



WHISTLEBLOWER'S CHARTER

What is the purpose of the whistleblowing hotline?

Elior Group has set up an outsourced whistleblower hotline managed by an external and independent service provider (currently iSope Solution) that allows its employees to report a concern confidentially.

When they fall within the scope defined in this Charter, reports are sent to the Compliance Department, which is responsible for processing them.

The Group, eager to promote a culture of dialogue, encourages all of its employees to read this Charter and to use the whistleblowing hotline to voice their concerns if they come across unethical and/or illegal behavior.

Can I report a concern?

The following persons can use the whistleblowing hotline to raise a concern:

- Employees (employees, shareholders, managers and executives) including external and occasional workers (temporary workers, apprentices, trainees) (hereinafter collectively referred to as “employees”);
- Persons whose employment relationship with the Elior Group has ended, provided that the information was obtained within the framework of this relationship;
- Persons who have applied for a job within Elior Group, provided that the information was obtained in the context of this application;
- The co-contractors of the Group as well as their subcontractors.

What can I report ?

It is possible to report via the whistleblowing hotline information obtained directly or indirectly (in the professional context) relating to:

- Breach of competition rules (for example: sharing any confidential information with competitors or agreeing on prices with competitors)
- Corruption (for example: offering/receiving sums of money or gifts in exchange of obtaining/granting a contract)
- Influence peddling (for example: paying a third party to use his/her influence with a public authority or administration to obtain an undue advantage)
- Conflict of interest (for example: selecting as a supplier a company in which one of the family members of the decision maker works)
- Money laundering
- Financing of terrorism
- Fraud
- Non-compliance with the rules set out in the Group's Integrity Guide or the Ethics Charter
- Psychological and/or sexual harassment
- Violations of the environment or of human rights and fundamental freedoms.



Is it possible to report inappropriate behavior (repeated jokes with a sexual connotation) on behalf of a colleague who does not feel comfortable talking about it?

Repeated jokes with a sexual connotation can be considered as sexual harassment. As such, this type of behavior can be reported through the whistleblowing hotline.

An employee may file a complaint regarding facts that have been reported to him or her in a **professional context**, even if he or she is not directly affected, as long as the interests in question are legitimate (in particular, if they fall within the scope of this Charter).

How can I file a report?

A report can be filed via the whistleblowing hotline set up for this purpose and whose management has been entrusted to an external third party (currently iSope Solutions), which offers all the guarantees in terms of integrity and confidentiality. The hotline makes it possible to transmit any information, regardless of its form or medium, likely to support the facts reported.

Reporting can be done:

By email : alert.eliorgroup@isope.solutions

By mail:

iSope solutions (Alerte Elior)
90/92 Route de la Reine
92100 Boulogne-Billancourt – France

By phone (European Union and United Kingdom),

Monday to Friday from 9am until 18pm (CET) at the following number: **00 800 180 620 19**

An operator will answer in your chosen language.



The whistleblower can request a videoconference or a physical meeting (organized by the Compliance Department no later than twenty working days after receiving the said request).



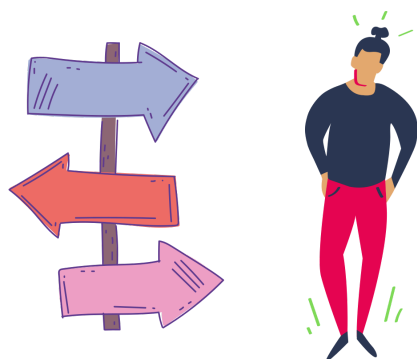
Friendly reminder

Anonymous reports will be examined under the same conditions as other reports, except that it will not always be materially possible to keep the whistleblower informed of the action taken following his/her report.

The report will only be taken into account after an initial examination to ensure that the information provided is sufficiently consistent and substantiated.

Furthermore, it should be noted that the absence of dialogue may make the investigation that will be carried out less effective.

Regardless of the method chosen (anonymous or not), the report, that will be filled in an electronic safe of the external service provider, will be timestamped.



Do I have to go through the whistleblowing hotline to make a report?

No. The purpose of the whistleblowing hotline is not to replace other whistleblowing channels but to provide employees with an additional reporting tool that offers enhanced confidentiality. Nevertheless, the employee is free to choose amongst the different channels in place.

Thus, a report can be made directly to a trusted member of the Personnel: a manager, a member of the Compliance network (contact details for the Compliance network can be found on the website <https://integrity.eliorgroup.net/>), the Legal Department, the Human Resources Department, or a staff representative.

It is also possible to report directly to one of the external authorities listed in the appendix to decree no. 2022-1284 of October 3rd 2022 relating to the procedures for collecting and processing reports by whistleblowers, if the whistleblower does not feel comfortable with the reporting channels made available internally.

What follow-up will be given to my report?

An acknowledgment of receipt (specifying the date and time of the report), accompanied by a summary of the attachments communicated, will be sent to the whistleblower by the service provider within 7 working days following the report. The service provider will check that the facts reported fall within the scope of the Charter and that they are sufficiently consistent to be subject to in-depth checks.

If the external service provider finds that the facts reported are not admissible, the whistleblower will be informed of the reasons why his or her report does not comply with the required conditions and that, consequently, no action will be taken. The whistleblower will then be directed to alternate internal avenues allowing him or her to address his or her grievances/concerns.

A monthly report will detail all the alerts that were not admissible in an anonymized form and will be sent to the Group Compliance Officer.

Nevertheless, if the report falls within the scope of the Charter and is sufficiently substantiated, the report will be forwarded to the Compliance Department for an in-depth analysis.

No later than three months from the report's acknowledgment of receipt, the whistleblower will be informed by the Compliance Department of the follow-up to be given to the report:

- Either the closing of the investigation when the allegations are inaccurate or unfounded or when the report holds no longer merit;
- Or additional measures are being considered or taken to assess more precisely the accuracy of the allegations and, if necessary, remedy the subject of the report.

How am I protected in the event of a report?

In accordance with the law and with the Group's Integrity Guide and the Ethics Charter, there will be no retaliation against whistleblowers.

The whistleblower is protected against any adverse actions following a report, provided that the said report has been made in good faith and that the whistleblower has reasonable grounds to believe the said report was necessary to safeguard the interests in question (the safety and health of employees and guests, protection of the Elixir Group's reputation in terms of probity, etc.).

Thus, the Group prohibits all measures of retaliation, threats or attempts to resort to these measures, in particular in the following forms:

- Suspension, layoff, dismissal or equivalent measures;
- Demotion or denial of promotion;
- Reassigning to a less desirable position, change of place of work, reducing or changing pay or hours;
- Suspension of training;
- Negative performance evaluation or work certificate;

- Imposed or administered disciplinary measures, reprimand or other sanctions, including financial sanction;
- Coercion, intimidation, harassment or ostracizing;
- Discrimination, disadvantageous or unfair treatment;
- Failing to hire;
- Failure to rehire or early termination of a fixed-term employment contract or a temporary contract;
- Harm, including damage to reputation, in particular on an online communication service, or financial loss, including loss of business and loss of income;
- Blacklisting (sector or industry level);
- Early termination or cancellation of a contract for goods or services;
- Cancellation of a license or permit;
- Improper referral to psychiatric or medical treatment.

Important: facilitators (third parties who aid the whistleblower to make a report, such as unions or NGOs) and the **relatives** and **colleagues** of the whistleblower are also protected under this Charter and are entitled to the same level of protection as the whistleblower.



As part of a call for tenders organized by the Group, the company belonging to the brother of your manager wins the contract even though its offer was less advantageous than those of other competitors. You hesitate to report this situation because you are afraid of suffering retaliation. You also fear being penalized if your report turns out to be unfounded or inaccurate.

Any form of retaliation against a whistleblower will not be tolerated within the Group. Moreover, filing a report that is later proven to be inaccurate or unfounded does not warrant disciplinary action, provided the whistleblower was in good faith.

Nevertheless, any report made in bad faith with the intention to harm individuals or the Group or whose content was known to be false at the time of the report can be subjected to disciplinary or even criminal action.

How is my confidentiality protected?

The Group guarantees confidential treatment of all information collected through the whistleblowing hotline, which only records the personal data received from the whistleblower or necessary to process the alert, which is generally as follows:

- The identity, contact details and job title of the whistleblower(s),
- The identity, job title and contact details of the person (s) who aided the whistleblower, if applicable,

- The identity, job title and contact details of the person(s) implicated in the alert,
- The identity, title and contact details of the person(s) questioned during the investigations, when necessary,
- The identity, job title and contact details of the person(s) involved in collecting or processing the alert, when necessary,
- The allegations reported,
- The information gathered as part of the verification of the facts reported,
- The report on the measures taken to investigate and remedy the alert.

Data collected within the European Economic Area will not be transferred to a country outside the European Economic Area unless there is an adequacy decision in place.

The identity of the whistleblower is disclosed within the company, if necessary, only to those who need to know it for the purposes of verifying or processing the alert and its consequences. and only after they have signed a specific confidentiality agreement. Under no circumstances the identity of the whistleblowers is disclosed to the person(s) implicated in the alert.

Save as set out above, any information which is liable to reveal the whistleblower's identity will not be disclosed without his or her consent, except to the judicial authorities, or to satisfy a legal requirement, once the validity of the alert has been established.

In the same way, the elements likely to identify the person implicated by a report cannot be disclosed, except to the judicial authority or to satisfy a legal requirement, once the validity of the alert has been established.

How are my data stored and what are my right of access / to rectification?

The data collected is encrypted and stored in an electronic safe hosted by the external service provider. Access to the electronic safe is restricted to the Compliance Department, in their capacity as sole recipient. Only they possess an individual username and password.

If the whistleblower has made a report directly to a manager or a member of the HR department (or another employee authorized to process an alert), the person having collected the alert is responsible to answering any inquiry relating to the methods of data storage and more generally, to data collection.

The data collected will be retained only for the time required to process the case under investigation and will be destroyed as soon as their conservation no longer appears necessary from a legal point of view (for example, for the duration of a contentious procedure). When possible, the data collected will be stored anonymously. (i.e. by neutralizing the personal data within the retained data).

Furthermore, and in accordance with the General Data Protection Regulations ("GDPR"), every person identified in the whistleblower hotline can access the data concerning him/her and request, if necessary, their rectification or erasure.

They can also object to the processing of which they are subjected but only within the limits of Article 21 of the GDPR (i.e. legitimate and compelling reasons may prevail over the interests and rights and freedoms of the data subject).

Nevertheless, the implicated party may not receive (given limitations on the right of access) information concerning third parties and in particular the identity of the whistleblower.

For any information on the rights related to the protection of personal data, the whistleblower or any person concerned may **contact: gdpr-contact@eliorgroup.com**.

How is the person implicated by the alert informed?

In accordance with the GDPR, the Compliance Department informs the person implicated by an alert within a reasonable period of time, which should not exceed one month in principle. He indicates to him or she the allegations made, as well as of the procedures for exercising his or her right of access and to rectification.

However, the information of the person in question may only intervene after the adoption of precautionary measures when these prove to be essential, in particular to prevent the destruction of evidence necessary for the processing of the alert.

Furthermore, the information of the person in question does not contain elements relating to the identity of the whistleblower or of third parties. It should be noted that the Group applies the principle of proportionality when enforcing any sanctions.