Procedure on the whistleblowing system

Group scope

Updated on : 18/04/2023

Version: A

Table of contents

Since 2009, the Eiffage Group has been committed to pursuing the values and objectives of the charter, in particular through the implementation of a whistleblowing system to eradicate unethical behaviour.

Such behaviour damages the Group's reputation, can lead to very significant financial risks and has an impact on all of its stakeholders, particularly its employees, shareholders, etc.

Law 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life notably instituted a whistleblower status in the event of a serious violation of a certain number of rules, thus constituting a first step in the protection of whistleblowers. In order to comply with these provisions, it was then decided to develop the existing whistleblowing system within the Group and to implement a code of conduct.

In transposition of the European directive of 23 October 2019 aimed at harmonising the protection of whistleblowers within the European Union, France adopted the law of 21 March 2022 and the decree of 3 October 2022.

The other EU countries in which the Group has subsidiaries are also in the process of transposing this directive. In the event of transposition in these other countries providing for more stringent measures than those set out below, these measures shall apply and prevail where appropriate.

This has led us to develop Eiffage's whistleblowing system.

A. Scope and modalities of the whistleblowing system

A.1. What is the scope of the alert system?

The whistleblowing system applies to all Eiffage Group companies, both in France and abroad (subsidiaries and controlled companies).

In particular, it aims to:

- failure to comply with the Group's code of conduct, which defines and illustrates the various types of behaviour to be avoided, in particular those likely to constitute corruption or influence peddling, as well as other unethical or illegal behaviour;
- the reporting of the existence or realisation of any risk relating to human rights and fundamental freedoms, the health and safety of individuals, and the environment as provided for by the law of 27 March 2017 on the duty of care of parent companies and ordering companies.

More broadly, the whistleblowing system can also be used to report information and transmit all available material in any form or medium on:

- a crime or an offence;
- a threat or harm to the public interest;
- a violation, an attempt to conceal a violation of an international commitment regularly ratified or approved by France, of a unilateral act of an international organisation taken on the basis of such a commitment, of European Union law, of the law or of the regulations.
  However, facts, information or documents, whatever their form or medium, covered by national defence secrecy, medical secrecy, the secrecy of judicial deliberations, the secrecy of investigations or judicial enquiries, or the secrecy of relations between a lawyer and his client are excluded from the whistleblowing system.

A.2. **Which physical persons are entitled to issue an alert?**

The following natural persons can enter an alert:

- employees ;
- persons whose employment relationship has ended where the information was obtained in the course of that relationship;
- persons who have applied for employment with the entity concerned where the information was obtained as part of that application;
- shareholders, partners and holders of voting rights in the general assembly, members of the administrative, management or supervisory body of the entity;
- external and occasional employees (such as temporary workers, employees on secondment, trainees, etc.);
- co-contractors and subcontractors and their respective staff.

A.3. **What kind of information or facts can be reported?**

The persons mentioned in b) may report unlawful professional acts described in a) of which they have knowledge or which have been reported to them.

A.4. **What are the procedures for reporting a professional alert?**

A.4.a. **How to report**

The persons mentioned in A2 can choose either the internal or the external channel to send their report, and this in a non-hierarchical way.

Finally, public disclosure is also possible under certain conditions as set out below.

A.4.b. **The internal channel**

If an employee of the Group has questions or doubts about a situation or behaviour, he or she can raise these concerns with their line manager.

If they consider it necessary or useful, they may at any time use the professional alert system and send their report:

- For France, to the Group alert system manager;
- For foreign countries, to the local alert system manager or the Group alert system manager.

For both France and abroad, referrals can be made online via the link: https://eiffage.integrityline.org/

The identity and contact details of the Group alert system manager and the local alert system managers are available in the annex to this procedure. They are subject to appropriate local communication and regular update.

The employee then provides the facts, information or documents that he or she has in order to support the report, as well as the elements that will allow an exchange with the person in charge of the alert system (local or Group).

Persons whose employment relationship has ended and who have applied for employment with the entity concerned, as well as shareholders, members of the administrative, management or supervisory body of the entity concerned, co-

contractors, subcontractors or members of their staff, or external or occasional employees, may refer the matter to the local professional whistleblower or the Group whistleblower mentioned above, in accordance with the same procedures as those described above.

In all cases, a physical meeting or a remote exchange can also be organised with the person in charge of the alert system entered (local or Group).

Lastly, they can enter their alert either by name or anonymously, although it is preferable that they state their name in order to facilitate exchanges with the persons referred to the internal channel and the conduct of investigations.

A.4.c. **The external channel**

The whistleblower may also make an external alert, either after having made an internal alert in accordance with the procedures described above, or directly to a competent authority (for France, among those designated by the decree of 3 October 2022) which will receive and process it in accordance with its established procedure in this area, to the defender of rights who will direct him or her to the authority or authorities best able to deal with it, to the judicial authority or to a European institution, to a European body or to a body of the European Union competent in this area.

A.4.d. **Public disclosure**

Finally, the whistleblower may make his or her alert public after having made an external alert (whether or not preceded by an internal alert), without any appropriate action having been taken in response to that alert, and this at the end of a period of three months in case of referral to a competent authority and of 6 months in case of referral to another authority, from the acknowledgement of receipt of his or her alert or, in the absence of acknowledgement, at the end of the period of seven days following the alert, or at any time in the event of an imminent or obvious danger to the general interest. It is also possible where external reporting would run the risk of retaliation or would not effectively address the subject matter of the disclosure due to the particular circumstances of the case.

A.5. **Treatment modalities**

A.5.a. **Alert through the internal channel**

The local alert system manager or the Group Alert System Manager, internal recipients of the alert, will acknowledge receipt of the alert in writing within 7 days.

In the event of a report received from a subsidiary, the Group alert system manager may, when he or she considers it relevant in view of the facts reported, invite the sender of the alert to report directly to the local alert system manger, provided that the latter exists and that the sender of the alert has not chosen to address the Group directly.

The person in charge of the local alert system or the person in charge of the Group alert system will then check the admissibility of the alert. If necessary, he/she will inform the sender of the alert of the reasons for its non-admissibility.

It shall decide on the follow-up and may order all investigations to be carried out under its responsibility with the internal or external means it deems useful.

The investigation shall be conducted as quickly as possible. The sender of the alert

shall be informed in writing, within a reasonable period of time not exceeding three months from the acknowledgement of receipt of the alert or, in the absence of such acknowledgement, three months from the expiry of a period of seven working days following the alert, of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy the subject matter of the alert, as well as of the reasons for such measures.

In the event that the allegations are found to be inaccurate or unfounded, or when the alert has become irrelevant, the local alert system manager or the Group alert system manager will inform the sender of the alert in writing (via the platform) that the case has been closed.

A.5.b. **2.2 Alert via the external channel**

Each EU country sets the conditions and deadlines within which external authorities must acknowledge receipt of whistleblowing reports and provide feedback to whistleblowers under the conditions set out in the EU Directive of 23 October 2019.

As a reminder of the preamble, for France, the law to improve the protection of whistleblowers was adopted on 21 March 2022. This law is complemented by texts issued by the competent authorities.

A.6. **Reporting arrangements**

A.6.a. **Local alert in a foreign subsidiary**

As soon as an alert is received, the local alert system manager completes and updates the “integrity line Eiffage” alert platform.

A.6.b. **Alerts at Group level (general case)**

The Group alert system manager:

- reports on the alerts received to the Group's ethics officer appointed by the Board of Directors of Eiffage S. A.;
- performs an anonymised consolidation of alerts for communication in line with the Group's regulatory obligations.

B. Rights and duties under the whistleblowing system

B.1. **What should the whistleblower's principles of action be?**

The whistleblower must act responsibly, without direct financial gain and in good faith.

It must report sufficiently substantiated facts and provide, where appropriate, precise information to facilitate the handling of the alert.
If the whistleblower has used the system in good faith, he or she will benefit from the protections described below - even if the facts he or she has reported are later found to be inaccurate or do not lead to any follow-up.
Finally, in the event of misuse of the system or defamation, possible disciplinary measures or legal proceedings may be considered.

B.2. What protective measures are applicable?

B.2.a. Protective measures for whistleblowers

B.2.a.i. The whistleblower is in France

By exercising the whistleblowing right in accordance with the provisions described above, the whistleblower benefits from :

- special protective measures provided for by the French law of 9 December 2016 and the law of 21 March 2022 and its implementing decree. He or she may not, in particular, be subject to disciplinary sanctions, retaliatory measures, or threats or attempts to resort to such measures, in particular in the forms mentioned by the law;
- civil immunity for damage caused by their reporting or public disclosure under the conditions provided for by law;
- immunity from prosecution as provided for in Article 122-9 of the Criminal Code.

B.2.a.ii. The whistleblower is abroad

The whistleblower is entitled to the same protection measures as well as those provided for by national/local regulations. The whistleblower can obtain further information from the local whistleblower.
It should be noted that the protection measures described above also apply to the whistleblower's facilitator, i.e. to any natural or legal person under private non-profit law who helps the whistleblower to report, whether in France or abroad.

B.2.b. Is confidentiality guaranteed ?

If the whistleblower has made the alert by name, he or she is assured by the Group that his or her identity will be treated in strict confidence.
The identity of the whistleblower will not be communicated either to the persons who may be implicated, or to any third party he or she may have mentioned in the context of his or her alert, or to his or her direct hierarchy (if he or she has not informed it beforehand), except to the judicial authority if the persons in charge of the investigation are obliged to denounce the facts to him or her (and this only once it has been established that the whistleblower's allegations are well founded). The whistleblower will then be informed, unless such information would compromise the judicial proceedings. Written explanations will be attached to this information.
Finally, in the event that the alert is received by collaborators who are not authorised by this procedure (see paragraph A.4.a), the aforementioned collaborators must forward the alert without delay to the persons who must be notified in the context of this procedure.

B.2.c. How is the whistleblower's personal data managed and protected?

The information collected in the context of the whistleblowing system is processed electronically and recorded in the Group's data processing register.
The legal basis for this processing is compliance with a legal obligation and associated local regulations.
Only information relevant and necessary for the purposes of the processing is collected and stored in the alert system, namely

- Identity, functions and contact details of the sender of the alert, of the persons who are the subject of the alert and of the persons involved in the collection or processing of the alert;
- Reported facts ;
- Elements collected in the framework of the verification of the reported facts ;
- Reports of verification operations ;
- Follow-up to the alert.

B.3. **Receiving alerts**

Eiffage uses an IT platform provided by EQS (Integrity Line Eiffage), whose data is encrypted and stored on a server in the European Union. Only authorised Eiffage employees (local and Group alert managers) have access to this data. Each alert received is stored on a durable and retrievable medium.

When the report is collected during a physical meeting with authorised Eiffage employees, they will enter it on the Integrity line Eiffage platform. The same storage procedures as those described above will apply.

The whistleblower will have the opportunity to check, correct and approve these transcripts or entries.

B.4. **Handling alerts**

Once the admissibility of the report has been checked by authorised Eiffage employees, the whistleblower's data will be processed as follows:

If the referral does not fall within the scope of the scheme, the related data will be destroyed or anonymised without delay.

If the referral falls within the scope of the scheme, any verified data will be destroyed or anonymised by the relevant whistleblower within two months of the completion of the verification of the information, except in the case of disciplinary proceedings or legal proceedings against the person(s) concerned or the author of the abusive alert or any other person, or unless there are objective legal or procedural reasons. In the latter case, the data will be kept until the end of the proceedings or the legal obligations to keep it.

This closure will be made known to the whistleblower and to the persons to whom the alert was issued.

Anonymised data are kept for an unlimited period of time.

In accordance with the General Data Protection Regulation n°2016/679 and with Law n°78-17 of 6 January 1978 as amended, the whistleblower has a right of access, rectification, deletion of data concerning him/her, a right to limit processing and a right of opposition, as well as the right to formulate specific and general directives concerning the conservation, deletion and communication of his/her post-mortem data.

To exercise these rights or for any questions about the processing of whistleblower

data under this scheme, whistleblowers may contact the Group Data Protection Officer by writing to dpo.groupe@eiffage.com. If the whistleblower believes, after having contacted the Group's data protection officer, that his or her "data protection" rights have not been respected, he or she may file a complaint with his or her competent data protection authority (e.g., for France, the CNIL).

Editor : Direction gestion des risques et conformité – Contrôle interne