Whistleblowing Policy
Collecting and Handling Reports

ATALIAN GLOBAL SERVICES

Type: Group Policy
Category: Compliance
Reviewed by : Audrey Morin, Group Compliance Director
Approved by : Quentin VERCAUTEREN, Group Executive Chairman
Implementation date: 25/03/2026

ATALIAN
GLOBAL SERVICES

1. Introduction

ATALIAN provides an internal system for collecting and handling reports, allowing individuals to report, in complete confidentiality, facts contrary to the law, the Code of Ethics, the Anti-Corruption Code of Conduct or the Group's internal policies, as well as any situation likely to seriously harm the public interest or ATALIAN's legitimate interests.
This policy describes:

- who may submit a report;
- the facts that may be reported;
- the available reporting channels;
- the procedures for assessing, investigating, and closing reports;
- the right to information of the persons concerned;
- the governance applicable to the handling of alerts.

This policy applies to all companies controlled by the ATALIAN Group, subject to any necessary adaptations to comply with applicable local laws.

The system is based on the following principles:

2. Definitions

Concern: any information brought to ATALIAN's attention, in writing or orally, concerning facts potentially contrary to the law, ethics, or internal rules.

Alert : a concern that falls within the scope of the whistleblowing system, meets the validity conditions defined by this policy, and warrants formal handling.

Not valid alert: a concern outside the scope, submitted outside the designated channels without justification, insufficiently substantiated despite a request for additional information, or manifestly abusive.

Whistleblower: a natural person who reports or discloses, without any direct financial compensation and in good faith, information relating to facts covered by the applicable legal protection.

Alert Manager: the person appointed to manage the alert end-to-end, ensure traceability of decisions, coordinate the stakeholders, and ensure compliance with the principles of confidentiality, impartiality, and non-retaliation.

Internal investigation: the set of checks and investigations decided by ATALIAN to assess the accuracy of the reported facts and determine the appropriate follow-up.

3. Receipt of the concern

3.1. Who can report ?

The system is open to any person who has obtained information relating to facts concerning ATALIAN and its activities, including in particular:

- employees, including temporary staff, apprentices/work-study employees and interns;
- job applicants and former employees;
- corporate officers and members of governance bodies;
- customers, subcontractors, suppliers and their employees or representatives;
- any third party in a professional relationship with ATALIAN.

It is not necessary to have been a direct witness to the facts. However, the person making the concern must have elements giving them a reasonable assurance as to the accuracy of the reported facts.

Protection against retaliation extends, under the conditions provided by law, to facilitators, to natural persons connected with the person making the concern, and to the entities they control or for which they work.

3.2. What can be reported

In particular, the following may be reported:

- a crime or an offence;
- a serious and manifest breach of a law or regulation;
- a serious and manifest breach of an international commitment duly ratified or approved;
- a serious threat or harm to the public interest;

To make reporting easier, the professional whistleblowing system allows users to choose from 5 categories (fraud and professional misconduct, HR, QSHE, IT security and other), which are further divided into subcategories (e.g., sexual harassment, discrimination, corruption, etc.).

Individual requests that do not fall within these categories, in particular certain ordinary HR or operational complaints, may be redirected to the appropriate departments.

The following information does not fall within the scope of this system:

- medical confidentiality;
- national defence secrecy;
- a lawyer's professional secrecy.

3.3. How to report

A concern may be submitted to ATALIAN through one of the following channels:

- your line manager, where no conflict of interest exists: if the concern sets out the reported facts and they correspond to one of the topics to be reported under section 2.2, they must relay it to their Compliance Contact or to the Compliance department.
- Human Resources or the Compliance Contact: if the concern sets out the reported facts and they correspond to one of the topics to be reported under section 2.2, they must relay it via the dedicated report management platform.
- the Group Compliance department;
- the dedicated platform accessible at: https://ethicslineatalian.com;
- the dedicated telephone channel by country: https://atalink.atalian.com/alerte-ethique/

Concerns made via the dedicated platform and the telephone channel generate a unique code so that the person making the concern can track progress on the platform.

Anonymous concerns are permitted.

To facilitate handling, the person making the concern is invited, as far as possible, to specify:

- the reported facts;
- the persons or entities concerned;
- the dates, locations and circumstances;
- any documents or elements already available;
- the possible existence of an immediate risk;
- any useful measures to preserve evidence or protect people.

3.4. When can a concern be made

A concern may be made as soon as a person concerned has information and, in good faith, considers that it reveals or makes it possible to suspect facts falling within the scope of this policy.

The system may be used before any harm occurs, in particular in the event of a serious risk, an attempt, an ongoing situation, or a threat to the public interest, people's safety, or ATALIAN's interests.

ATALIAN encourages the use of the internal channel where it allows for effective handling and without risk to the person making the concern. However, using the internal system does not deprive the persons concerned of external channels provided for by the applicable regulations.

4. Assessment and management of the concern

Any concern received under this policy is handled with rigor, impartiality, proportionality and confidentiality.

4.1. Processing timelines

Processing is organised according to the following steps:

These steps are time-bound, with the maximum deadlines defined below:

Step	Maximum timeframe	Comment
Acknowledgement of receipt	7 working days	Does not constitute validity of the concern
Validity	15 working days after acknowledgement of receipt	May include a request for additional information
Closing of the investigation	3 months after acknowledgement of receipt	Without details of the investigation (confidentiality). This may be longer in the event of complexity of the investigation/alert: the whistleblower will be informed within 3 months, with a brief justification.
Case closure	As soon as possible	Written information to the whistleblower

4.2. Validity conditions for a concern as an alert

A concern is valid as an alert when it meets the following cumulative conditions:

1. **Status of the author**: the author acts in good faith and without direct financial compensation;
2. **Nature of the facts**: the reported facts fall within the scope of this policy;
3. **Minimum level of detail**: the report contains sufficiently specific elements to allow an initial analysis;
4. **Absence of legal exclusion** : the report does not relate to information excluded from the system.

If the information provided is insufficient, additional details may be requested from the person making the report, where it is possible to contact them.

A concern may be not valid, in particular, when it is manifestly out of scope, insufficiently substantiated despite a request for clarification, abusive, malicious, or deliberately false.
Where the concern is not valid as an alert, its author is informed, as far as possible, that the file has been closed or redirected to the appropriate department.

4.3. Governance for alert management

Once validity is confirmed, the alert is assigned to a person as **Alert Manager**, responsible for managing it end-to-end. They:

- ensure the principles of the system are applied;
- ensure decisions and actions are traceable, in particular regarding the investigation, and the decisions taken, including disciplinary and remediation measures;
- coordinate internal and/or external contributors;
- immediately withdraw in the event of a real, apparent or potential conflict of interest.

In particular, the Alert Manager ensures that the criticality of the alert is assessed, based in particular on the following criteria:

- potential seriousness of the facts;
- urgency of the situation;
- risk of destruction of evidence or collusion;
- case sensitivity, in particular where a senior executive is involved, where there is media risk, or where there is a conflict of interest.

This assessment determines:

- whether protective measures are appropriate;
- whether an internal investigation is needed and, if so, how it should be conducted to ensure the principles of the system (impartiality, confidentiality, no retaliation, proportionality), including whether to involve an external party;
- the level of follow-up by the competent bodies.
- For sensitive, high or critical cases, the alert must be brought to the attention of the **Whistleblowing Committee** (CAP -Professional Alerts Monitoring Committee), which decides in particular the resources, protective measures, possible outsourcing of the investigation, and the main processing orientations.

4.4. Internal investigation

When it is decided, the internal investigation aims, while respecting individuals' rights, to determine whether the reported facts are confirmed.

The investigation may include, in particular:

- interviews;
- a documentary review, including email mailboxes and correspondence;
- collection of relevant information and data;
- accounting or operational checks;
- involvement of internal or external specialists.

The investigator, who may be different from the Alert Manager, conducts the investigation in accordance with their mandate, in compliance with the principles of the system and with personal data protection requirements.

Persons interviewed as part of the investigation are informed, as required by the needs of the investigation, of the reasons for their involvement and the rules applicable to the process. This information may be deferred where immediate information would create a risk of destruction of evidence, pressure on witnesses, or compromise of the checks.

ATALIAN may, where necessary, implement proportionate protective measures or precautionary measures, in particular to prevent a risk of retaliation, preserve evidence, protect individuals, or secure operations.

4.5. Closing the investigation and individual and collective actions

At the end of the investigation, several outcomes are possible:

- Founded misconduct;
- Unfounded misconduct;
- Findings not conclusive.

Where the facts are confirmed, ATALIAN may implement any appropriate measure, in particular:

- disciplinary measures, in compliance with applicable law;
- organizational corrective actions;
- remediation actions;
- strengthening of controls and/or launching an audit;
- training or awareness actions;

- coaching measures and development plans;
- reporting to the competent authorities, including filing a criminal complaint.

ATALIAN prohibits any form of retaliation against a person who has made a report in good faith or who has contributed to its handling under the conditions provided by law.

If, during the investigation, it is demonstrated that the alert was made in bad faith (intent to harm or knowledge that the facts were materially inaccurate), its author may be subject to disciplinary measures and, where applicable, legal action.

4.6. Data retention

The retention periods for data relating to the report are specified in Article 13 of the appendix on personal data protection.

4.7. Preventing conflicts of interest

Any person involved in receiving, assessing, managing, investigating, deciding on, or following up on a report must act with impartiality, independence, and objectivity.
No person may take part in handling a report when they:

- are named in the report;
- have a direct reporting line with the person named or with the author of the report, such as to compromise their impartiality;
- have a personal, financial, professional or relational interest in the case;
- have already taken a position on the facts under conditions incompatible with a neutral review;
- are, more broadly, in a situation of real, apparent or potential conflict of interest.

Any person who identifies such a situation must inform the Group Compliance department without delay and immediately withdraw from handling the case.

When a concern implies:

- a member of the Executive Committee (COMEX), France CODIR and International CODIR;
- a member of the Compliance, Legal, Human Resources function, or any other function likely to be involved in the case;
- or presents a high level of sensitivity, seriousness, or reputational risk,

the case is subject to **enhanced escalation** and may be entrusted, in whole or in part, to an external party providing the required guarantees of independence and confidentiality.

1. Right to information

To ensure compliant, transparent and balanced processing, ATALIAN recognizes information rights tailored to the different categories of persons concerned.

4.8. Author of the report

The author of the report is informed, as far as possible:

- that the report has been received;
- that the case is admissible or not;
- no later than 3 months after the acknowledgment of receipt;
- of the closure of the case, when possible.

For reasons of confidentiality, personal data protection and respect for the rights of the persons concerned, ATALIAN does not communicate the processing details, the evidence collected, or the full detail of the conclusions.

5.2 Persons named and other persons concerned

Persons whose data are processed as part of a report are informed of such processing as soon as possible, unless such information is likely to compromise the checks or lead to the destruction of evidence. In that case, the information is deferred until the risk has disappeared.

ATALIAN ensures that the presumption of innocence is respected, that the reputation of those involved is protected, and that the principle of confidentiality is strictly observed.

Subject to the legal limitations applicable in an investigation context, these persons have the rights provided for by personal data protection regulations, as specified in Article 14 of Appendix 1.

5.3 Management and other parties involved

Management is informed only of the elements strictly necessary to implement precautionary, disciplinary, corrective or organisational measures, and only when it is not concerned by the report. It may be involved only where an operational need is identified by the Case Supervisor or the Whistleblowing Committee (CAP).

Any information provided as part of a report is strictly limited to those authorized to access it for the purposes of processing the case. Any unauthorized disclosure subjects the person who disclosed the information to appropriate sanctions.

Management is involved only when operationally necessary and strictly on a “need-to-know” basis. A person who is the subject of a report may not be involved in its assessment, handling, or in decision-making following the conclusion of the investigation.

1. Controls and audit

Monitoring compliance with this policy is incorporated into the internal control plan. An internal or external audit may also be conducted to ensure the effectiveness of the system.

1. Sanctions

Any intentional breach of the policy may result in disciplinary measures, in accordance with the applicable rules.