

Ethics alert system

VADEMECUM

SUMMARY

| | |
|--|----------|
| Preamble | 2 |
| What is the purpose of the ethics alert system? | 2 |
| General principles | 3 |
| Who can report an incident? | 3 |
| What type of incidents can be reported? | 3 |
| How should the reporting be done? | 4 |
| How to benefit from the whistleblower status? | 4 |
| Maât ethics alert line | 5 |
| How does the Maât ethics alert line work? | 5 |
| Can a potential breach be reported anonymously? | 5 |
| Processing of an alert | 6 |
| Once an alert is filed on Maât, who receives and processes it? | 6 |
| How is the investigation conducted ? | 7 |
| How is confidentiality, and the case being, anonymity, guaranteed? | 7 |
| How long does it take to process an alert? | 7 |
| How is the collected personal data protected? | 8 |
| Consequences of reporting | 9 |
| Can retaliation measures be taken against the whistleblower? | 9 |

Preamble

What is the purpose of the ethics alert system?

The Soitec group is committed to respect a set of **values** and **fundamental principles**, defined in its **Code of conduct**, as well as in the group general management policies, particularly in terms of human rights and preservation of the integrity of persons, of the environment, of health, the safety of people and property, and is committed to conducting its business in an ethical manner with regard to the prevention of corruption¹ and insider trading, export control compliance, competition law and personal data management.

In order to ensure compliance with these commitments and rules, the Soitec group has set up an **ethics alert system** allowing any stakeholder to **report any breach** of which he/she may be a victim, witness or have knowledge.

Reporting can be done either through the hierarchy (to a direct or indirect manager), through human resources or social partners, or *via* the **Maât ethics alert line** (which is further described below).

Regardless of the reporting channel used, the author of the report will be assured of the **preservation of the confidentiality of the processing of his/her alert** and, if he/she has chosen not to reveal his/her identity (for example by using the Maât ethics alert line, or by reporting by anonymous letter), the **preservation of his/her anonymity**.

This ethics alert system reflects Soitec group's desire to enable all its stakeholders to **speak out in good faith, freely and without fear of reprisal**, to identify any violation as soon as possible, and if these violation are proven, to provide the appropriate responses as soon as possible.

The **success of this whistleblowing system** is based on its appropriation by all the stakeholders, and on their **confidence** in the way their reports are handled. To this end, the Soitec group undertakes to provide its best efforts to process as soon as possible, and according to the principles and procedures described below, all reports made in **good faith**.

¹ In particular, with the French law relating to transparency, the fight against corruption and the modernization of economic life ([law n°2016-1691 of December 9, 2016, known as the "Sapin 2" law](#)), which specifies the legal regime applicable to reports and the protection of whistleblowers.

General principles

Who can report an incident?

All Soitec group stakeholders may report a potential breach, and in particular (without this list being exhaustive):

- employees of the Soitec group as well as temporary staff, interns, etc. ;
- former employees of the Soitec group, when the information was obtained in the context of their relationship with the Soitec group;
- people who have applied for a job within the Soitec group, when the information was obtained in the context of this application;
- shareholders of Soitec SA or companies of the Soitec group;
- the members of the board of directors of Soitec SA or companies of the Soitec group;
- the economic and institutional partners of the Soitec group (customers, suppliers, service providers, subcontractors, R&D partners, research laboratories, financial institutions, etc.) and their staff.

The ethics alert system applies to **all Soitec group companies**, regardless of their geographic location.

Where applicable, local law provisions that are more stringent or contradictory with this document shall apply.

What type of incidents can be reported?

The scope of suspected breaches likely to be reported includes in particular (without this list being exhaustive):

- Any suspected violation of the **Code of conduct** : violation of human rights, discrimination, sexual or moral harassment, safety rules, environmental rules, theft, money laundering, corruption, conflict of interest, insider trading, anti-competitive behavior, personal data breach, export control violation, etc.
- Any suspicion of violation of **internal procedures**, and in particular [group general management policies](#).
- Any other suspicion of violation that the **applicable law and regulations** define as reportable².

² For France, see in particular all the subjects defined by the "[Law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of economic life](#)", and the [implementing decree no. 2022-1284 of October 3, 2022](#) including information relating to a crime, misdemeanor, threat or harm to the public interest, violation or attempted concealment of a violation of an international agreement, violation of any regulation insofar as it involves or impacts Soitec.

On the other hand, facts, information or documents, whatever their form or medium, covered by national defense secrecy, medical secrecy or the confidentiality of relations between lawyers and their clients, cannot be subject to a report.

How should the reporting be done?

In order to encourage people who suffer or witness breaches to report them, the Soitec group offers numerous reporting channels. A breach can be reported:

- **Internally:**
 - To a direct or indirect manager;
 - To the human resources department;
 - To employees' representatives;
 - To the legal department;
 - To the competent department with regard to the suspected breach;
 - Through the Maât ethics alert line, which is further described below.
- **Externally**, with the competent authorities, if the whistleblower believes that he/she is exposed to a risk of reprisals in the event of an internal report or if his/her alert has not been dealt with within the applicable deadlines (detailed below)³.

How to benefit from the whistleblower status?

In order to benefit from the protective status of whistleblower:

- The report must be made **in good faith**;
- The whistleblower must **not receive direct financial compensation** for reporting;
- The whistleblower may file a report relating to facts of which he/she was not personally aware, but which were reported to him/her by another person, provided that this information was obtained in the context of professional activities.

³ In France, these authorities are those listed in the Appendix of the implementing decree no. 2022-1284 of October 3, 2022.

Maât ethics alert line

How does the Maât ethics alert line work?

The Maât ethics alert line, provided by a third-party, offers the following guarantees and features to the author of a report:

- Sound preservation of his/her **anonymity**, if he/she has chosen not to reveal his/her identity;
- Preservation of **confidentiality of his/her report**;
- Preservation of **data security** exchanged *via* Maât, it being specified that the provider of the Maât ethics alert line acts as a mere technical intermediary between the author of the report and the Soitec group, and does not have access to any information relating to the reports;
- **Removal of metadata** attached to the documents transmitted;
- **Ease of use** for the author of a report as well as for the case managers.

Can a potential breach be reported anonymously?

Yes.

Reporting a violation of the law or the commitments and internal procedures of the Soitec group sometimes asks for **courage**. This is why the Soitec group allows the whistleblower to file an **anonymous** report.

For example, if the report is filed through the Maât ethics alert line, the **Soitec group will not have access to any information**, including technical (IP address, metadata, etc.) likely to reveal the identity of the author of the report, other than information relating to the content of the report itself. Similarly, if the report is filed *via* an anonymous letter in which the author does not wish to reveal his/her identity, the Soitec group undertakes not to seek to establish his/her identity.

At any time during the reporting procedure, the author of a report has the **possibility of lifting his/her anonymity if he/she wishes**, in particular in order to facilitate exchanges, if he/she considers that this can facilitate the internal investigation.

Processing of an alert

Once an alert is filed on Maât, who receives and processes it?

First, the recipients of the report made through the Maât ethics alert line ensure that it fulfills the **conditions of eligibility** described above, and may, for this purpose, request any additional information from the whistleblower.

In the event that the recipients of the report consider that the report does not meet the eligibility conditions, they inform the whistleblower, specifying the ground for refusal.

The choice of the recipients of the report meets the **principles of necessity** (so that only people who strictly need to know have access to the content of a report) and **collegiality** (in order to avoid arbitrary decisions). Recipients of reports made *via* the Maât ethics alert line are:

- The EVP People and Sustainability;
- The EVP Secretary General.

By exception, when the author of the report considers that one of the recipients of the report is likely to be in a **conflict of interest situation**, the latter may request that the person not be aware of the report and withdraw from the related investigation. When reporting it, the author of the report can also indicate whether he/she wishes other people to be excluded from the conduct of the internal investigation (for example if he/she thinks that the person in question is likely to intervene in the context of internal investigation).

Second, the recipients of the report allocate responsibility for the investigation and/or involve all persons who, given the nature of the report, will have the competence and independence required to process it:

- **either internally:** for example concerning a problem relating to the quality of the products, the VP Quality and/or the director of the site and/or the VP Operations;
- **either externally:** a law firm for example, in order to ensure the privileged nature of information, on a subject for which technical expertise is necessary or even if they believe that their independence could be questioned and consider that they are not able to assess the facts submitted to them with complete peace of mind. If applicable, this third party undertakes beforehand to strictly comply with the processing rules and guarantees defined in this document, and to conduct its investigation according to the recommendations made by the Conseil national des barreaux⁴.

⁴ https://www.cnb.avocat.fr/sites/default/files/documents/guide-cnb_enquetes-internes_juin2020.pdf

How is the investigation conducted ?

The investigation is carried out according to a process that ensures (i) the **confidentiality** of the identity of the whistleblower as well as of any other person implicated and (ii) the **presumption of innocence** of any person involved.

The person(s) in question will be informed of the existence of the report and heard within the framework of the internal investigation, without however being associated with the conduct of the investigation and its conclusions. When precautionary measures are necessary, in particular to avoid the destruction of evidence, the person who is the subject of a report will be informed after the adoption of these measures.

Depending on the results of the investigation, disciplinary or legal proceedings may be initiated by Soitec SA or the companies of the Soitec group, in particular against the employees involved, if necessary⁵.

In addition, the Soitec group undertakes to make its best efforts to remedy the reported violation and to conduct an analysis of the root causes of the breach in order to continuously improve its ethics and compliance procedures.

In any case, the investigation will be conducted in accordance with any provisions provided for by the applicable national law.

How is confidentiality, and the case being, anonymity, guaranteed?

All reports will be handled with the **highest degree of confidentiality** and the confidentiality of the person making the report will be guaranteed as well as the confidential personal data that is collected, communicated and stored. Information about a report is only shared with a limited number of people who strictly need to know.

Conversely, we also ask anyone who is the subject of or involved in an internal investigation to maintain confidentiality and not to share or discuss the report with anyone outside the scope of the investigation.

If the whistleblower does not wish to disclose his/her identity, he/she has the **possibility of reporting completely anonymously** via the Maât ethics alert line. This platform serves as a confidential, secure and anonymous communication channel between the person reporting a problem and the people in charge of the internal investigation. However, it should be noted that it is sometimes more difficult, or even impossible in certain circumstances, to investigate an anonymous report.

⁵ However, when the limitation periods so require, disciplinary or legal proceedings may be initiated before the end of the internal investigation.

How long does it take to process an alert?

The deadlines below are applicable following a report, except for stricter deadlines provided for by the applicable national law:

- The author of the report is informed in writing of the receipt of his/her report within a period of **seven business days** from the date of receipt;
- At the latest **three months** from the acknowledgment of receipt of the report, the Soitec group communicates to the whistleblower information on the measures planned or taken to assess the accuracy of the allegations and, if necessary, to remedy the violation reported, as well as on its root causes.

How is the collected personal data protected?

The recipient of the report shall take all necessary precautions to preserve the **data security** during their collection, communication and conservation.

In accordance with French and European data protection law, any person identified in the context of a report has a **right of access and rectification** on its personal data by contacting the address dpo@soitec.com.

Reports may only be kept for the duration strictly necessary and proportionate to their processing and the protection of the whistleblower, the people involved and the third parties they mention, taking into account the time limits for any additional investigations. Data relating to reports may however be kept beyond this period, provided that the persons concerned are neither identified nor identifiable.

The personal data protection policy is available on Maât platform's homepage.

Consequences of reporting

Can retaliation measures be taken against the whistleblower?

No, as long as the author of the report meets the conditions of eligibility described above, in particular good faith. Especially, **the whistleblower cannot be subject to any retaliation measures**, or threats or attempts of retaliation⁶.

It should also be emphasized that these protective measures apply not only to the whistleblower, but also to:

- **Facilitators**, i.e. any natural or legal person who helps a whistleblower to make a report;
- **Natural persons linked to a whistleblower** who risk being subject to retaliation in the course of their professional activities;
- **Legal entities controlled by the whistleblower**, for which he/she works or with which he/she is linked in a professional context.

In addition, under applicable law, the author of the report is likely to benefit from civil and criminal immunity⁷, and the witnesses from specific protective measures.

Conversely, in the event that the alert mechanism is used in **bad faith**, for example for the purpose of **calumny** or **defamation**, the author of the alert is exposed to possible **disciplinary and criminal proceedings**.

⁶ And in particular: suspension, layoff, dismissal or equivalent measures; demotion or denial of promotion; transfer of functions, change of place or hours of work, reduction of salary; negative performance evaluation or work certificate; disciplinary measures; bullying or harassment; discrimination, disadvantageous or unfair treatment; non-conversion of a fixed-term employment contract or a temporary contract into a permanent contract, when the worker could legitimately expect to be offered a permanent job; non-renewal or early termination of a fixed-term employment contract or a temporary contract; early termination or cancellation of a contract; etc. In France, if such measures were nevertheless to be taken, they would be null and void.

⁷ In France, persons who report or publicly disclose information benefit from civil immunity for damages caused as a result of their reporting or public disclosure if they had reasonable grounds to believe, when they did so, that reporting or public disclosure of all of this information was necessary to safeguard the interests at stake. Similarly, in France, persons who have reported or disclosed information benefit from the criminal immunity provided for in article 122-9 of the penal code.