to the extent that this constitutes a necessary and proportionate measure - the rights normally granted to data subjects under GDPR.

If a data subject wishes to exercise any of their rights under the GDPR, they may contact the Econocom Group Data Protection Officer (DPO) at [dpo@econocom.com](mailto:dpo@econocom.com) or the local DPO at [dpo@asystel-bdf.it](mailto:dpo@asystel-bdf.it) or [econocom.dpo@avvera.it](mailto:econocom.dpo@avvera.it).

## **5. Measures and sanctions**

Proven breaches identified through an internal investigation will be subject to disciplinary sanctions or legal action depending on the seriousness, on a case-by-case basis.

These sanctions are decided by the Ethics Committee, considering the incidents and circumstances, in conjunction with Econocom Group General Management and the Human Resources Department. Some functions and/or managers may be consulted for this purpose.

Sanctions applicable to Econocom Group employees are decided and implemented in accordance with applicable disciplinary procedures.

In the event of a proven breach, Econocom Group may also decide to take legal action before the competent courts.

Proven misconduct and the corresponding sanctions will be reported to the Group General Management.

In accordance with Article 21 of Italian Legislative Decree 24/2023, the National Anti-Corruption Authority may apply against any individual who has taken reprisal actions; obstructed or attempted to obstruct the report; or who, as the designated responsible person, has violated the confidentiality obligation referred to in Article 12 of the Decree.

## **6.3 Annex 3: Dutch Law specificities added to the “Ethical Whistleblowing system”**

### **2. Glossary**

In the case of the Dutch entities, in addition, Whistleblowing reports can be received by the designated internal officer(s) at the subsidiary.

### **3.2. What incidents are covered by the whistleblowing system?**

Reports must relate to suspected wrongdoing (“vermoeden van een misstand”) as defined under the DWPA.

A suspicion of wrongdoing means the suspicion of a reporter that there is wrongdoing within the organization in which he works or has worked, or at another organization with which he came into contact through his work, insofar as the suspicion is based on reasonable grounds arising from knowledge obtained through his work.

Wrongdoing under the DWPA includes:

- 1) Acts or omissions that are unlawful or defeat the purpose of European Union acts and areas falling within the material scope of Article 2 of the EU Whistleblower Directive; or
- 2) Acts or omissions whereby the public interest is at stake, such as (a) a violation or risk of violation of a statutory provision or internal company rules established under statutory regulation, or (b) a danger to public health, the safety of persons, environmental protection, or the proper functioning of a public service or company.

The public interest is in any case considered to be at stake where the act or omission has a structural character or is serious or extensive.

It must be clear that a whistleblower is “a natural person who, in the context of his or her work-related activities, reports or discloses a suspicion of misconduct.”

A whistleblower is protected against retaliation during and after the handling of a report of suspected misconduct, provided that at the time of reporting, the whistleblower has reasonable grounds to believe that the information reported about the suspected misconduct is correct.

No exceptions are made for persons who receive financial compensation, nor are exceptions made for non-personal suspicions of misconduct outside of professional activities.

### **3.3.1.2. Reporting by post or e-mail**

Whistleblowing reports may be submitted by post or secure e-mail. Reports must clearly state that they are whistleblowing reports.

Reports can be submitted to the following designated internal officer(s).

These designated internal officer(s) are responsible for carefully following up on the reports and providing feedback to the reporting person.

### **3.3.3. External reporting channels**

External reporting channels in the Netherlands include the competent authorities designated under the DWPA, such as the Huis voor Klokkenluiders. Employees may contact these authorities directly if they wish, in addition to using the internal reporting procedure.

## **6.4 Annex 4: German Law specificities added to the “Ethical Whistleblowing system”**

### **3.3.3 External reporting channels**

External reporting channels in Germany include the competent authorities designated under the law, such as the Financial Supervision Authority (BaFin). Employees may contact these authorities directly if they wish, in addition to using the internal reporting procedure.

### **3.4 Who handles whistleblowing reports?**

Under the German Whistleblowing Act (HinSchG), German entities with fewer than

Employees are permitted to delegate the operation of their internal whistleblowing channel to a group-level function or an external provider. In this context, the Group has opted for a centralized whistleblowing system operated at group-level.

However, this delegation does not relieve the individual subsidiary of its legal responsibilities. Each entity remains fully accountable for:

- Assessing and investigating reports relevant to its scope,
- Implementing appropriate corrective actions,
- Providing feedback to the whistleblower within the statutory deadlines (acknowledgment within 7 days, follow-up within 3 months).

These obligations are non-transferable and must be fulfilled by the subsidiary itself, regardless of the centralized operational setup.