GROUPE CCF

Alerte Professionnelle

Instructions for use

The Alerte Professionnelle platform and its instructions for use are made available to all business relationships and employees of Groupe CCF and its subsidiaries, in accordance with Act no. 20161691 of 9 December 2016 on transparency, combating corruption and modernizing economic life.

Alerte Professionnelle is a platform that can be accessed 24 hours a day from any device (smartphone, tablet, PC), using an up-to-date web browser. **Alerte Professionnelle** provides secure access with an authentication code for reporting incidents. All data is encrypted.

The authentication code gives the reporter access to the follow-up of their report and to a personal and secure dialogue box on **Alerte Professionnelle**. This confidential code is unique, cannot be renewed if lost and cannot under any circumstances be passed on to a third party. It must be kept securely to prevent loss or identity theft.

Upon validation of the report, the reporter will receive an acknowledgement of receipt. Registrant can also access the acknowledgement of receipt by logging on to the platform using his code. Groupe CCF undertakes to send the reporting party, within ten days and to give its conclusions within a reasonable period not exceeding three months from the acknowledgement of receipt (information on the measures envisaged or taken to assess the accuracy of the facts and to remedy the subject of the report). This period is extended to six months if circumstances of the case, linked to its nature or complexity, require further diligence.

GROUPE CCF

Warnings

The business alert system is based on the principle of trust and transparency, enabling any employee or business associate to report a malfunction in a protected environment to ensure the company's long-term survival.

It is part of the company's ethical culture and the prevention of risks to which our activities are exposed.

For reasons of confidentiality and data security, Alerte Professionnelle does not send notifications to notifiers. Notifiers must regularly log in to Alerte Professionnelle using their authentication code in order to find out about requests for information and the progress of the processing of their alert, and to ensure that they are kept informed within the legal three-month time limit. It must be kept securely to prevent loss or identity theft.

This user manual is accompanied by the privacy policy. Notifiers are invited to read them before making any declaration.

GROUPE CCF

GROUPE CCF

1. Preliminary instructions

All Groupe CCF business relations wishing to make a professional alert are invited to read this notice beforehand to find out how it **is processed, the conditions of acceptance, their rights and those of any person incriminated. This notice is available in the Alerte Professionnelle legal notice.**

To report an alert, the reporter logs on to **Alerte Professionnelle**.

Before making a declaration, the declarant is invited to:

- Read the **instructions for use, which set out the processing procedures, associated protections and rights of the whistleblower and any person named in the alert**;
- Read the privacy policy, which sets out how personal data is processed under the scheme, and your rights of access, rectification and deletion;
- Report in good faith, without malice or financial gain. The information provided is factual and objective. It is sufficiently detailed to enable an analysis and assessment of the risk that the reported situation poses to the Group and/or its employees.
- Before sending your declaration, make sure that it does not contain any sensitive data, unless it concerns a case of discrimination or an infringement of human rights, fundamental freedoms or health.

1.1. Whistleblower protection

If the report is made in good faith, without intent to harm, without any direct or indirect financial consideration, and as long as the report falls within the scope of professional whistleblowing, the employee benefits from whistleblower protection as soon as he or she activates the system, in order to guarantee maximum protection.

No whistleblower may be punished, dismissed, or subjected to any direct or indirect discriminatory measure for having reported or testified, in good faith, to facts constituting an offence or a crime of which he or she may have become aware in the performance of his or her duties, or for having reported a whistleblowing incident falling within the scope of the professional whistleblowing system[1] .

A person who discloses a secret protected by law is not criminally liable, provided that the disclosure is necessary and proportionate to protect the interests in question, that it is made in compliance with the reporting procedures defined by law and that the person meets the criteria for whistleblowers.[2]

Nor is a whistleblower criminally liable if he or she removes, misappropriates, or conceals documents or any other medium containing information of which he or she has lawful knowledge.

In the event of an appeal against a retaliatory measure or obstruction of reporting, it will be up to the defendant to prove that its decision is duly justified.

[1] Articles L1132-3-3 and L.1121-2 of the Labour Code. "No person may be excluded from a recruitment procedure or from access to an internship or training period in the company, no employee may be sanctioned, dismissed or be the subject of a direct or indirect discriminatory measure, particularly with regard to remuneration, profit-sharing measures or the distribution of shares, training, redeployment, assignment, qualification, classification, professional promotion, transfer or renewal of contract or any other measure, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract, or any other measure, for having reported or testified, in good faith, to facts constituting an offence or crime of which he or she had knowledge in the performance of his or her duties, in compliance with the Sapin II Act".

[2] Article 7 Sapin 2 Act

For specific details concerning the protection of whistleblowers as employees, the declaring party shall refer to the French Labor Code, and Groupe CCF employees may consult the internal rules setting out the said code as well as the Professional Alert Policy applicable within Groupe CCF.

1.2. Protection of the facilitator

Whistleblower protection extends to facilitators under the same terms.

A facilitator within the meaning of the Act is[3] :

a) any natural person or non-profit-making legal person governed by private law who assists a whistleblower in reporting or making a disclosure;

b) Natural persons in contact with a whistleblower who risk being subjected to a discriminatory measure in the context of their professional activity by their employer, their client or the recipient of their services;

c) The legal entities controlled by a whistleblower for which he or she works or with which he or she has a professional relationship.

For operational purposes within Groupe CCF, to benefit from whistleblowing protection as a facilitator, the reporting party must mention, with their consent, the persons concerned in their alert. They will also be able to make an individual alert on the problem encountered. The facilitators may, if necessary, be approached by the referent in charge of processing the alert to obtain additional information to provide a better understanding of the situation reported.

1.3. Protecting and informing people affected by whistleblowing or investigations:

In the specific case of a whistleblowing alert, **any person who is the subject of a whistleblowing alert is presumed innocent until the allegations against him or her are established.**

Information likely to identify the person implicated by an alert may only be disclosed, except to the judicial authority, once it has been established that the alert is well-founded. Disclosing confidential information is punishable by two years' imprisonment and a fine of €30,000[4] **.**

The denunciation, by any means and directed against a specific person, of a fact which is likely to lead to judicial, administrative or disciplinary sanctions and which is known to be totally or partially inaccurate, when it is addressed either to an officer of justice or of the administrative or judicial police, or to an authority with the power to follow it up or to refer it to the competent authority, or to the hierarchical superiors or employer of the person denounced, is punishable by five years' imprisonment and a fine of 45,000 euros.[5]

The accused person is informed of the charges against him or her so that he or she can exercise his or her rights, including the right of defence and respect for the adversarial principle. This information also specifies the procedures for exercising their rights of access, rectification and opposition to personal data concerning them.

The data subject will be informed no later than one month after the alert has been issued, unless there is a risk of evidence being lost, if the information is likely to "seriously compromise the achievement of the objectives of the said processing operation". In this case, the information provided to the person concerned may be suspended until the end of the investigation. In such cases, the person concerned

[3] Article 6-1 of the Sapin II Act
[4] Article 9 of the Sapin II Act
[5] Article 226-10 of the Criminal Code

must be informed of the recording of personal data concerning him or her at the end of the investigation, and of any subsequent action taken.

If Groupe CCF considers that the risk is moderate, the notice sent to the person concerned will remind them that tampering with or destroying evidence is a criminal offence liable to prosecution.

Under no circumstances will the identity of the whistleblower be disclosed to him or her, to guarantee the whistleblower's protection.

If a breach is established, any employee implicated may be subject to disciplinary sanctions as defined by the internal regulations of each legal structure. Legal action may be taken against the individual concerned if the company decides to bring the facts to the attention of the judicial authorities by means of a complaint or a simple report.

If the breach is established and the person in question is a business associate (natural person and/or legal entity) of Groupe CCF or one of its subsidiaries, the latter reserve the right to terminate the contract binding them but also to take any legal action they deem necessary.

2. Applicable rules

2.1. What are my obligations as a registrant?

1. Consent to the privacy policy
2. Make sure that the report I wish to make falls within the scope of the whistleblowing procedure specified in section 2.3 of these instructions. If in doubt, I should specify the reason for my alert. In any case, it will be analysed and its admissibility will be confirmed.
3. Report in good faith, without malice or financial gain
4. Present the facts in an objective and factual manner and, where appropriate, provide any document or medium that supports the facts: messages and supporting documents are secured and archived in accordance with the conditions set out in the confidentiality policy.
5. Not to communicate sensitive data (see definition in the confidentiality policy) unless the case reported involves discrimination.)
6. Keep the confidential code generated when my alert was created, as it will enable me to log in again and follow the progress of the processing in **Alerte Professionnelle**. Under no **circumstances may it be passed on to a third party, nor may it be regenerated if lost.**
7. Only use the **Alerte Professionnelle** platform for written exchanges with the referrer or any designated expert, to ensure traceability and confidentiality.

2.2. Anonymity

On **Alerte Professionnelle**, employees (or any business relations) can report an alert anonymously, talk to the contact person and follow up their alert, while retaining the benefit of anonymity, thanks to a private and secure dialogue box.

Allowing and guaranteeing anonymity to those who wish to do so means allowing them to report something that they would not otherwise do for fear of exclusion, loss of job or other reprisals.

The URL for accessing **Alerte Professionnelle** can be used from a computer, a connected mobile phone, a company tablet or an external connection. **The use of an external connection medium reinforces the anonymity of the declarant (unknown IP address).**

If the whistleblower is anonymous, he or she cannot benefit from the protections that require the whistleblower to be known. They are, however, protected by anonymity.

Where the report is anonymous, the whistleblower whose identity is subsequently revealed will benefit from the same protections as an identified whistleblower.

The anonymous alert[6] will only be processed if the facts mentioned are established, and only if the factual elements are sufficiently detailed and make it possible to establish the accuracy of the facts declared. Reporters may use the **Alerte Professionnelle** function to attach any evidence, regardless of its form or medium, to support the facts mentioned.

Where the allegations appear to be true, the Reporting Officer will use the means at his disposal to remedy the matter and will inform the reporting party of the action taken. If the allegations are inaccurate or unfounded, or if the alert has become devoid of purpose, the Reporting Officer will give reasons and inform the reporting party in writing of the closure of the alert.

The time limits for providing feedback to the originator of an internal or external alert do not apply to anonymous alerts.

2.3. Eligible reports

In order for an upstream report to be classified as a professional alert, it must comply with the following cumulative:

- The declarant is a natural person who falls within the scope of this policy[7]
- The report is made without financial consideration and in good faith [8]
- The information provided must be factual and directly related to the subject of the alert. It must relate to objective, materially verifiable facts likely to reveal the presumed nature of any breaches. Only information that is objective, relevant, appropriate, and directly related to the scope of the alert and strictly necessary for subsequent verification will be considered.

  As any written document is likely to be made available to the authorities in the event of legal proceedings, the whistleblower must describe the facts objectively, with the rigor and professionalism that would naturally be expected of an external and occasional employee or collaborator, and in such a way as not to run the risk of committing the entity, and more generally a Groupe CCF entity, the managers of the entities and its employees or collaborators beyond their responsibilities.

  Whistleblowers must use wording that, on the one hand, makes clear the presumed nature of the facts and, on the other hand, is in no way such as to infringe the privacy of employees or managers of the entity or the Group, or of any third party.

- The alert relates to events that have occurred or are very likely to occur and concerns:
  - ✓ information relating to a crime, an offence, a threat or harm to the general interest, a violation, or an attempt to conceal a violation of an international commitment duly

[6] CNIL guidelines on the processing of personal data for the purpose of implementing a professional alert system, adopted on 18 July 2019
[7] Paragraph 1.1 of the introduction.

[8] Cf 2.4

ratified or approved by France, a unilateral act of an international organization based on such a commitment, European Union law, a law or regulation"[9] ;

- ✓ reports from employees of conduct or situations that contravene the company's code of conduct[10] (legislative, regulatory, professional, ethical, or procedural provisions)
- ✓ acts of corruption or influence peddling, misappropriation of public funds or favoritism[11]
- ✓ any alert or report aimed at preventing serious violations of human rights and fundamental freedoms, the health and safety of individuals and the environment, resulting from the activities of the company and those of the companies it directly or indirectly controls, as well as from the activities of subcontractors or suppliers with whom it has an established commercial relationship, in accordance with the French Commercial Code[12] , in application of the law relating to the duty of vigilance[13] ;
- ✓ any behavior for which the whistleblower benefits from whistleblower protection under the Labor Code (discrimination, moral or sexual harassment, reprisals, or obstruction of the right to blow the whistle, etc.).[14]

This scheme does not apply to :

- Requests for mediation
- Customer complaints, which must be addressed to the dedicated departments of each commercial brand:
  - My Money Bank: ccrp@mymoneybank.com
  - Sorefi: serviceclients@sorefi.com
  - Somafi Soguafi: departement.consommateurs@somafisoguafi.com
  - CCF: https://ccf.fr/particuliers/aide-et-contacts.html
- Facts, information and documents, whatever their form or medium, the revelation or disclosure of which is prohibited by provisions relating to national defence confidentiality, medical confidentiality, the confidentiality of judicial deliberations, investigations or judicial enquiries or the professional confidentiality of lawyers[15] .

2.4. Good faith and misuse

The reporter has "*reasonable grounds to believe, in the light of the circumstances and the information available to them at the time of reporting, that the facts they are reporting are true*".

[9] Article 6, amended Sapin II Act
[10] Act no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (Sapin II), in accordance with Article 17, II, 2°.
[11] Article 17 of the Sapin II Act
[12] article L. 225-102-4
[13] LAW no. 2017-399 of 27 March 2017 on the duty of care is applicable to any company which employs, at the close of two consecutive financial years, at least five thousand employees within the company and in its direct or indirect subsidiaries whose registered office is fixed on French territory, or at least ten thousand employees within the company and in its direct or indirect subsidiaries whose registered office is fixed on French territory or abroad
[14] in the cases specified in Appendix 7: extracts from the Labour Code
[15] Article 6 of the Sapin II Act

The 2019 European Directive is explicit on this point: the requirement for whistleblowers to have reasonable grounds for believing that the facts they report are true is an essential safeguard against malicious, fanciful, or abusive reporting, since it ensures that persons who, at the time of reporting, have deliberately and knowingly reported false or misleading information are not granted protection. At the same time, this requirement ensures that the author of the alert remains protected when he or she has reported inaccurate information about violations in good faith.

The denunciation, by any means and directed against a specific person, of a fact which is likely to lead to judicial, administrative or disciplinary sanctions and which is known to be totally or partially inaccurate, when it is addressed either to an officer of justice or of the administrative or judicial police, or to an authority with the power to follow it up or to refer it to the competent authority, or to the hierarchical superiors or employer of the person denounced, is punishable by five years' imprisonment and a fine of 45,000 euros.[16]

Abusive use of the system may expose its author to possible sanctions or prosecution. Conversely, use of the system in good faith, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up, will not expose its author to any disciplinary sanction.

The processing of data as part of this internal system considers the CNIL reference dated 18 July 2019[17] relating to the processing of personal data intended for the implementation of a professional alert system.

2.5. Use of sensitive personal data[18]

Sensitive data means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as the processing of genetic data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

The processing of sensitive data is prohibited unless one of the following conditions is met:

1. the person concerned has given their explicit consent;
2. processing is necessary for the purposes of fulfilling the data subject's obligations and exercising his or her rights in the field of employment law, social security and social protection;
3. the processing is necessary in order to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent;
4. the processing relates to personal data which are manifestly made public by the data subject;
5. the processing is necessary for the establishment, exercise or defence of legal claims.

Processing is necessary for reasons of substantial public interest[19] , on the basis of Union law or the law of a Member State, which must be proportionate to the objective pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

[16] Article 226-10 of the Criminal Code
[17] Subject to repeal or reinforcement in application of the most recent laws applicable and taken into account in this notice.
[18] Regulation (EU) 2016/679 of 27 April 2016 (RGPD)
[19] Within the meaning of Article 9.2.g of the RGPD

It should be noted here that when processing an alert, Groupe CCF cannot intervene in the content of the alert issued by the reporting party, who is responsible for the sensitive data communicated.

3. Persons authorized to process an alert or who have access to the data

3.1. Confidentiality

Only those people strictly necessary to deal with the situation reported are involved in handling the alert, and they sign a confidentiality agreement before being given access to the details of the alert.

Access rights are limited and assigned by the ethics officer.

They sign a confidentiality agreement prior to accessing the platform, which commits them to strictly respecting the confidentiality of the identity of the authors of the alert, the persons targeted by the alert and the information collected, including in the event of communication to third parties where this is necessary solely for the purposes of verifying or processing the alert.

This confidentiality extends to the information gathered and all supporting documents submitted.

Elements likely to identify the whistleblower may only be disclosed with the whistleblower's consent. They may, however, be communicated to the judicial authorities if Groupe CCF is required to report the facts to them. The whistleblower is informed unless this information could compromise the legal proceedings. Written explanations are attached to this information.

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

Disclosing confidential information is punishable by two years' imprisonment and a €30,000 fine.

3.2. The Groupe CCF ethics unit:

The Ethics Officer and the General Secretary of Groupe CCF have, by virtue of their position and status, the competence, authority and resources required to carry out their duties. This position guarantees independent treatment.

- The Ethics Department is responsible for the system. It has access to all data and has rights to consult, write to, delete and configure the tool.
- It ensures that alerts are admissible by checking that they meet the eligibility criteria for whistleblowing. Once the alert has been assigned, and depending on its category, it is forwarded in **Alerte Professionnelle** to an internal or external expert, as appropriate. They will systematically check beforehand, in consultation with the reporting party, that the experts called upon are not personally involved in the alert or in a conflict of interest.
- It can request an internal investigation
- The Ethics Office ensures that the decision is taken in the absence of any conflict of interest and in accordance with the protection of whistleblowers, facilitators and, where applicable, any other persons concerned.

3.3. Business experts:

The experts are the business line experts (compliance, legal, HR, internal audit, risk and any other specialist department that can help resolve the situation reported). The expert only has access to the alert shared with him/her by the Ethics Officer and has consultation and writing rights.

In their alert, notifiers specify whether they wish to involve an expert from the legal structure or a group expert in the handling of their alert, and give their reasons for doing so in order to ensure that only strictly necessary persons are involved in the handling of their alert.

3.4. Technical administrator :

The technical administrator, who reports to the Ethics Officer, is responsible for the technical administration of the platform. He/she signs a confidentiality agreement and all the associated obligations mentioned in this policy apply to him/her.

3.5. Internal audit control

As part of the periodic control of the system, Groupe CCF provides access to Internal Audit on a one-off basis to enable it to carry out its controls. All auditors concerned sign a confidentiality agreement and all the obligations associated with the protection of whistleblowers and any other persons concerned apply to them.

4. Processing the alert

2.1. Acknowledgement of receipt, admissibility, processing time

- The reporting party, whether the alert is anonymous or not, can access at any time the acknowledgement of receipt generated on the platform on the day the alert was created.
- Exchanges take place exclusively within **Alerte Professionnelle**, which provides a secure dialogue box. Supporting documents are archived in **Alerte Professionnelle** in accordance with the retention rules set out in the confidentiality policy, which should be consulted.

For reasons of confidentiality and data security, Alerte Professionnelle does not send notifications to notifiers when they are asked for additional information. Notifiers must regularly log in to Alerte Professionnelle using their confidential code in order to find out about requests for information and the progress of the processing of their alert, and to ensure that they are kept informed within the legal three-month time limit.

- On receipt of the alert, Groupe CCF has three months[20] in which to carry out its analysis, confirming or denying the admissibility of the alert with the reporting party, without this period constituting a limit for ensuring exhaustive processing of the alert. It will base its analysis on the

[20] From the date of issue of the alert

acceptance criteria specified in these instructions and may, if it considers it necessary, ask the reporting party for additional information. The acceptability of the alert and the measures taken are communicated to the reporter via the **Alerte Professionnelle** secure dialogue box.

Groupe CCF will give the reasons why it considers that the alert does not fall within the scope of the system.

- If the alert does not fall within the scope of the professional alert system, or if the allegations are unfounded or inaccurate, or if the alert has become irrelevant, the reporting party is informed as soon as possible that the file has been closed[21] . Reporters are invited to contact their usual contact person (line manager, specialized departments, etc.) if necessary.

2.2. Handling alerts

If the report falls within the scope of the system, the ethics officer will ask a business expert to take charge of the situation reported in order to respond with the necessary expertise. Before any assignment, the ethics officer checks with the reporter that there is no conflict of interest.

The expert signs a formal confidentiality agreement prior to accessing the data contained in the alert. The Ethics Officer or the expert, in consultation with the Ethics Officer, shall inform the person who issued the alert of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy the subject of the alert, as well as the reasons for these measures. This information shall be provided within a reasonable period of time, not exceeding three months[22] , although this period of time shall not constitute a limit for ensuring that the alert is dealt with exhaustively.

Where the alert mentions an alleged perpetrator of inappropriate facts or behavior, Groupe CCF informs the latter of the facts of which he or she is accused within one month of the alert being issued so that he or she can exercise his or her rights, including his or her rights of defence and respect for the adversarial principle. Groupe CCF may decide to take precautionary measures, in particular to prevent the destruction of evidence relating to the alert and to defer information when this is likely to seriously compromise the achievement of the objectives of the said processing.[23.]

Groupe CCF can:

- **Contact the facilitators** appointed by the declarant (provided they have their contact details) or who have made a parallel alert on the same situation as that reported by the declarant. It should be remembered here that the facilitator enjoys the same protection as the whistleblower (see paragraph 1.2) of these instructions.
- **Request an internal investigation from Internal Audit**, depending on the seriousness or complexity of the facts raised. Internal Audit launches the internal investigation in accordance with its own rules and the principle of independence. The internal investigation is subject to strict rules designed to respect the obligations of confidentiality and protection of the whistleblower and any other designated person. Any designated investigator and/or third party must sign a confidentiality agreement prior to any access to the data contained in the alert.

[21] Article 4 Decree no. 2022-1284 of 3 October 2022
[22] From the date of issue of the alert
[23] See chapter 1.3.

Following an internal investigation, the formal drafting of an investigation report is intended to record all the facts and evidence gathered, both incriminating and exculpatory, to establish or dispel suspicion, as well as the method followed.

On **Alerte Professionnelle**, the secure dialogue box made available to the reporter enables the progress of the report to be monitored, discussions to be held with the ethics referent and the expert, and useful information and attachments to be sent. The retention/deletion of personal data complies with the rules set out in the Sapin II Act and its implementing regulations. Employees should refer to the "confidentiality policy" appendix[24] .

The time limits for providing feedback to the originator of an internal or external alert do not apply to anonymous alerts.

In all cases, the expert will formally record on the platform, in writing, the action taken on the alert, its admissibility as a professional alert, any measures that will be taken to guarantee its protection and remedy the situation, and the closure of the alert.

2.3. Information of the whistleblower and the person concerned

At the end of the analysis, a formal, reasoned decision is sent to the whistleblower and to the person concerned (perpetrator, victim, witness), applying the rules of confidentiality specific to the protection of the whistleblower and the person concerned and on condition that this communication does not prejudice the ongoing investigation, in particular to prevent the destruction of evidence.

This decision concludes the handling of the alert and specifies the action to be taken on the alert depending on the facts reported and their seriousness:

- No further action if the allegations are unfounded,
- Measures against the declaring party in the event of misuse (absence of good faith) in accordance with the sanctions defined by the internal regulations of the legal structure concerned,
- The introduction of measures to protect whistleblowers from professional discrimination,
- Where appropriate, measures to protect and/or compensate the victim,
- Where appropriate, legal action may be taken against the individual concerned if the company decides to bring the facts to the attention of the judicial authorities by means of a complaint or a simple report. It is obliged to do so if it falls within the remit of the authorities listed in article 40 of the Code of Criminal Procedure,
- Any measures required to strengthen the control system and identify newly identified risks,
- Pursuant to Article L. 4133- 4 of the French Labor Code, the Social and Economic Committee is informed of alerts transmitted by any employee indicating a serious risk to public health or the environment linked to the manufacturing processes used or implemented by the establishment.

[24] Please refer to the appendix "Confidentiality and personal data processing policy".

5. External reporting

Whistleblowers may also submit an external alert, either after having submitted an internal alert or directly:

- To the competent authority, in particular :
    - the ACPR or the AMF[25] for any failure to comply with the obligations set out in European regulations, the Monetary and Financial Code, the Insurance Code, the Mutual Insurance Code and the Social Security Code or the General Regulation of the Autorité des marchés financiers and which are supervised by one or other of these authorities.
    - The AFA (French Anti-Corruption Agency) for breaches of probity
    - The DGFIP for fraud involving value added tax, taxes, etc.
    - The DGCCRF for anti-competitive practices, fraud and consumer protection
    - CNIL and ANSSI (Protection of privacy and personal data, security of networks and information systems)
    - To the Défenseur des droits, who will direct the complainant to the authority or authorities best placed to deal with it;
    - To the judicial authorities ;
    - To a European Union institution, body, office or agency competent to collect information on breaches falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019

➢ **Public disclosure :**

Whistleblowers are protected when they publicly disclose information obtained in the course of their professional activities:

- In the event of imminent or obvious danger to the public interest, in particular where there is an emergency situation or a risk of irreversible harm;
- If no action is taken in response to an external alert, whether or not preceded by an internal alert, and no appropriate action has been taken in response to this alert by the end of the 3-month feedback period (not applicable in the case of anonymous alerts);
- If referring the matter to one of the competent authorities referred to above would expose the person concerned to a risk of reprisals or would not enable the matter to be dealt with effectively, owing to the particular circumstances of the case, in particular if evidence could be concealed or destroyed or if the person issuing the alert has serious grounds for believing that the authority may have a conflict of interest, be in collusion with the person making the disclosure or be implicated in the disclosure.

In these particular cases, he or she is not civilly liable for damage caused by public disclosure if he or she had reasonable grounds to believe, at the time he or she made the public disclosure, that public disclosure of all the information was necessary to protect the interests in question[26] . He is not criminally liable under article 1229 -of the French Criminal Code[27] .

[25] Articles L.634-1 to L.634-4 of the Monetary and Financial Code
[26] Article 6 of Act 2022-401 of 21 March 2022 to improve the protection of whistleblowers
[27] Article 6 of Law 2022-401 of 21 March 2022

This protection does not apply where public disclosure is prejudicial to the interests of national defence and security.

In the event of an external alert, the anonymous whistleblower will not be able to benefit from the protections that require knowing the person who made the alert. In addition, he or she will not be able to benefit from a return or a delay in the processing of his or her alert, given that the external authority will not be able to get back to him or her for lack of an address.

6. Penalties

Failure to comply with Law 2022-401 aimed at improving the protection of whistleblowers may expose Groupe CCF, one of its entities and/or its employees to a significant reputational risk, as well as to disciplinary, administrative, criminal, or financial sanctions[28] .

More specifically, the following **criminal penalties apply to** the whistleblowing system:

The denunciation, by any means and directed against a specific person, of a fact which is likely to lead to judicial, administrative or disciplinary sanctions and which is known to be totally or partially inaccurate, when it is addressed either to an officer of justice or of the administrative or judicial police, or to an authority with the power to follow it up or to refer it to the competent authority, or to the hierarchical superiors or employer of the person denounced, is punishable by five years' imprisonment and a fine of 45,000 euros.[29]

Any person who obstructs, in any way whatsoever, the transmission of an alert to the persons and bodies mentioned in the first two paragraphs of I and II of article 8 shall be punished by one year's imprisonment and a fine of €15,000.

In proceedings against a whistleblower for information reported or disclosed, the amount of the civil fine that may be imposed in the event of an abusive or dilatory action is increased to €60,000.

The civil fine may be imposed without prejudice to the award of damages to the party who has been the victim of dilatory or abusive proceedings. Offenders may also be subject to the additional penalty of posting or broadcasting the decision.

Disclosing the confidential details of a professional alert is punishable by two years' imprisonment and a €30,000 fine.

Any distinction made between individuals based on their status as whistleblowers, facilitators or persons in contact with a whistleblower constitutes discrimination.

Harassing another person through repeated comments or behavior with the purpose or effect of causing a deterioration in working conditions likely to infringe their rights and dignity, alter their physical or mental health or compromise their professional future, is punishable by two years' imprisonment and a fine of €30,000[30] .

If the bank fails to apply its obligations to prevent and detect corruption (including the internal whistleblowing system), it may be liable to a fine not exceeding €1 million, and individuals may be liable to an individual fine of €200,000. The financial penalty is proportionate to the seriousness of the breaches observed and to the financial situation of the legal entity or individual sanctioned[31] .

[28] Article 9 of law 2022-401
[29] Article 226-10 of the Criminal Code
[30] Article 222-33-2 of the Criminal Code
[31] Article 17 Sapin II