



Ethic & Compliance Alert Process

CONTENTS

Our commitment.....	3
General rules.....	4
Purpose of the procedure	4
Objectives of the system	4
A good-faith approach	4
Right to raise an internal alert	5
Right to raise an external alert	5
Public alerts	5
No retaliation.....	5
Issuing & handling alerts	6
Ethic and compliance committee	6
Reportable incidents	7
Issuer identification.....	7
Identification data of the targeted persons	8
Verification and treatment of the alert.....	8
Result of the alert processing	9
Retention of personal data.....	9
Authorisation, access and rectification rights	9
Transfers of personal data outside the European Union	9

Our commitment

Scalian is committed to full compliance with regulations and ethical standards in the conduct of its business, as set out in its Ethics and Compliance programme and Codes of Ethics.

Ethics is the responsibility of each member of the Scalian. It is reflected in the relations of employees with each other and with third parties (in particular: public and private customers, business partners, suppliers, service providers, shareholders).



In case of doubt or worry about the application of the law or ethical standards, employees can use several channels: their hierarchy, the "Ethics and Compliance" committee. The Group's Ethics Officer can also be consulted for advice and guidance. In addition to the traditional channels of communication, and in accordance with the new legal provisions, the Scalian Group has set up a professional alert system.

General rules

Purpose of the procedure

The purpose of this Process is to determine the modalities for collecting reports of an alert issued by a member of the Scalian group. A member of the Scalian group is defined as any person acting in the name and on behalf of Scalian in his or her capacity as an employee (salaried, temporary, trainee), partner and/or external service provider, as well as any associate, agent and member of the supervisory committee.

Objectives of the system

The purpose of the system for collecting professional alerts is to support the Scalian Group's ethical approach and to complete the employees' expression means, so that everyone can be a player in ethics and the prevention of related risks.

The present system for collecting professional alerts is a complementary system that is not intended to replace the traditional channels of internal communication, according to the rules applicable in each country, such as the hierarchical channel and the employee representation bodies.

Its use is optional. No sanction may be taken against an employee for not using this warning system.

Since the purpose of the whistleblowing system is to enable honest, reliable and responsible communication, Scalian Group guarantees the

confidentiality of the data processed and prohibits any form of retaliation or threat of retaliation against employees who use it.

A good-faith approach

The choice to whistle blow is an individual responsibility. Employees using the whistleblowing system must act in good faith and not deliberately make false accusations or have the sole intention of causing harm or gaining personal advantage.

Good faith is understood to mean that a report is made without malice or the expectation of personal gain. Good faith thus implies that the employee can establish or produce objective data, directly related to the scope of the whistleblowing system and strictly necessary to verify the alleged facts, through formulations that show the presumed nature of the reported facts.

Any employee who knowingly, or in a grossly negligent manner, makes false statements, discloses misleading information, or acts in bad faith or in an abusive manner may be subject to disciplinary action or prosecution in accordance with applicable laws and regulations.

On the contrary, an employee acting in good faith will not be subject to any disciplinary action or prosecution if the alleged facts turn out to be inaccurate or do not lead to any consequences.

Right to raise an internal alert

Everybody shall send a report to Scalian if they suspect that a Scalian employee or any person involved in the activities carried out by or for Scalian has failed to comply with our Code of Ethics, our Supplier Code of Ethics or the laws, rules and regulations in force.

The report must be made through one of the following channels:

- ✕ By using the secure website <https://scalian.integrityline.app>
- ✕ By contacting by email our Ethics and Compliance committee at : ethic.compliance@scalian.com

Right to raise an external alert

Without having to report internally, the whistle-blower either can also, after having made an internal alert or directly, send an external alert to:

- ✕ The competent local or French authority for the group's headquarter;
- ✕ The local or group's headquarter rights defender, if any, who will direct him/her to the authority or authorities best placed to deal with it;
- ✕ The local or French judicial authority;
- ✕ An institution, body or agency of the European Union competent to collect information on violations falling within the scope of the Directive of 23 October 2019.

Public alerts

An alert can be made public immediately in the following cases:

- ✕ In case of serious and immediate danger ;
- ✕ In the case of information obtained within the professional context, in cases of imminent or manifest danger to the public interest, in particular where there is an emergency situation or a risk of irreversible harm;
- ✕ Where referral to the competent authority would expose the whistle-blower to a risk of retaliation or would not allow the whistle-blower to be effectively dealt with because of particular circumstances (suspected conflict of interest, risk of concealment or destruction of evidence, collusion, etc.).

However, there is a notable exception in some local laws: a threat cannot be immediately made public if it affects the interests of defence and national security.

No retaliation

No action or threat of reprisal, direct or indirect, against an employee who has issued a warning in good faith or provided assistance to those in charge of handling a warning, will be accepted.

Nor should any employee be subjected to harassment, or suffer adverse employment consequences, for raising an alert in good faith.

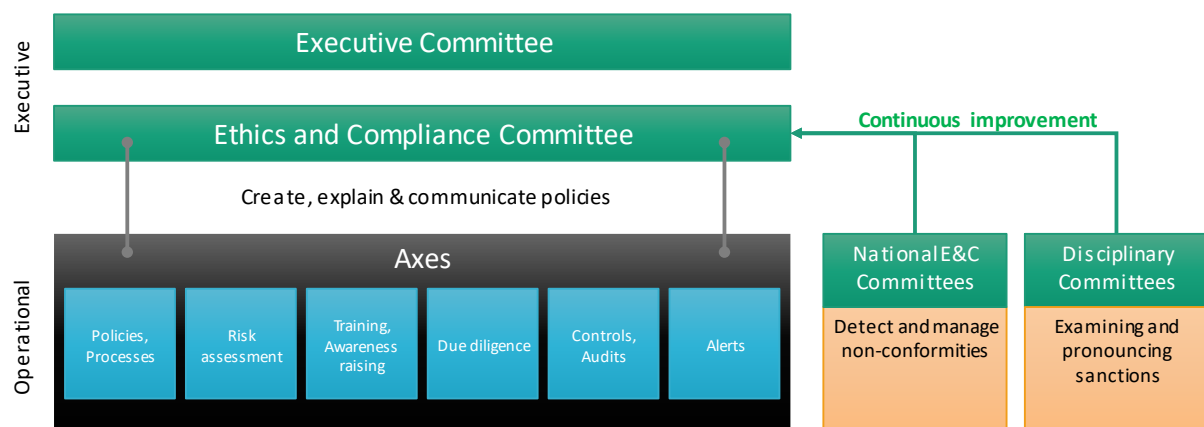
Also protected are facilitators (associations; trade unions), individuals connected with the whistle-blower (colleagues, relatives) and legal entities controlled by the whistle-blower, in accordance with the local regulations applicable.

Issuing & handling alerts

Ethic and compliance committee

By decision of the President of Scalian SASU, the head company of the Scalian Group, the referent of the Scalian Group is the Ethics and Compliance Committee with the following members

- ✕ Yvan Chabanne as Chairman of the Scalian Group
- ✕ Jean- Manuel Silva (General Secretary) as Chairman of the Ethics and Compliance Committee,
- ✕ Pascal Gavaud (Quality Director) as Group Ethics Officer
- ✕ Camille Stonehouse (Head of Legal Affairs)



For the Indizen & Tagueri subsidiaries, the compliance programme is supported by local ethics and compliance committees. Their objective is to ensure the full implementation of the compliance programme according to local regulations and risks.

Reportable incidents

According to the legal regulations, the system for collecting alerts can be used by any individual who reports, in a disinterested manner and in good faith, a fact of which he or she has personal knowledge and which he or she considers to be:

- ✖ A crime or an offence,
- ✖ A serious and manifest violation of an international commitment duly ratified or approved by a country where the Scalian Group operates,
- ✖ A serious and manifest violation of the law or regulation,
- ✖ Or a serious threat or prejudice to the general interest.

These findings may also relate to the possibility of behaviour or situations contrary to the Scalian Group's "Ethics and Compliance" policy and the Codes of Ethics.

However, the alert may not relate to matters covered by national defence secrecy, medical secrecy or lawyer-client privilege.

Only data strictly limited to the areas covered by an alert may be processed (please refer to the Scalian Group's personal data register).

Any data not falling within the scope of the system will not be processed under this process and will be destroyed or retained under the conditions set out below.

An employee who decides to use the whistleblowing process to make a professional alert may contact the Ethics and Compliance Committee in accordance with the Scalian Group Code of Ethics¹.

The employee using the whistleblowing procedure set up within the framework of the present process will benefit from the legal

protection attached to the status of "whistle-blower".

Issuer identification

The issuer of a professional alert:

- ✖ Can remain anonymous if local law allows it, in which case only the alert platform should be used. The platform guarantees the anonymity of the issuer and allows communication between the issuer and the Ethics and Compliance Committee
- ✖ Can identify itself, in exchange he or she benefit from a confidential treatment of their identity and personal data, in compliance with the applicable legislation.

Employees who use this system can be confident that every precaution will be taken to ensure that their identity and personal data will be kept strictly confidential, including by those involved in the verification or processing of alerts.

Precautions will be taken by the Ethics and Compliance Committee to ensure that only the data necessary for the accomplishment of their respective missions of verification or treatment of a professional alert are transmitted to third parties involved in the procedure of verification or treatment of a professional alert (personnel within the Group entity concerned or external service provider).

In addition, the Ethics and Compliance Committee will take all appropriate precautions to preserve the security of the data, in particular by restricting access to the data by means of individual identifiers and passwords that are regularly renewed.

With the exception of the judicial authority, information identifying the sender of the alert

¹ Any Scalian employee is free to also use the whistleblowing procedures of all stakeholders (shareholders, insurers, banks, customers, suppliers, institutions, employee representatives,

etc.) without informing Scalian. The procedure of the interested party will be applied to the employee.

may only be disclosed with the consent of the person.

Alerts made anonymously will not be processed unless the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed, and only after prior examination by the first addressee in order to decide on the appropriateness of processing them in the framework of the present process.

Identification data of the targeted persons

The person concerned by an alert is informed by the Ethics and Compliance Committee, as soon as the alert is registered, of the data concerning him or her in order to enable him or her to object to the processing of the said data. However, when protective measures are necessary, in particular to prevent the destruction of evidence relating to the alert, the person concerned is only informed once these measures have been adopted.

The information, which shall be in writing and sent by e-mail or post, shall specify the entity responsible for the system, the facts complained of, the departments to which the alert is addressed and the procedures for exercising rights of access and rectification. The information shall be accompanied by a copy of this procedure.

Information that could identify the person who is the subject of an alert may only be disclosed, except to the judicial authority, once it has been established that the alert is well founded.

Verification and treatment of the alert

As soon as the Ethics and Compliance Committee receives a professional alert, either through this alert procedure or via traditional communication

channels, the sender of the alert shall be informed in writing and without delay of the receipt of the alert issued, as well as of the reasonable and foreseeable period of time required to examine its admissibility and of the terms and conditions according to which he/she will be informed of the follow-up given to his/her alert.

In a first phase called verification, the Ethics and Compliance Committee makes a preliminary assessment of whether the alert falls within the scope of this process.

Any report which is clearly outside the scope of the process, which is not serious, which is made in bad faith, or which constitutes an abusive or even defamatory denunciation, as well as any report concerning unverifiable facts, will be destroyed without delay; the author will then be informed within the time limit set by the Ethics and Compliance Committee at the time of receipt of the professional alert. Where appropriate, the Ethics and Compliance Committee shall inform the person who has been targeted that he or she was the subject of an alert.

In the event that, after a preliminary assessment, the Ethics and Compliance Committee concludes that the alert is admissible, it shall inform the author within the time limit initially indicated.

The Ethics and Compliance Committee will take all useful actions to deal with the professional alert, in particular by launching an investigation if necessary. This investigation may be carried out either by a small internal team of Scalian Group employees bound by an obligation of reinforced confidentiality, or, if the facts justify it, by third parties specialised in conducting investigations or in certain fields useful to the investigation (for example, IT, legal, financial and accounting fields).

In this case, these third parties shall contractually undertake not to use the data for improper purposes, to ensure their confidentiality, to respect the limited period of retention of the data, and to proceed to the destruction or return of all manual or computerised personal data carriers at the end of their service.

The sender of the whistle-blower will only be involved in the investigation process for the verification of the facts he/she has reported. The progress of the investigation, its content, its outcome and the resulting report are strictly confidential, including with regard to the sender of the alert.

Result of the alert processing

At the end of the alert processing operations, the Ethics and Compliance Committee will draw up a confidential report.

The Ethics and Compliance Committee will organise an oral presentation of the conclusions of the investigation to the issuer of the alert in order to confirm the validity or otherwise of the facts reported, while respecting an obligation of confidentiality with regard to the other persons mentioned in the report.

If corrective action is required, the Ethics and Compliance Committee will approach the appropriate line management to recommend treatment. Any disciplinary or legal action will be taken in accordance with the applicable legal provisions.

The management line concerned shall notify the Ethics and Compliance Committee of the measures taken.

Retention of personal data

Data relating to an alert considered by the Ethics and Compliance Committee as being outside the scope of the system will either be destroyed or archived (after anonymization) without delay.

Where the alert is not followed by disciplinary or judicial proceedings, the data relating to the alert shall be destroyed or archived, after

anonymization, within two months of the closure of the verification operations.

Where disciplinary proceedings or legal proceedings are initiated against the respondent or perpetrator of an unlawful alert, the data relating to the alert shall be kept until the end of the proceedings.

Data subject to archiving measures are kept in a separate information system with restricted access for a period not exceeding the time limits of legal proceedings. Refer to the asset management procedure of the Scalian Group's Global Management System.

Authorisation, access and rectification rights

Any individual identified in the whistleblowing system has the right to access data concerning him or her and to request to be corrected or deleted if they are inaccurate, incomplete, ambiguous or out of date.

The person who is the subject of an alert may under no circumstances obtain, on the basis of his or her right of access, information concerning the identity of the sender of the alert.

Transfers of personal data outside the European Union

In the event of a transfer of data to a legal entity established in a country outside the European Union, such communications will be made in accordance with the specific provisions of the law of the country where the alert relating to international data transfers takes place. In the absence of local law, French law will apply.

These provisions are met where the legal person in which the data recipient works has joined the Privacy Shield, insofar as the company concerned has expressly chosen to include human resources

data within the scope of that membership. These provisions are also met when the recipient has concluded a transfer contract based on the standard contractual clauses issued by the European Commission in its decisions of 15 June 2001 and 27 December 2004, or when the group to which the entities concerned belong has adopted internal rules which guarantee an adequate level of protection of the privacy and fundamental rights of individuals.