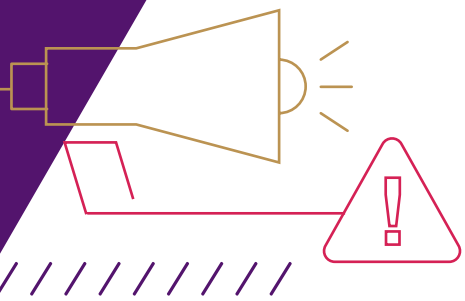
PROFESSIONAL ALERT SYSTEM

AFNOR INTERNATIONAL



This system has been set up in accordance with:

- Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and modernisation of economic life revised by the Law of 21 March 2022 aimed at improving the protection of whistleblowers, known as the "Waserman" Law (hereinafter referred to as the "Sapin 2 Law");
- Decree No. 2022-1284 of 3 October 2022 issued by the Council of State pursuant to Article 8 of Law No. 2016-1691 above, hereinafter referred to as the "Decree";
- Implementation Decree 2017-564 of 19-4-2017 on the procedures for collecting whistleblower alerts;
- Organic Law No. 2022-400 of 21 March 2022 aimed at strengthening the role of the Defender of Rights in terms of whistleblowing.

1 ONLY ONE SYSTEM

For all reports

To **simplify and improve efficiency**, the AFNOR group decided to set up a single alert system covering all types of alerts such as:

- a **crime**, an **offence**;
- a **threat to the general interest**: public **health** alerts (e.g. discovery of unexpected diseases or animal deaths in a specific location); **hygiene** (e.g. adverse health events resulting from the use of a cleaning product, medical device, etc.), **safety** (e.g. detection of a technical problem on a certified product) and the **environment** (e.g. environmental release of known toxic substances; accumulation of dangerous substances in an inappropriate location, etc.).
- any **violation of the regulations or legislation**;
- **sexual and gender-based violence** at work (alerts of this nature are subject to specific procedures depending on the involved parties);
- situations that c**onflict with the ethical charter** of the AFNOR group;
- behaviour **contrary to the AFNOR Group's code of conduct against corruption**;

Facts, information or documents covered by national defence secrecy, medical secrecy, the secrecy of deliberations, enquiries or investigations, or the confidentiality of lawyer-client relationships shall not be covered by this system.

Open to all

- Members of **staff**,
- **Former employees and job applicants** (where the information was obtained in the course of their professional activity and application respectively);
- **Individual members of the AFNOR association**;
- Directors and members of the **Executive Committee**.
- **External and occasional employees** of the AFNOR group, particularly temporary workers and trainees;
- Any **member of staff or manager of a company bound by a contract** with an AFNOR entity (service provider, client, etc.);
- Any **staff member or manager of a subcontractor** or co-contractor of an AFNOR entity.

2 WHAT IS A WHISTLEBLOWER?

To qualify as a whistleblower and benefit from protective status, the following conditions must be met:

- "a natural **person**":
  - someone who has direct knowledge of the facts they are reporting, where the information was not obtained as a result of their professional activities
  - someone who has knowledge of the facts they are reporting, including on account of being informed of them, where the information was obtained as a result of their professional activities;
- "who reports or **discloses this information, without direct financial consideration and in good faith**": someone who receives no benefits and is not paid for their efforts.
- "a **crime**, an **offence**, a **threat or detriment to the general interest**, a violation or an attempt to conceal a violation of an international commitment regularly ratified or approved by France, a unilateral act of an international organisation taken on the basis of this type of commitment, the law of the European Union, the **law or the regulations**. "

3 HOW TO RAISE AN ALERT?

Alert directed to AFNOR ("internal alert")

Any internal or external person can create an alert to AFNOR. For people within the AFNOR group: if there are doubts or questions about a particular situation, the line manager or compliance officer (head of the legal department) can be informed in advance.

The internal alert is directed to AFNOR:

- **Or to the following email address: alerte@afnor.org**
- **Or by post:** Groupe AFNOR, To the attention of the Compliance Officer (Head of the Legal Department), 11 rue Francis de Pressensé, 93570 La Plaine Saint Denis.

The information to be provided is as follows:

1. If the creator gives consent: first name, last name, position and place of work;

2. Required: The facts that the person wishes to disclose, in an objective and precise manner, to enable the admissibility of the alert to be verified;

3. Required: The postal or email address, if applicable, where the person wishes to be informed about the status of the alert, if different from the one used for the initial alert.

Alert directed to the authorities ("external alert")

If the internal alert is addressed by AFNOR within 3 months of receipt, or even directly without sending an alert to AFNOR, the alert creator may create an external alert by referring the matter to one of the legal or administrative authorities mentioned in the appendix to the Decree, categorised according to the field in which the alert relates to (public markets, financial services and products, product safety, transport safety, environmental protection, food safety, child protection, etc.).

Alert directed to the media ("public alert")

Finally, the alert creator may disclose it publicly (media, networks, associations, etc.) in the following cases:

- In the event of **serious and imminent danger**, clear danger to the general interest, when the information has been obtained as a result of their professional activities;
- Where external whistleblowing would put them at **risk of reprisals** or would not effectively address the subject matter of the disclosure or where there is a **conflict of interest**
- If no appropriate action has been taken by the external authorities in response to the external alert before the deadline expires. These deadlines vary depending on the external authority involved:
  - All external authorities other than the Defender of Rights, the legal authority or an EU institution, body, or agency:
    - 3 months from the acknowledgement of receipt of the alert, or;
    - in the absence of an acknowledgement of receipt 3 months from the expiry of a period of 7 business days following the alert. This period is extended to 6 months if the circumstances of the alert (nature, complexity, etc.) require further action, in this case the authority shall inform the whistleblower before the expiry of the 3-month period.
  - The Defender of Rights, legal authority, an institution, body or agency of the European Union responsible for collecting information on violations falling within the scope of EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 mentioned above:
    - 6 months from the acknowledgement of receipt of the alert or;
    - in the absence of an acknowledgement of receipt 6 months from the expiry of a period of 7 business days following the alert.

4 HOW ARE ALERTS PROCESSED?

Admissibility

Once the alert is received at the dedicated email address or by post, it is considered receivable by the Compliance Officer who examines whether the following cumulative conditions are met:

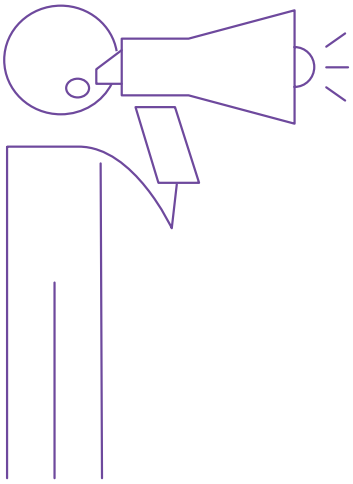
- it is **within the scope** of the system;
- it is being conducted in **good faith**;
- there is **no financial consideration**;
- it is of a **serious nature**;
- the **information provided is sufficiently precise** and can be verified.

If the alert is considered to fall within the scope of VSST, it is transmitted to the AFNOR contacts according to the specific procedure in force.

Receiving

When an alert is received, an **acknowledgement of receipt is sent to the sender within 7 working days** of receipt, to the email or postal address used by the sender:

- Informing the sender that the alert has been received;
- Informing them whether or not their report constitutes an alert;
- Where applicable:
  - giving a 3-month deadline to investigate the admissibility of his alert;
  - asking them to provide any additional information or documents in support of the alert;
  - informing them of the way in which they will be informed of the outcome to the alert.



Ad hoc committee

After receiving the alert, the Compliance Officer will set up an ad hoc committee composed of **members selected according to the subject** of the alert to carry out an internal investigation.

Internal investigation

After examining the serious nature of the alleged facts and the prima facie admissibility of the alert, the committee members carry out the necessary investigations to find any evidence that may or may not demonstrate the reality and materiality of the alleged facts, organise the processing of this alert, and list the actions to be implemented (search for evidence, computer searches, questioning of individuals, etc.) within 30 days of sending the acknowledgement of receipt.

The committee decides whether an **investigation report** should be prepared.

It will be systematically prepared if the issued alert demonstrates that there is a threat to the general interest, violation of regulations or legislation, sexual and sexist violence in the workplace, violation of the AFNOR Group's anti-corruption code of conduct or violation of the AFNOR Group's ethics charter. In this event, the ad hoc committee transmits its investigation report to the AFNOR Group's general management or human resource department, which will take the necessary corrective measures and any sanctions concerning the individuals involved in the alert.

Response

Following the examination of the alert by the ad hoc committee, whatever the outcome of the alert, a **thorough response** is sent by the Compliance Officer to the whistleblower **within 3 months after the sending of the response acknowledging receipt** of the alert.

Archiving and destruction of the data

Whatever the nature of the alert, including VSST, two possibilities should be considered:

- **It does not qualify as an alert under this system**: the destruction of all transmitted data identifying the alert creator and the person implicated shall be carried out within a maximum period of 4 months following receipt of the alert. The alert creator and the individuals concerned shall be informed.
- **It is qualified as an alert under this system**: the destruction of all transmitted data is carried out within the following deadlines:
  - If the alert is followed by a disciplinary procedure, or legal proceedings are initiated: the elements of the alert file allowing the identification of the alert creator and the person implicated shall be promptly destroyed after the closure of the disciplinary or legal procedure;
  - If no action is taken on the alert: the file shall be closed without further action and the elements of the alert file identifying the alert creator and the person implicated shall be destroyed within four months from the end of the admissibility analysis or the verification procedure.

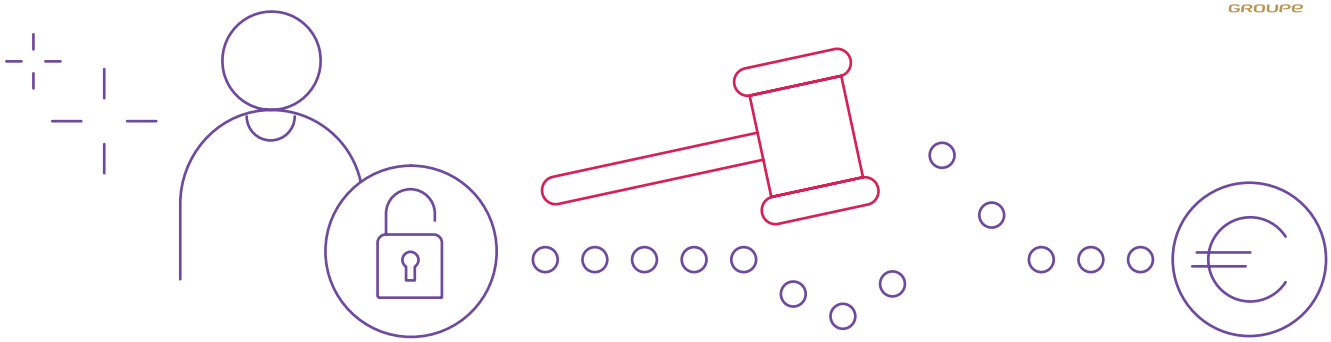
In all cases, the Compliance Officer keeps the anonymous elements to ascertain the number of alerts received, the reasons for them and the action taken. If necessary, these elements will permit the updating, monitoring and improvement of the AFNOR group's alert system.

5 FUNDAMENTAL PRINCIPLES

All data collected within the context of this alert system shall be treated confidentially, whether it concerns the identity of the alert's creator, the facts which are the subject of the alert or the individuals concerned by the alert. Specifically, the identity of the whistleblower shall not be communicated to the individual(s) involved in the alert, unless approved by the whistleblower. All necessary precautions are taken to safeguard the security of this information. The individuals responsible for collecting or responding to alerts are therefore subject to an obligation of increased confidentiality, enforced by a confidentiality charter.

Confidentiality

All data collected within the context of this alert system shall be treated confidentially, whether it concerns the identity of the alert's creator, the facts which are the subject of the alert or the individuals concerned by the alert. Specifically, the identity of the whistleblower shall not be communicated to the individual(s) involved in the alert, unless approved by the whistleblower. All necessary precautions are taken to safeguard the security of this information. The individuals responsible for collecting or responding to alerts are therefore subject to an obligation of increased confidentiality, enforced by a confidentiality charter.



Confidentiality can be lifted in the following cases:

- disclosure of the whistleblower's identity with their consent;
- disclosure of the person who is the subject of the alert once the validity of the alert has been established;
- transmission to the legal authority, informing the whistleblower in advance of this transmission, unless this information would jeopardise legal proceedings.

Disclosing confidential information is punishable by two years' imprisonment and a €30,000 fine (Article 9 of the Sapin 2 law).

Protection of Personal Data

Personal data collected within the context of this alert system is subject to an automated processing procedure which has received a declaration of conformity from the CNIL. Alert issuers or individuals concerned by the alert may exercise their right of access, rectification and modification of their data by sending their request to the email address dpo@afnor.org; for legitimate reasons they may object to the processing of their data and have the right to submit a complaint with the CNIL.

Whistleblower protection

The protected status of whistleblower provides **civil and criminal non-responsibility** for damage caused by their alert as long as the **disclosure of the information is necessary and proportionate to the protection of the interests involved** and that it takes place in compliance with the procedures for reporting alerts (Article 10-1 of the Sapin 2 law). A whistleblower may not be made redundant, sanctioned, excluded from a recruitment procedure, a work placement or professional training or discriminated against in any way for having reported facts in accordance with the alert reporting procedure.

Benefitting from the protected status of whistleblower (Article 6.1 of the Sapin 2 law):

- Person **with whistleblower status**;
- **Facilitators**, understood as any natural or legal person under private non-profit law (e.g. associations and trade unions) assisting the whistleblower in reporting and disclosing information about unlawful activities. Public organisations and for-profit companies are therefore not considered as facilitators;
- **Individuals who are in contact with a whistleblower and who may be at risk of reprisals** in their professional activities by their employer or client. This includes colleagues and relatives of the whistleblower;
- **Legal entities controlled** (within the meaning of Article L 233-3 of the Commercial Code) by the whistleblower, for whom they work or are linked to in a professional context.

Sanctions in case of voluntary obstacles or misuse of the system

The law stipulates a penalty of one year's imprisonment and a €15,000 fine for any person who in any way obstructs the internal transmission of an alert to the company or externally to the external authorities listed in the appendix to the Decree (Article 13 of the Sapin 2 law). The civil fine that can be applied in the event of abusive or delaying action is €60,000 notwithstanding the award of damages to the victim and the possibility of applying the additional penalty of publishing or broadcasting the verdict. Finally, the improper use of the alert system may result in the following sanctions for the alert creator:

- a disciplinary procedure that could lead to dismissal for misconduct, depending on the seriousness of the alleged offences;
- criminal proceedings for the offence of false accusation (punishable by 5 years' imprisonment and a €45,000 fine in France), breach of trust (punishable by 3 years' imprisonment and a €375,000 fine), and/or deletion or alteration of electronic data (punishable by 3 years' imprisonment and a €100,000 fine);
- civil liability towards the victim of the false accusation.

At La Plaine Saint-Denis, on .....

Myriam Augereau-Landais,
Managing Director AFNOR INTERNATIONAL