



**REGULATIONS FOR  
MANAGING WHISTLEBLOWING REPORTS OF CIFA GROUP  
S.P.A.**

Approved by the CIFA S.p.A. Board of Directors on 30 November 2023

**CONTENTS**

**1.    PREMESSA..... 3**

**2.    DEFINIZIONI ..... 5**

**3.    DESTINATARI ..... 6**

**4.    PRINCIPI GENERALI..... 6**

**5.    MODALITÀ DI SEGNALAZIONE E ATTIVITÀ D’INDAGINE..... 8**

**5.1.    I SOGGETTI SEGNALANTI ..... 8**

**5.2.    OGGETTO DELLE SEGNALAZIONI..... 9**

**5.3.    I CANALI INTERNI DI SEGNALAZIONE ..... 11**

**5.4.    AZIONI, FATTI E CONDOTTE CHE NON POSSONO ESSERE SEGNALATE ..... 12**

**6.    GESTIONE DELLE SEGNALAZIONI RICEVUTE ..... 12**

**7.    TRATTAMENTO DEI DATI PERSONALI DEL SEGNALANTE ..... 14**

**8.    TRACCIABILITÀ E ARCHIVIAZIONE..... 15**

**9.    TEMPISTICHE DI IMPLEMENTAZIONE ..... 16**

## 1. INTRODUCTION

### The aim of the breach reporting system

Cifa S.p.A. Group, in compliance with “Provisions for the protection of persons who report offences or irregularities they come into the knowledge of in their capacity as public or private employees” (Italian Law 179/2017), has adopted a breach reporting system (hereinafter also “*whistleblowing*”), defining the procedures for reporting unlawful conduct, both commissive and omissive in nature, which constitute or potentially constitute a breach and give rise to the breach of laws, rules, values and principles set forth in the Organisation, Management and Control Model and the Ethical Code of Cifa S.p.A., as well as in the policies, procedures and regulations adopted by each company of Cifa S.p.A. Group.

Italian Legislative Decree no. 24 of 10 March 2023 regarding “*The implementation of (EU) directive 2019/1937 of the European Parliament and Council, of 23 October 2019, regarding the protection of persons who report breaches of European Union law and containing provisions regarding the protection of persons who report breaches of provisions set forth in national legislation*”, introduced new whistleblowing provisions, specifically:

- The obligation to activate **reporting channels that guarantee**, also by means of the use of encryption instruments, the confidentiality of the reporting person's identity as well as that of the person involved and the person mentioned in the report in any way, as well as of the report's contents and relative documentation;
- the need to entrust management of the **internal reporting channel** to a **person** or **autonomous internal office specifically assigned for this purpose** and staffed by professionals specifically trained to manage the reporting channel;
- specific **methods for preparing reports**:
  - in writing, also by computerised means;
  - orally, over the phone or by means of voice messaging systems; or
  - upon the reporting person's request, at a direct meeting scheduled within a reasonable date;
- specific obligations with reference to **report management methods**:
  - Diligently follow-up received reports;
  - notify the reporting person of report reception within seven days from reception;
  - correspond with the reporting person, also for the purposes of receiving additional information and/ or supplementation of the contents of the submitted report, and
  - inform the reporting person of report closure within three months from the sending date of the relative notice of reception;
- the obligation to provide all concerned parties with **clear information** on the channel, procedures and precepts for submitting reports. This information must be posted and made

easily visible in workplaces and accessible to persons who provide their services for the Company without necessarily accessing work places;

- activation of an external channel for reporting breaches by ANAC (Italian National Anti-Corruption Authority). A report can only be submitted to ANAC, **regarding breaches of European Union provisions** under one of the following conditions:
  - the mandatory opening of an internal reporting channel does not apply at the work place, or is not active despite being mandatory, or is available but not compliant with statutory provisions;
  - the reporting person has already submitted an internal report, which was not followed up;
  - the reporting person has reasonable grounds to believe that if they were to submit an internal report, it would not be effectively followed up and may result in the risk of retaliation;
  - the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to public interest.

With the reform introduced by Italian Legislative Decree 24/2023, A.N.A.C has been assigned the power/ duty to adopt guidelines regarding procedures for submitting and managing external reports.<sup>1</sup> Reports can be submitted at the following link: <https://www.anticorruzione.it/-/whistleblowing>;

- the opportunity for **public disclosure**. Public disclosure means making information on breaches public through the press or by electronic means, or using any means of disclosure that reaches out to a large number of people.

The whistleblower can **only publicly disclose breaches of European Union provisions** when:

- The Whistleblower has previously submitted an internal and external report, or has directly submitted an external report and failed to receive a response within the established time limits laid down for measures that are necessary or adopted in order to follow up reports;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the whistleblower has reasonable grounds to believe the external report may result in the risk of retaliation or may not be effectively followed up, due to specific circumstances of the case at hand, such as when evidence may be hidden or destroyed, or when there are reasonable grounds to fear that those who receive the report may be in collusion with the perpetrator of the breach, or involved in said breach;
- the opportunity to **report to Jurisdictional Authorities**. The use of the internal or external channel for reporting does not compromise the possibility of addressing the competent Judicial Authorities;
- ANAC (Italian National Anti-Corruption Authority) is responsible for issuing sanctions and may apply the following administrative and pecuniary measures:
  - from 10,000 to 50,000 Euros incurred by the company in the following cases:

---

<sup>1</sup> These Guidelines were adopted and published by ANAC with resolution no. 311 of 12 July 2023.

- failure to establish reporting channels;
- failure to adopt procedures for submitting and managing reports;
- non conformities in procedures adopted as per the provisions set forth in Italian Legislative Decree 24/2023;
- failure to conduct verification and analysis activities with reference to received reports;
- committing acts of retaliation;
- preventing or attempting to prevent the submission of a report;
- breach of confidentiality obligations;
- from 500 to 2,500 Euros incurred by the Whistleblower when they submit a report with malice or gross negligence, unless they are convicted for the crimes of slander or defamation, including in a first instance judgement.

## 2. DEFINITIONS

- Ethical Committee or report manager: the internal supervisory body that sits as a united bench of Cifa S.p.A., appointed by the Board of Directors. It has the right to receive, analyse and verify reports. The Ethical Committee consists of the Corporate & Legal Counsel and Human resources & General Services Director functions.
- **Italian Legislative Decree no. 231 of 2001 or Italian Legislative Decree 231/2001:** Italian Legislative Decree no. 231 of 08 June 2001 incorporating “Regulations on the administrative responsibility of legal entities, companies and associations even without legal personality, in accordance with Article 11 of Italian Law no. 300 of 29 September 2000” as subsequently amended and supplemented. For further details on offences covered in Italian Legislative Decree 231/2011 go to the link: <https://www.reatipresupposto231.it/>
- **Cifa S.p.A. Group or the Group:** consists of Cifa S.p.A., Zoomlion Italia S.r.l. and Valme S.r.l..
- **Organisation, Management and Control Model pursuant to Italian Legislative Decree 231/2001 or the Model:** Model and Ethical Code of Cifa S.p.A. approved by the Board of Directors of Cifa S.p.A..
- **Supervisory Board or SB:** the internal supervisory body of Cifa S.p.A. that sits as a united bench (hereinafter also the "Company" or "Cifa"), appointed by the Board of Directors.
- **Staff or Employee:** all employees of any Group companies.
- **Reported Person or entity** anyone reported by the Whistleblower as having committed or being suspected of committing an offence.
- **Whistleblower:** the person who witnesses an offence or irregularity at the work place and decides to report it. Can be anyone performing a specific duty or function at or for the Company (e.g. employees, executives, directors and members of corporate bodies, third parties including non-

employed professionals, consultants, intermediaries, agents providers of products and services, customers).

- **Report:** Notice from the Whistleblower regarding the reasonable and legitimate suspicion or awareness of breaches committed by employees or representatives of the company, which may directly or indirectly give rise to damage to the finances, equity or image of the Group.
- **Reported Person or entity** anyone reported by the Whistleblower as having committed or being suspected of committing an offence.
- **Breach:** any action that goes against: (i) legislation and regulations, including those of the European Union; (ii) the Group's regulations and procedures; (iii) principles, regulations and activities set forth in the Organisation, Management and Control Model and the Ethical Code pursuant to Italian Legislative Decree 231/2001 adopted by Cifa S.p.A..

### 3. RECIPIENTS

The recipients of these Regulations are:

- Top management and members of Group company corporate bodies;
- all employees of Group companies, partners, customers, suppliers, consultants, non-employed professionals, shareholders and in general anyone in a relationship of interest with Group companies (so-called "Third Parties").

### 4. GENERAL PRINCIPLES

**Through the whistleblowing instrument, the protection of those who report situations of non-conformity in good faith**, for the purpose of preventing the occurrence of irregularities in the organisation and involving all stakeholders and the general public, in an activity that counteracts illegality through active and responsible participation.

In compliance with legislation in force, the Group has adopted a series of general principles in order to guide and regulate methods for investigating possible cases of breaches. Specifically, the following principles apply:

- **zero tolerance:** the Group's companies do not tolerate any unlawful conduct that breaches the Model, Ethical Code and any regulations, company procedures, principles and regulations adopted by companies of the Group. The Group aims to ensure the spread of a company culture in which whistleblowers can feel comfortable with submitting reports of any offences, without fear of incurring any direct or indirect acts of retaliation due to a report; therefore, any acts in breach of the prohibition of retaliation are to be considered null and void;
- **full clarification:** any potentially fraudulent activities or those potentially in breach of company regulations must be promptly and accurately investigated and desist immediately;
- **compliance with regulatory and legislative provisions:** national legislation and regulatory provisions must be complied with;

- **protection of the whistleblower:** the Company's Model, Ethical Code, regulations, procedures, as well as the principles and regulations adopted by the group's companies and these Regulations explicitly encourage and protect all staff who in good faith report potentially fraudulent activities or suspicious circumstances and provide information on or evidence of any fraudulent activities or suspicious circumstances, must not fear negative consequences. Protection of the reporting person is applied, formalised and also extends to situations in which the report is submitted when the **legal relationship is yet to enter into force, during the trial period or following the termination of the legal relationship**. Whistleblowing protection measures also extend to the following persons:

- facilitators (persons who assist the whistleblower in the reporting process);
- persons who work with the whistleblower and is in a stable relationship with or related to them;
- colleagues of the whistleblower with whom they have a habitual and ongoing relationship;
- entities owned by the whistleblower exclusively or by means of their being part of a majority shareholding with third parties, which whistleblow or execute public disclosure;
- entities where the whistleblower who submits a report or executes public disclosure, works.

**Italian Legislative Decree no. 24 of 10 March 2023 recognises an additional form of protection: limitation of the whistleblower's responsibility with respect to the disclosure and dissemination of certain categories of information**, which would otherwise subject them to penal, civil and administrative liability.

In particular, the whistleblower will not be called to respond in penal, civil or administrative proceedings for:

- disclosure and use of professional secrecy (art. 326 Italian Penal Code);
- disclosure of professional secrecy (art. 622 Italian Penal Code);
- disclosure of scientific and industrial secrets (art. 623 Italian Penal Code);
- breach of the duty of faithfulness and loyalty (art. 2105 Italian Civil Code);
- breach of copyright protection provisions;
- breach of personal data protection provisions;
- disclosure or dissemination of information on breaches that undermines the reputation of the person involved.

Italian Legislative Decree 10 March 2023 no. 24 establishes two conditions for the exercise of the above-mentioned limitations of responsibility:

- ✓ upon disclosure or dissemination there are reasonable grounds to believe that information is necessary in order to disclose the breach at hand in the report;
- ✓ the report is submitted in compliance with conditions set forth in the Decree for benefiting from protection against retaliation (reasonable grounds for believing reported facts are true, the breach is reportable, and the methods and conditions for accessing the report are complied with).

Therefore it should be highlighted that the limitation applies if the reasons for the disclosure or dissemination are not based on mere speculation, gossip, vindictive, opportunistic or scandal-inciting purposes.

In any case it must be considered that responsibility is not excluded for conduct that:

- is not connected to the report;
- is not strictly necessary for disclosing the breach;
- enables the illicit acquisition of information or access to documents.

Whenever the acquisition constitutes an offence, for example in the case of unlawful access to an IT system, or an act of software piracy, penal liability prevails, as does all other civil, administrative and disciplinary liability of the reporting person.

Vice versa, extraction (by means of copy, photography, removal) of lawfully accessible documents will not be punishable.

- **protection of the reported person:** reports of a purely discriminatory nature regarding the reported person are not permitted, including news of a defamatory nature, or any information provided in bad faith with the sole purpose of causing damage to the reported person;
- **protection of report confidentiality:** information must be processed by all parties involved with the utmost confidentiality, concerning both the whistleblower and the reported person. The Group has activated its own reporting channels, which ensure the confidentiality of the person involved or in any case mentioned in the report, as well as of report content and relative documentation. Such information/ documentation must remain confidential at all times and may only be disclosed:
  - to persons responsible for managing reports and persons involved in managing any disciplinary procedures linked to received reports;
  - to any additional persons internal or external to the Group, exclusively for report managing purposes, when the data subject's prior consent is obtained;
  - persons legally authorised to access such confidential information.

For the purpose of incentivising the use of reporting systems and encouraging the spread of a culture of legality, the Group clearly, precisely and comprehensively illustrates the adopted reporting procedure, ensuring the confidentiality of the whistleblower's personal data and of the presumed perpetrator of the offence, **in this document and by means of an information campaign** (for its employees) **and the provision of information** (externally for example by publication on the Group company's institutional website).

## 5. REPORTING METHODS AND INVESTIGATION ACTIVITIES

### 5.1. Reporting persons

All Recipients of this document have a duty to communicate any suspected fraud, irregularity and commission of offences through the reporting channels adopted by the Group in a specific report for (which is defined as "*Whistleblowing*").



Above-mentioned persons are not requested to ascertain the infringement, however they are required to promptly report it, even if only suspected. Therefore they are requested to refrain from undertaking personal investigations or appointing coworkers to perform preliminary investigations.

**In line with legislation in force and *best practices*, reporting persons may be in top management or employees, or third parties who witness illicit or irregular conduct, i.e.**

- employees with a fixed-term or permanent contract, including interns, trainees, apprentices, non-employed professionals and temps;
- former employees (if events occurred during their period of employment);
- potential candidates for hire;
- shareholders (natural persons);
- members of the Board of Directors;
- goods and service providers, including their employees;
- consultants and freelancers, including their employees, who provide their services for the Company;
- customers, including their employees.

## **5.2. Subject of reports**

Reports may be made on the subject of conduct regarding:

### **BREACHES OF NATIONAL LEGISLATIVE PROVISIONS**

- **administrative, accounting, civil or penal breaches, other than those specifically identified as breaches of EU law**, as defined in the following paragraph.
- **Illicit conduct pursuant to Italian Legislative Decree 231/2001;**
- **Breaches of the Organisation Management And Control Model** pursuant to Italian Legislative Decree 231/2001;

### **BREACHES OF EU LEGISLATION**

- **offences which breach European Union legislation indicated in Annex 1 of Italian legislative Decree no. 24 of 10 March 2023 and all national implementing provisions** (including those not explicitly cited in said Annex). In particular, breaches pertaining to the following main sectors: public tenders; services, products, financial markets and the prevention of laundering and financing of terrorism; safety and production conformity; environmental protection;
- **other acts or omissions that harm the financial interests of the European Union** (art. 325 of the Treaty on the Functioning of the European Union against fraud) as identified in regulations,

directives, decisions, recommendations and opinions of the EU (e.g. fraud, corruption and any other illegal activities connected to EU expenses);

- **acts or omissions regarding the internal market and which undermine the free circulation of goods, persons, services and capital** (art. 26, paragraph 2 of the Treaty on the Functioning of the European Union). Breaches of EU legislation on competition and State aid, corporate taxation legislation and mechanisms with the purpose of obtaining a fiscal advantage that undermine the subject or purpose of applicable corporate tax legislation are included;
- **acts or conduct that undermine the subject or purpose of European Union provisions in sectors indicated in previous points** (e.g. a company operating on the market in a dominant position, which compromises actual and fair competition on the internal market due to its conduct, by resorting to so-called abusive practices, such as the adoption of predatory pricing, target discounts, tying agreements, etc.), thus failing to safeguard free competition.

**Illicit conduct (or suspected illicit conduct), in breach of the Ethical Code, Policies and Procedures adopted by the Group's companies,** may also be reported.

**Such breaches must be capable of causing damage to or undermining the Group's company or even only its image.**

**In contrast, the following should not be reported: issues of a personal nature concerning the whistleblower, claims or motions pertaining to the employment contract or relations with hierarchical superiors or colleagues.**

In particular, **the following should not be reported: issues of a personal nature concerning the whistleblower, claims or motions pertaining to the employment contract or relations with hierarchical superiors or colleagues.** In particular, **the following kinds of reports are excluded from the remit of new regulations:**

- ✓ **those linked to the whistleblower's personal interest, pertaining to individual work relationships, i.e. regarding work relationships with superior figures** (e.g. labour disputes, discriminations, interpersonal conflicts between colleagues, reports on data processing in the context of the individual work contract without harm to public interest or the integrity of the private entity or public administration), insofar as new legislation aims to safeguard the integrity of the entity-legal person and includes *“all situations in which the subject or purposes of activities undertaken in the public and private sector for the full achievement of public purposes, which undermine purposes or correct action”*.

Complaints recognised as being connected to the whistleblower's personal interest are not to be considered whistleblowing reports and can therefore be handled as ordinary reports, if provided for (e.g. conduct undermining principles or prescriptions contained in the Ethical Code, for example, or in staff regulations, and thus should be addressed to the Human Resources function).

- ✓ regarding **national security and defence;**
- ✓ regarding **breaches already subject to compulsory regulation in certain special sectors,** to which

specific reporting regulations already apply (e.g. financial services, laundering prevention, terrorism, transport safety, environmental protection<sup>2</sup>).

Regulations prevail regarding the following: i) classified information; ii) medical and professional secrecy; iii) secrecy of court deliberations; iv) penal procedure obligations regarding the obligation of secrecy in investigations; v) magistrature autonomy and independence provisions; vi) national defence and public order and security; vii) exercise of the right by workers to consult their representatives or trade unions.

**The following information must be provided in the report:**

- **whistleblower's identification data** (e.g. type of employment or professional contract in force with the Group); Identity and email address are to be considered optional for the purpose of reports submitted on the platform or in hard copy;
- **subject of the report** and detailed description thereof;
- **any documentation** proving the reported matters.

Any reports from which it is not possible to identify the whistleblower's identity are considered anonymous. Anonymous reporting is **permitted despite not being recommended**, insofar as it limits the possibility of corresponding with the whistleblower and adequately verifying the truthfulness of facts.

In any case anonymous reports that are detailed and which enable the emergence of facts and situations linking them to specific contexts **are identified as "ordinary" reports**.

It should be noted that confidentiality of the whistleblower's data is always guaranteed, as is their protection from any form of retaliation or discrimination.

### **5.3. Internal reporting channels**

In compliance with provisions set forth in applicable legislation (pursuant to art. 6, par. 2-b of Italian legislative Decree no. 231/01 and pursuant to art. 4 of Italian Legislative Decree no. 24/2023), **the whistleblower can submit their report using the following reporting channels:**

- **ordinary or registered mail<sup>3</sup>**, to the offices in Via Stati Uniti d'America 26 - 20030 Senago (MI), to the confidential attention of the Ethical Committee of Cifa S.p.A.;

---

<sup>2</sup> E.g. as per ANAC (Italian National Anti-Corruption Authority) Guidelines, see: articles 52-bis and 52-ter of the Consolidated Banking Act, containing provisions on the reporting of breaches in the banking sector; articles 4 point eleven "Internal systems for the reporting of breaches" and 4 point twelve "Procedures for reporting to Supervisory Authorities" introduced in the Consolidating Act on financial intermediation, which introduce detailed provisions on the protection of whistleblowers in this sector too.

<sup>3</sup> ANAC (Italian National Anti-Corruption Authority) guidelines indicate reports should be placed inside two sealed envelopes, the first containing the whistleblower's identification data and an identity document; the second containing the subject of the report; both envelopes should then be placed inside a third envelope bearing the following sentence externally "reserved for the Ethical Committee of Cifa S.p.A.".

- **By computerised means**, using the specific platform, accessible from each of the official websites of the Group's companies, under the "Whistleblowing" section, leading to the following links: [cifa.integrityline.com](http://cifa.integrityline.com) (for Cifa S.p.A.), [valme.integrityline.com](http://valme.integrityline.com) (for Valme S.r.l.) and [zoomlionitalia.integrityline.com](http://zoomlionitalia.integrityline.com) (for Zoomlion Italia S.r.l.).
- **orally**, through the voice messaging system provided on the IT platform and upon the Whistleblower's request, submitted using one of the above-mentioned channels - in a direct meeting with the Company's Ethical Committee.

#### **5.4. Actions, facts and conduct that cannot be reported**

**Whistleblowing must not be used as an instrument for offending or damaging the honour and/or personal and/ or professional decorum of the person or persons to which reported facts refer, or for deliberately spreading unfounded allegations.**

Therefore specifically, by way of example but not of limitation, the following is **forbidden**:

- use of **libellous expressions**;
- the sending of **reports for purely libellous or defamatory purposes**;
- the sending of **reports that are discriminatory in nature**, insofar as they refer to sexual, religious and political orientations or the racial or ethnic origin of the reported person;
- the sending of **reports with the sole intent of harming the reported person**.

**Reports devoid of any substantial supporting elements, which are excessively vague, insufficiently detailed, or with evident defamatory or libellous contents, will not be taken into consideration. Fines will be issued for any unfounded reports.** Specifically, in the case of reports in which the reporter's bad faith and/or merely defamatory intent is ascertained, or also confirmed due to the unfoundedness of the report, the Ethical Committee reserves the right to request the directors, general managers of Group companies, in cooperation with the specific HR Management of Group companies involved, to undertake disciplinary actions against the Whistleblower in case of breach of Regulations.

Therefore the whistleblower shall be held liable and subject to disciplinary action if the report is found to be defamatory and libellous and if reports are submitted with malice, gross negligence or untruthful content.

**Pursuant to art. 21, par. 1 lett. c) of Italian Legislative Decree 24/2023, ANAC (Italian National Anti-Corruption Authority) may issue the reporter with a fine of 500 to 2,500 Euros if their civil liability is confirmed due to malice or gross negligence, for the offences of libel and slander.**

## **6. THE MANAGEMENT OF RECEIVED REPORTS**

**The Group's companies have entrusted the Ethical Committee with the management of reports thus with the duty of:**

- ensuring the correct execution of the report management process and continuous monitoring thereof;
- undertaking **investigation activities** following the reception of reports;
- **forwarding the report to the Supervisory Board if the subject of the report is within the remit of Italian Legislative Decree 231/2011.** Upon receiving the report, the Supervisory Board will report to the Board of Directors in accordance with procedures set forth in the Model, regarding relative activities for managing the received report;
- **ensuring the confidentiality of information contained in the report and safeguarding the identity of whistleblowers**, acting to ensure they do not suffer any form of retaliation or discriminatory conduct, direct or indirect in nature, for reasons directly or indirectly linked to reports.

Specifically, after receiving a report through designated channels, the Ethical Committee will send notice of reception of the report to the whistleblower **within 7 days** starting from report reception date, in order to:

- confirm reception of the report;
- notify the whistleblower that the report will be examined in the utmost confidentiality;
- inform the whistleblower that:
  - the group adopts a zero tolerance policy against retaliation;
  - any retaliation can be reported in order to benefit from protection measures provided by the law<sup>4</sup>.

In the pursuit of its investigative activities, the Ethical Committee may request meetings with Functions involved in the report, in order to verify the veracity of what has been reported and if required, with the assistance of the Supervisory Board.

The Ethical Committee analyses and assesses received reports and if necessary, summons the whistleblower to obtain further information, in order to undertake all necessary inspections and investigations to confirm the report's truthfulness.

For a report to be "admissible", it must be:

- 1) prepared by persons specified in these Regulations in paragraph 5.1.;
- 2) sufficiently **precise, clear, detailed** and include suitable supporting evidence for the purpose of ascertaining the facts (e.g. letters, emails, text messages, etc.);
- 3) based on concrete proof that can be verified and confirmed (and not on vague suspicions or gossip); and
- 4) refer to one of the categories of offences specified in paragraph 5.2.

---

<sup>4</sup> Any person who believes they have been subjected to retaliation, including attempts or threats, as a consequence of a report/ disclosure/ complaint, must inform ANAC (Italian National Anti-Corruption Authority), which will ascertain the causal nexus between the retaliation and the report and duly adopt consequent provisions.

All information, documentation and reports collected by the Ethical Committee, duly received in the pursuit of its institutional duties, are processed in compliance with regulatory personal data processing provisions.

If the report is confirmed as founded, the Ethical Committee may propose:

- disciplinary and/or legal actions against the reported person and any other persons involved (if deemed appropriate in relation to the seriousness of the identified offence and applicable legislation); and
- an action plan for resolving any shortcomings and/or anomalies reported by investigators, requiring the implementation of corrective measures.

The whistleblower is informed of report closure by the Ethical Committee in writing within 90 days from the sending of report reception confirmation.

The information statement to be provided to the whistleblower upon report closure is different, based on whether the report (i) is not admissible or (ii) admissible.

(i) If the report is assessed as **not admissible**, the Ethical Committee informs the whistleblower of:

- the reasons why the report was found to be not admissible; and
- any Management offices or company persons the Whistleblower can refer to in order to discuss the facts at hand in the report, to ensure relative resolution thereof, whenever necessary.

(ii) If the report is assessed as admissible, the Ethical Committee illustrates the following to the whistleblower:

- actions undertaken following the report;
- measures adopted to verify the truthfulness of facts at hand in the report; and
- defined corrective actions.

Should any **conflict of interest arise**, i.e. any situation in which the manager of the report is also the whistleblower, the reported person or in any case a person involved or implicated in the report, the report can be addressed to the Top Management of the implicated Group Company or to another person/ office (e.g. Chairman of the Cifa S.p.A. Supervisory Board), which can guarantee effective, independent and autonomous management in compliance with the statutory confidentiality obligation.

## 7. WHISTLEBLOWER'S PERSONAL DATA PROCESSING

The Group ensures:

- **the protection of information regarding any person and which can be used to directly or indirectly identify said persons ("Personal Data");** and
- data security.

**Personal data are managed in compliance with data protection procedures adopted by the group and in compliance with applicable regulations and legislation, with particular reference to the European Union General Data Protection Regulation ("GDPR").**

This implies that:

- any person capable of using the Whistleblowing system is informed of the method used to process their personal data. The privacy information statement for the Whistleblowing portal regulates rights to access, rectify and erase personal data;
- personal data management is limited to use strictly necessary for the purposes of managing reports and conducting internal investigations in order to verify the truthfulness and seriousness thereof;
- any third party whose personal data are processed as part of checks run with reference to a report must be promptly informed of the applied processing method, in compliance with applicable legislation and regulations;
- Reports and relative documentation are conserved for the length of time necessary for report processing and in any case no longer than five years from the date of disclosure of the final outcome of the reporting procedure.

If information regarding a report must be disclosed to third parties, the Ethical Committee verifies that said disclosure:

- is agreed to in advance with the whistleblower if it entails the disclosure of their identity or of personal data contained in the report;
- is carried out for the sole purpose of managing the report;
- does not result in the disclosure of confidential information that enables the identification of reported persons before the report is confirmed as truthful (unless requested by judicial authorities).

Whenever possible, whistleblowers, reported persons and in general any person involved in a report are informed of the methods applied for personal data processing. Said persons have the right to access, rectify, object to and whenever possible, erase their personal data.

To this effect, Annex 1, enclosed with this document, contains the WHISTLEBLOWING PRIVACY INFORMATION STATEMENT, pursuant to art. 13 of (EU) Regulation 679/2016 regarding personal data processing for the purposes of reporting breaches specified in Italian Legislative Decree 24/23.

## **8. TRACEABILITY AND STORAGE**

**The Ethical Committee is required to document reports received through designated channels, in order to ensure full traceability of actions undertaken in the fulfilment of its institutional functions.**

These regulations, prepared in compliance with requirements indicated by laws and regulations in force and the values contained in the Ethical Code, are an integral part of the Organisation, Management and Control Model pursuant to Italian Legislative Decree 231/2001 adopted by Cifa S.p.A..

## **9. IMPLEMENTATION TIME FRAME**

**In order to ensure correct implementation, these Regulations have been translated into English, made available and disclosed to all employees of all the Group's companies. A copy of Regulations has been filed in the CIFA Employees Human Resources Portal of the Group and published on the company website at the following link <https://www.cifa.com/it/documentazione>.**



## ANNEX 1

### **PRIVACY INFORMATION STATEMENT -WHISTLEBLOWING** **pursuant to art. 13 of (EU) Regulation 679/2016 regarding personal data processing for the purposes of reporting** **breaches specified in Italian Legislative Decree 24/23**

Dear colleagues,

Pursuant to article 13 of (EU) Regulation 2016/679 (*General Data Protection Regulation*, hereinafter "GDPR") and applicable personal data protection legislation, we inform you that personal data processed by our Company as part of the management of reports of breaches of national and European Union legislative provisions and which harm public interest or the private entity's interests, received through special internal reporting channels provided by the Company pursuant to Italian Legislative Decree 24/2023, will be processed in compliance with above-mentioned regulations and legislation and according to the principles of propriety, lawfulness and transparency, by persons authorised by the Company pursuant to article 29 of the GDPR and article 2 *point fourteen* of the Personal Data protection Code (Italian Legislative Decree 196/2003).

#### **1. Data Controller**

The Personal Data Controller is Cifa S.p.A (hereinafter also the "Company" or "Controller") with registered office in via Stati Uniti d'America n. 26 – 20030 Senago (MI).

#### **2. Purposes of processing and legal basis**

Personal data are processed to manage internal reports of presumed breaches or conduct, acts or omissions that harm public interest or the integrity of the private entity, defined in art. 2 par. 1 lett. a) of Italian Legislative Decree 24/23, which Reporting Persons come into the knowledge of in their capacity as employees of the Controller.

Processed personal data are those contained in the internal report and/ or in enclosed deeds and documents, and may refer to the Reporting Person or involved Persons, indicated as potentially responsible for unlawful conduct, and to those who are involved in the report in any way.

Personal data may also be processed during necessary investigative activities conducted to verify the truthfulness of what has been reported and, if applicable, for the adoption of adequate corrective measures and the issuing of suitable disciplinary and/ or judicial actions to perpetrators of breaches. The legal basis of personal data processing is the fulfilment of a legal obligation to which the Controller is subjected (Art. 6 par. 1, lett. c) of the GDPR), specifically set forth in Italian Legislative Decree. 231/2001, Law 179/2017 and Italian Legislative Decree 24/2023; processing may also involve special data and data on penal convictions and offences included in reports, in compliance with provisions set forth in articles 9 and 10 of the GDPR.

#### **3. Categories of data recipients**

Provided personal data will be processed by Whistleblowing Committee members in their capacity as persons authorised by the Controller to process data for the purposes of responding to and following up received reports, in compliance with provisions set forth in Italian legislative Decree 24/2023.

If the Company assigns a third party the task of managing the reporting channel, above-mentioned personal data will be processed by these persons in their capacity as Data Protection Officers, appointed by the Controller pursuant to art. 28 of the GDPR. Said data will be only be processed by explicitly authorised staff and in compliance with provisions set forth in Italian Legislative Decree no. 24/2023.

Personal data will not be subject to disclosure but may be transmitted to Judicial Authorities if required. No collected data will be transferred to Third Countries, meaning Countries that are not members of the European Economic Space (EES). In the case of an external report presented, as provided for in articles 6 and 7 of Italian Legislative Decree 24/2023, to ANAC (Italian National Anti-Corruption Authority), information on personal data processing will be provided by said authority using channels specifically designated for this purpose.

#### **4. Criteria on conservation periods**

Internal reports and relative documentation will be conserved for the length of time necessary for report processing and in any case no longer than five years from the data of disclosure of the final outcome of the reporting procedure, in compliance with confidentiality obligations as set forth in article 12 of Italian Legislative Decree 24/2023 and the principle as per article 5, paragraph 1, letter e), of the GDPR and 3, paragraph 1, letter e), of Italian Legislative Decree no. 51 of 2018. On expiry of the maximum five-year period, information referring to the report may be conserved by the Company for the purpose of ensuring and preserving its right to defence and provide proof of the correct managing of received reports, whenever requested. To this effect, personal data referring to the Reporting Person and involved Persons, indicated as possibly responsible for unlawful conduct, and those involved in any way in the report, will be anonymised.

#### **5. Data processing methods**

Personal data will be processed by persons who are explicitly authorised, with methods that ensure the confidentiality of the Reporting Person's identity as well as of the content of internal reports and relative documentation, with the adoption of adequate technical and organisation methods for protection from unauthorised or illicit access, destruction, loss of integrity and confidentiality, including accidental in nature. In order to ensure the confidentiality of the Reporting Person's identity for the entire duration of the internal report's management, their identity shall only be disclosed to persons explicitly authorised to manage reports. Except for cases in which liability for libel and slander are ascertained pursuant

to provisions of the penal code or art. 2043 of the Civil Code, or, wherever applicable, during penal proceedings and within the processes and limits as set forth in art. 329 of the Penal Procedure Code, the Reporting Person's identity is protected in any context subsequent to the report. Therefore, without prejudice to cited exceptions, the Reporting Person's identity cannot be disclosed without their explicit consent, and all those who receive or are involved in managing the report are required to safeguard the confidentiality of this information.

#### **6. Conveyance of data**

The conveyance of the Reporting person's personal data is optional. However, failure to provide data may undermine investigation of the report: anonymous reports will only be taken into consideration if there are adequate circumstances and details to ensure the emergence of facts and situations connected to specific contexts.

#### **7. Rights of the data subject**

The rights set forth in articles 15-22 of the GDPR can be exercised, within the limits specified in art. 2-point eleven, par. 3, of Italian Legislative Decree no. 196/2003, by contacting the Controller using the contact details provided here above. Specifically, the above-mentioned rights cannot be requested by submitting a request to the Controller, or as a complaint pursuant to article 77 of the GDPR to the Personal Data Protection Authority, when the exercise of such rights may effectively and concretely undermine the confidentiality of the identity of the person reporting breaches they have come into the knowledge of due to their work contract or any executed functions. The exercise of the above-mentioned rights can in any case be delayed, limited or excluded with a notification motivated and promptly provided by the Controller, unless notification undermines the purpose of the limitation, due to the time and within the limits that it constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the Reporting Person, the Person or persons involved for various reasons in reports. In such cases, pursuant to art. 2-point eleven, par. 3, of Italian Legislative Decree no. 196/2003 the data subject has the right to exercise the rights cited here above through the Personal Data Protection Authority, in accordance with procedures as per art. 160 of the above-mentioned Legislative Decree. In cases in which it is believed personal data are processed in breach of the provisions of the GDPR, a complaint can be lodged to the Personal Data Protection Authority, as provided for in art. 77 of the GDPR (except for above-mentioned exclusion of limits to the exercise of rights as provided for in art. 2 point eleven, par. 3, of Italian Legislative Decree no. 196/2003), or to undertake suitable legal action (art. 79 of the GDPR).