

## PROFFESIONAL ALERT SYSTEM – EIFFAGE INTEGRITY LINE

Since 2009, the Eiffage Group has been committed to pursuing the Charter of Values and the objectives it sets out, 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 its stakeholders, particularly its employees and shareholders.

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 European Union countries in which the Group has subsidiaries are also transposing this directive.

This has led us to develop Eiffage Integrity Line - whistleblowing system of Eiffage Group.

### Scope and modalities of the whistleblowing system

#### a. 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 elements, regardless of their form or medium, concerning a crime or offence, a threat or harm 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 such a commitment, European Union law, or the law or 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.

#### b. Who is entitled to report?

The following natural persons may report unlawful professional acts referred to above of which they have knowledge or which have been reported to them:

- Employees and persons whose employment relationship has ended where the information was obtained in the course of that relationship;
- Individuals who have applied for a job in 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.);
- The co-contractors and subcontractors and their respective staff.

### **c. How does the whistleblower scheme work?**

#### **1. Reporting and collection procedures**

Individuals may choose either the internal or the external channel for reporting, in a non-hierarchical way. Public disclosure is also possible under certain conditions as set out below.

The issuer shall act responsibly, without direct financial consideration and in good faith. They must report sufficiently substantiated facts and provide, where appropriate, precise information in order to facilitate the handling of the alert.

If the whistleblower has used the system in good faith, he or she will benefit from the protection measures described below - even if the facts he or she has reported subsequently prove to be inaccurate or do not lead to any follow-up. In case of misuse of the system or in case of defamation, possible disciplinary measures or legal proceedings may be considered.

##### **1.1. 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 whistleblowing system and send their report:

- For France, to the Head of the Group Alert System;
- For abroad, to the local Warning System Officer or the Warning 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 Warning System Manager and the Local Warning System Managers are available in the annex to this procedure. They are subject to appropriate local communication and regular updating.

The person then provides the facts, information or documents that he or she has to support the alert, as well as the elements allowing an exchange with the person responsible for the alert system. They may report the information by name or anonymously, although it is preferable that they declare their name in order to facilitate exchanges through the internal channel and the conduct of investigations.

Persons whose employment relationship has ended and who have applied for a job in 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 the latter's staff, or external or occasional employees, may refer the matter to the person responsible for the whistleblowing system (Warning System Officer or the Warning System Manager) in the same way.

In all cases, a physical meeting or a remote exchange can also be organised with the person responsible for the alert system entered (Warning System Officer or the Warning System Manager).

##### **1.2. The external channel**

The person 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 collect and process it in accordance with its established procedure in the matter, to the Defender of Rights, who will direct the person 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 the matter.

##### **1.3. Public disclosure**

Finally, the person may make his or her alert public after having issued an external alert (whether or not preceded by an internal alert), without any appropriate action having been taken in response to that alert, at the end of a period of three months from the acknowledgement of receipt of his or her alert or, if no acknowledgement has been given, 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.

## **2. Treatment modalities**

### **2.1. Alerting through the internal channel**

The person in charge of the alert system (Warning System Officer or the Warning System Manager), the internal recipient of the alert, acknowledges receipt of the alert in writing within seven working days. The Warning System Manager may, when he or she considers it relevant in view of the facts reported, invite the sender to report directly to the head of the Warning System Officer, provided that the latter exists and that the sender of the alert has not voluntarily chosen to address the Group directly.

The person in charge of the alert system (Warning System Officer or the Warning System Manager) checks the admissibility of the alert. If necessary, he/she informs the sender of the alert of the reasons for its non-admissibility. He/she decides on the follow-up to be given to the alert and can order all investigations to be carried out under his/her responsibility with the internal or external resources he/she 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 Warning System Officer or the Warning System Manager will inform the sender of the alert in writing (via Eiffage Integrity Line) that the case has been closed.

### **2.2 Alerting 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. In France, the law aimed at improving the protection of whistleblowers was adopted on 21 March 2022. This law is complemented by texts issued by the competent authorities.

## **3. Reporting arrangements**

Warning System Manager reports on the alerts received to the Group's ethics officer appointed by the Board of Directors of EIFFAGE SA. He/she consolidates the alerts in an anonymous manner so that they can be communicated in accordance with the Group's regulatory obligations.

Abroad in a subsidiary: as soon as the alert is received, the Warning System Officer completes and updates the Eiffage integrity line alert platform.

### **a) What protection measures are applicable?**

In France, by reporting in accordance with the provisions described above, the issuer benefits from the specific protective measures provided for by the French law of 9 December 2016 as well as by the law of 21 March 2022 and its implementing decree. He may not, in particular, be subject to disciplinary sanctions, retaliatory measures, or threats or attempts to resort to such measures, particularly in the forms mentioned by the law. They also benefit from civil immunity for damage caused by their reporting or public disclosure under the conditions provided for by law and from criminal immunity as provided for by Article 122-9 of the Criminal Code.

Abroad, the whistleblower benefits from the same protection measures as well as those provided by national/local regulations. The whistleblower can obtain further information from the Warning System Officer.

These protection measures also apply to the whistleblower's facilitator, i.e. any natural or legal person under

private non-profit law who helps the whistleblower to report, whether in France or abroad.

**b) Is confidentiality guaranteed?**

If the sender has made the alert by name, he/she is assured by the Group that his/her identity will be treated as strictly confidential. His identity will not be communicated either to the persons who may be implicated, or to any third party he may have mentioned in the context of his alert, or to his direct hierarchical line (if he has not informed them beforehand), except to the judicial authority if the persons in charge of the investigation are obliged to denounce the facts to him (and this only once it has been established that the alert is founded). He or she will then be informed (together with explanation), unless such information would jeopardise the judicial proceedings.

In the event of an alert to non-authorized staff, they must pass it on without delay to Warning System Officer or the Warning System Manager who must be notified under the system.

**c) How is the whistleblower's personal data managed and protected?**

The information collected in the context of the whistleblowing system is subject to computer processing recorded in the Group's 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 and elements collected in the framework of the verification of reported facts,
- Reports of verification operations and follow-up.

Eiffage uses an IT platform provided by EQS (Eiffage Integrity Line), whose data is encrypted and stored on a server in the European Union. Only authorized Eiffage employees (Warning System Officer or the Warning System Manager) have access to this data. Each alert received is stored on a durable and retrievable medium. When the alert is received during a physical meeting with authorized Eiffage employees, they enter it on the Eiffage Integrity line platform and the same storage procedures apply.

The issuer has the possibility to check, correct and approve these transcripts or entries.

Once the admissibility of the alert has been checked, if the referral does not fall within the scope of the system, it will be destroyed or made anonymous 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 issuer 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 procedures or legal obligations of conservation. The whistleblower will be informed of this closure, as well as of the persons concerned by the alert.

Anonymised data are kept for an unlimited period of time.

In accordance with the General Data Protection Regulation n°2016/679, in France with Law n°78-17 of 6 January 1978 as amended, and with local regulations, 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 Data Protection Officer of their entity or the Group Data Protection Officer by writing to [dpo.groupe@eiffage.com](mailto: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 lodge a complaint with his or her competent data protection authority (in France, the CNIL).