CFAO GROUP WHISTLEBLOWING PROCEDURE

CONTENTS

1 SCOPE, CONDITIONS AND GUARANTEES OF USE

1.1 Scope of the system

This ethics whistleblowing system allows any employee of CFAO group (hereinafter referred to as “CFAO” or the “Group”) or its commercial partners and any individual whose interests are likely to be affected by the Group’s activity to bring to its attention information concerning a crime, an offense, a violation of law or an attempt to conceal the law or regulations, a threat to the general interest or actions contrary to the Group’s Code of Conduct and Ethics (“COCE”), and/or the Group’s Anti-Corruption Code of Conduct of which he/ she has knowledge.

Facts that may be reported include corruption and influence peddling, conflicts of interest, money laundering and terrorist financing, anti-competitive practices, non-compliance with economic sanctions programmes; violations of human rights and fundamental freedoms; discrimination and moral or sexual harassment; breach of privacy and data security.

1.2 Conditions for admissibility and protection of the whistleblower

This whistleblowing system is complementary (does not replace) to other existing reporting methods within the company (hierarchical route; Human Resources Department; Legal Department; Compliance; Etc.).

To be admissible, alerts must meet the conditions listed below:

• **Natural person:** the use of this system is reserved for natural persons: employees of CFAO group or its commercial partners and any individual whose interests are likely to be affected by the Group’s activities.

• **Authentication:** The whistleblower will communicate his identity clearly and unambiguously (surname, first name, position, employer, email, telephones, Etc.) in such a way that it justifies his capacity to act;

• **Confidentiality:** CFAO undertakes to treat the identity of the whistleblower, the information and documents received as well as the identity of the persons named in the alert, with the strictest confidentiality;

• **Anonymity:** CFAO’s whistleblowing system is not anonymous; as an exception, anonymity is accepted if the supporting evidence provided is sufficiently detailed (documents, supporting data) to establish the seriousness of the facts. Indeed, the processing of an alert must be accompanied by special precautions, particularly at the time of its preliminary admissibility examination. In order to analyse the admissibility of the alert and to assess the accuracy of the allegations made, any additional information may also be requested from the whistleblower;

• **Good faith:** the whistleblower must act in good faith and without financial compensation. In this regard, the allegations in the alert must be presented objectively and factually. On the other hand, improper use of the system may expose the whistleblower to disciplinary procedures as well as legal proceedings;

• **Enhanced protection:** the whistleblower benefits from the guarantees associated with the status of a whistleblower against any form of retaliation or victimization, that being confidentiality of his/her identity; his/her alert; including in particular any third party mentioned (colleagues, close friends, etc.).

2 ALERT MANAGEMENT PROCESS

The alerts issued through the whistleblowing system are subject to an admissibility analysis and where applicable, an investigation into the materiality of the facts presented and the disciplinary measures against the perpetrators, in accordance with the applicable law, is conducted. The whistleblower is informed in writing of the receipt of the alert within 7 days of receipt of it.

2.1 Reporting an alert

The alleged infringement of the law, regulation or violation of the Group's Code of Conduct and Ethics (COCE), may be reported through the hierarchical route or via the appropriate Corporate Departments, alternatively, by means of CFAO group's whistleblowing system (Speak Up), accessible from the websites of CFAO group and its subsidiaries or from any internet browser under the link:

SPEAK UP

The whistleblowing system makes it possible to issue an alert, 24/7/365 days a year via an online form available in several languages or by phone.

The whistleblower is invited to complete a form, in good faith, identifying themselves and listing objectively and exhaustively, the alleged violations of which he/ she has become aware (dates, entity concerned, transaction details Etc.) as well as the identity of those persons involved. The alert should be accompanied by supporting evidence and documents (attached).

The whistleblower provides information or documents, regardless of their form or medium, to support their alert.

The alert is instantly communicated to the whistleblowing contact persons (hereinafter "contacts"), representatives of the Group, specially appointed to analyse its admissibility and carry out or coordinate the resulting investigation, where applicable.

2.2 Contacts authorised to receive and process alerts

When an alert is issued, one or more contacts are appointed to monitor the procedure.

The contacts are responsible for the smooth running of the procedure and communication with the whistleblower.

These contacts, specially trained to assess the admissibility of an alert, are limited in number, bound by an enhanced obligation of confidentiality and with the authority of competence and the resources necessary for the performance of this task:

• **Compliance Department** for acts of corruption, influence peddling, violation of economic sanctions programmes;

• **Human Resources Department** for acts of discrimination and moral or sexual harassment, damage to the health and safety of persons, human rights and fundamental freedoms involving an employee of CFAO group;

• **Legal Department:** anti-competitive practices.

Alerts that do not fall within any of the categories listed above ("other") will be sent to the **Compliance Department**.

Alerts are processed either at the level of the Division concerned or at Group level after a decision is made by the Compliance Department depending on the nature of the alert.

The contacts may appoint trusted persons to assist them. These persons are then bound by the same obligations.

The contacts inform the whistleblower of its receipt of the alert within 7 days and then provide feedback in accordance with the provisions of the law.

2.3 Admissibility analysis

In order to assess the admissibility of the alert, the contacts may request clarification through the whistleblowing system: if the whistleblower has identified himself/herself, he/she will receive an email notification inviting him/her to connect to the 'follow up' section; if he/she has opted for anonymity, the whistleblower must log in regularly to check for follow ups.

If it is certain that the alert is not admissible, the contact informs the whistleblower and closes the procedure.

Alerts filed anonymously are subject to special precautions regarding their processing: an alert will only be admissible if the supporting evidence is sufficiently detailed to establish the seriousness of the facts.

At the end of this analysis, the contacts conclude that the alert is admissible or inadmissible: if inadmissible, the procedure is closed and the data is immediately deleted; if admissible, the alert is the subject of an investigation to establish the materiality of the facts.

2.4 Investigation

The contacts shall initiate or coordinate the investigation aimed at establishing the materiality of the violations and characterising the liability of their alleged perpetrators ("accused persons").

This investigation may be carried out by the contacts or a third party (lawyers, experts, auditors) with appropriate guarantees for the protection of personal data.

As part of their investigation, authorised contacts or third parties are entitled to:

• **Collect** and process any data (accounting, banking, computer) that they deem relevant (excluding data prohibited from collection) concerning the company or the persons involved;

• **Conduct** adversarial interviews allowing the accused to respond to the accusations to which they are the subject;

• **Interview** any person to collect any information to verify the accuracy of the alleged facts.

CFAO is required to communicate to the whistleblower, in writing, and within a reasonable time not exceeding 3 months from the acknowledgment of receipt, or in the absence of acknowledgment of receipt, within three months from the expiration of a period of seven working days following the alert, information on the measures envisaged or taken to assess the accuracy of the allegations and, if necessary, the measures taken to remedy the subject of the alert and the reasons for it.

At the end of the investigation, the contacts present their findings and conclusions to the Compliance Committee of the Division or the Group depending on whether the alert is processed at the Division or Group level.

When the investigation is processed at the Division level, the Division Compliance Committee validates the follow-up to be given to the alert or convenes an extraordinary meeting of the Group Compliance Committee in charge of deciding.

When the alert is processed directly by the Group Compliance Department, the Group Human Resources Department or the Group Legal Department, the Group Compliance Committee validates the follow-up to be given to the alert.

2.5 Follow-up to the alert – Closing the file

Following the processing of alerts, the procedure is closed for one of the following reasons:

• **Inadmissibility:** if the analysis of the contacts makes it possible to establish that the alert does not meet the purpose of the system or the conditions of use (particularly in terms of anonymity) without the bad faith of the whistleblower being established, the procedure is closed without consequences;

• **Inaccuracy or inadequacy:** if the investigation carried out does not establish the materiality of the violations and the liability of their alleged perpetrators, without the bad faith of the whistleblower being established, the procedure is terminated without consequences;

• **Materiality of the facts:** if the investigation carried out makes it possible to establish the materiality of the violations and the liability of their alleged perpetrators, closure of the alert procedure with disciplinary action and/or legal proceedings against the person(s) involved;

• **Misuse of the system:** if the subsequent admissibility analysis or investigation demonstrates the bad faith of the whistleblower, the closure of the procedure with disciplinary action and/or legal proceedings against him/her;

The whistleblower and the accused persons are notified in writing of the closure of the procedure where applicable.

The use of the whistleblowing system and the measures taken to prevent or remedy the violations it has identified are on the agenda of ordinary or extraordinary meetings of the Division Compliance Committee (when the alert is handled by the Division concerned) or the Group Compliance Committee (when it is handled directly at Group level).

3 PROTECTION OF PERSONAL DATA

Information about individuals is collected and processed under this system in accordance with the applicable regulations on the protection of personal data.

In accordance with the same regulations, data subjects may, at any time, access their information and/or changes to the data in the event of an error.

However, the whistleblower, even if he/she has the right to access and modify his/her data, will not be able to obtain the identity of the whistleblower, unless the law provides otherwise.

The personal data collected under this system will be used by the data controller to meet legal obligations. The essential data from a regulatory point of view are reported at the time of collection.

Data is protected in compliance with local laws applicable to the processing of personal data.

- **Retention and deletion of data collected**

Situation	Retention period
Report found inadmissible	• Immediate deletion following closure
Alert classified for no further action after investigation (inaccurate or insufficient information)	• Until 2 months following closure, then deletion
Improper use of the system	• Retention until the end of the procedure and the expiry of legal remedies, followed by deletion
Proven facts that give rise to disciplinary or litigation proceedings	• Retention until the end of the procedure and the expiry of legal remedies, followed by deletion

Reference texts

French Labour Code	- Article L.1132-3-3 and L.1232-4
French Criminal Code	- Article 122-9
Other	- Law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (Sapin II law) - Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law - Law no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers - Decree No. 2022-1284 of October 3, 2022 relating to whistleblowers