IAF NETWORK SPA

REA Number: BS-448778
VAT Number: 02424060982
Registered office:
Via Flero 46 (Torre Sud) - 25125 Brescia - Italy

***

WHISTLEBLOWING PROCEDURE

***

This document constitutes an integral part of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 and adopted by **IAF NETWORK S.P.A.** (hereinafter the “Entity”).

1) REGULATORY REFERENCE AND NATURE OF THE WHISTLEBLOWING SYSTEM

Article 1, paragraph 51, of Law 190/2012 (the so-called anti-corruption law) had introduced the new article 54 bis into Legislative Decree 165/2001, entitled '*Protection of public employees who report wrongdoing*', by virtue of which a measure was introduced into our legal system aimed at facilitating the emergence of cases of wrongdoing, known in Anglo-Saxon countries as *whistleblowing. The* expression *whistleblower refers to an* employee of an organisation who reports to the bodies empowered to intervene specific violations or irregularities committed to the detriment of the public interest. Reporting, from this perspective, is an act of manifestation of civic sense, through which the *whistleblower* contributes to bringing out and preventing risks and situations detrimental to the entity to which the whistleblower belongs and consequently to the collective public interest. Law 179/2017, entitled "*Provisions for the protection of whistleblowers who report offences or irregularities of which they have become aware in the context of a public or private employment relationship*", which came into force on 29 December 2017, had amended the aforementioned Article 54 bis of Legislative Decree 165/2001, as well as Article 6 of Legislative Decree 231/2001.

More recently, this institution has been regulated by Legislative Decree 24/2023 in **force as of 30.03.2023** *implementing EU Directive 2019/1937 on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws*, which, inter alia, repealed Article 54-bis Legislative Decree 165/2001, Article 6, paragraphs 2-ter and 2-quater, Legislative Decree 231/2001, as well as Article 3 of Law 179/2017. Legislative Decree 24/2023 repeals the previous national regulations on whistleblowing and encapsulates in a single regulatory text - for both public and private sector - the **protection** regime for **individuals who report unlawful conduct of which they have become aware in a work context**.

2) PURPOSE AND AIM OF THE PROCEDURE

The current rules aim at encouraging the reporting of offences that undermine the public interest or the integrity of the entity and, at the same time, at strengthening the protection for whistleblowers, with a view to guaranteeing the whistleblower's freedom of expression and reinforcing legality and transparency within entities in order to prevent offences. This dual purpose gives rise to **protection rights for the whistleblower** (confidentiality, anonymity, prohibition of retaliatory acts) and specific **organisational obligations for the entities** (establishment of internal and external reporting channels, as well as procedures to ensure confidentiality rights).

The purpose of this document, therefore, is to remove the factors that may hinder or discourage recourse to the institution in question, such as doubts and uncertainties concerning the procedure to be followed and fears of retaliation or discrimination. In this perspective, the objective pursued by this procedure is to provide the *whistleblower* with clear operational indications on the subject, contents, recipients and methods of transmission of the reports, as well as with regard to the forms of protection offered.

3) OBJECT OF THE REPORT

Without prejudice to the possibility for the entity to extend the objective scope of application of this procedure, reports concerning conducts, risks, offences or irregularities, whether committed or attempted, to the detriment of the entity, with regard to violations of national or European Union law provisions that harm the public interest or the integrity of the entity, of which they have become aware in the working context, are to be considered relevant:

- administrative, accounting, civil or criminal offences;
- unlawful conduct relevant under Legislative Decree 231/2001 or the 231 Model adopted;
- offences, which may also be relevant with reference to European legislation, in the areas of (by way of example): public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and

animal health and welfare; public health; consumer protection; privacy and personal data protection and network and information system security;

- acts or omissions detrimental to the financial interests of the European Union;
- violations of competition and State aid provisions, as well as violations concerning the internal market related to acts infringing corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
- information on violations (reasonable suspicion of violations, concealment of violations).

This procedure **does not apply to**:

a) disputes, claims or demands linked to a personal interest of the whistleblower or of the person lodging a complaint with the judicial or accounting authorities, which relate exclusively to his or her individual employment relationships, or inherent to his or her employment relationships with hierarchically superior figures;
b) reports of violations that are already mandatorily regulated by European Union or national acts concerning financial services, products and markets and the prevention of money laundering and terrorist financing, transport safety and environmental protection, or by national acts that constitute implementation of European Union acts listed in Part II of the Annex to Directive (EU) 2019/1937;
c) reports of national security breaches, as well as of procurement relating to defence or national security aspects;
d) alerts on classified information, forensic and medical professional secrecy, secrecy of court deliberations.

With regard to **anonymous reports**, the discipline set out in this procedure does not apply, since it is designed to protect the whistleblower who, in the case of an anonymous report, is by definition anonymous. However, the same discipline will apply if, following an anonymous report, the name of the whistleblower is disclosed.

This is without prejudice to the application of the provisions of criminal procedure, as well as those concerning the exercise of the right of workers to consult their representatives or trade unions, protection against unlawful conduct or acts carried out as a result of such consultations, the autonomy of the social players and their right to enter into collective agreements, and the repression of anti-union conduct as referred to in Article 28 of Law No. 300 of 20 May 1970.

4) CONTENT OF THE REPORT

Reports shall in any case be circumstantiated and based on precise and concordant facts, of which the whistleblower has become aware by reason of the functions performed within the entity or in any case by working with the entity.

The whistleblower must provide all the useful elements to enable the competent corporate bodies to proceed with the due and appropriate checks to confirm the validity of the facts reported, in particular:

- a clear and complete description of the facts being reported;
- if known, the circumstances of time and place in which the reported facts were committed;
- if known, the particulars or other elements (such as the job title and the department in which the activity is carried out) enabling identification of the person(s) who has/have carried out the reported facts;
- an indication of any other persons who may give information on the facts being reported;
- an indication of any documents that may confirm the validity of those facts;
- any other information that may provide useful feedback on the existence of the reported facts.

5) WHO CAN REPORT AND WHO IS PROTECTED

The following persons are appropriately protected by this procedure and its implementation:

- **Whistleblowers:** employees of the entity, as well as self-employed workers, freelancers, consultants, shareholders, persons with administrative, management, control, supervisory and representative functions, volunteers and trainees, working for the entity or within the entity.
  It should be noted that the protective measures provided for in this procedure are guaranteed at every stage of the employment relationship (recruiting process or other pre-contractual stages, including the probationary period, if any) or collaboration (even after termination of the contractual relationship).

- **Facilitators:** those who work within the same work context as the whistleblower and assist him/her in the reporting process.
  This procedure guarantees the confidentiality of the facilitator's identity, as well as the assistance provided by him/her.

- **Colleagues, relatives, ownership entities:**
  - ✓ persons related to the whistleblower by a family relationship up to the fourth degree of kinship or by a stable emotional link and who work in the same work environment as the whistleblower;
  - ✓ work colleagues with whom the whistleblower has a regular and current relationship;
  - ✓ entities owned by the whistleblower or for which he/she works or which operate in the same work environment as the whistleblower.

The special protection reserved for the persons listed above requires the entity, also in the person of the person in charge of handling the report, to take all the measures provided for in paragraph 8 below.

6) WHSTLEBLOWING CHANNELS

Whistleblowers may use the following whistleblowing channels:

- **internal whistleblowing** channels: online platform, paper reporting, telephone reporting, voice mail, personal meetings;
- **external whistleblowing** channel: a channel set up by the ANAC, having a residual nature, as the whistleblower may only resort to the external channel if:
  - ➢ in its working context, there is no provision for internal channel activation as mandatory or, if provided for, it has not been activated;
  - ➢ internal whistleblowing was not followed up;
  - ➢ the whistleblower has reasonable grounds to believe that if it were to report internally, it would not be followed up or that it would face retaliation;
  - ➢ the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

This is without prejudice to the possibility of submitting complaints to the judicial or accounting authorities in cases within their jurisdiction, or of resorting to public disclosure if the conditions of Legislative Decree 24/2023 are met.

These are the internal reporting channels set up by IAF NETWORK S.P.A.:

a) written report to be submitted to:

- whistleblowing platform at the *link*: https://digitalroom.bdo.it/IAFNetwork

b) written report to be delivered by

- paper letter in a sealed envelope to:

  IAF NETWORK S.P.A.

  Via Flero n. 46 – 25125 Brescia

  To the persona attention of the HR Manager - confidential

  In this case, the whistleblower must use three envelopes:

  - the **first** envelope should contain a file with the identification data of the whistleblower and a copy of his/her identity document, unless he/she wishes to remain anonymous;
  - the **second** envelope should contain a file with a description of the report and any attachments;
  - the **third** envelope should contain the first two envelopes; this third envelope should be marked "to the attention of the whistleblowing Operator only".

c) oral report by means of a face-to-face meeting set within a reasonable time at the request of the whistleblower; in this case, subject to the consent of the person making the report, the report shall be documented by the staff member in charge by means of a recording on a device suitable for storage and listening or by minutes. In the case of minutes, the whistleblower is entitled to verify, rectify and confirm the minutes of the meeting by signing them.

7) WHISTLEBLOWING HANDLING

The report shall be taken over by the HR manager (hereinafter referred to as "Operator"), which shall perform the following activities:

a) issue the whistleblower with an acknowledgement of receipt of the report within 7 days of receipt;

b) maintain interlocutions with the whistleblower, as well as request additions from the latter if necessary;
c) diligently follow up the reports received and, therefore, initiate the investigation aimed at assessing the existence of the reported facts, also monitoring and managing the outcome of the investigations and any measures taken or adopted;
d) provide acknowledgement of the report within 3 months of the date of the acknowledgement of receipt or, in the absence of such notice, within 3 months of the expiry of the 7-day period from the submission of the report;
e) ensure that clear information is made available on the whistleblowing channel, procedures and prerequisites for making internal reports, and on the channel, procedures and prerequisites for making external reports.

An internal report submitted to a person other than the Operator shall be forwarded, within 7 days of its receipt, to the Operator, which shall inform the whistleblower thereof.

The Operator shall first carry out a **preliminary check on the admissibility of the report**. The latter shall be deemed inadmissible in the following cases:

- lack of data constituting the essential elements of the report;
- manifest groundlessness of the factual elements attributable to the breaches referred to in § 3;
- presentation of facts of such general content that they cannot be understood by the Operator;
- production of only documentation without the actual reporting of violations.

In the event of an inadmissible report, the Operator shall notify the administrative body and the whistleblower. Otherwise, it shall proceed as specified below.

The Operator shall carry out a **verification of the validity of the circumstances represented in the report and further handling of the report**; the Operator shall act in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the whistleblower and of any other persons who may report on the facts reported. In this case the Operator. In this case the Operator, without prejudice to the right of defence of the reported person, shall

a) initiate specific analyses, possibly involving the corporate functions concerned by the report, which shall guarantee the utmost and timely cooperation and shall be bound by the same obligations of confidentiality and impartiality as the Operator;
b) terminate the investigation at any time if, in the course of the investigation, it is established that the report is unfounded;
c) make use, if necessary, of experts from outside the entity.

The methodology to be used for the verification activities will be assessed by the Operator on a case-by-case basis, choosing the technique deemed most effective in relation to the nature of the event and the existing circumstances (interviews, document analysis, on-site inspections, technical consultations, research on public databases, checks on company equipment, etc.).

If the report proves to be unfounded, the Operator shall proceed with the filing of the report, providing the appropriate reasons and in any event informing the administrative body by sending it a **final report** and the whistleblower.

If the report proves to be well founded, the administrative body, on the basis of the **final report** issued by the Operator, may:

a) agreeing with the functions concerned on the possible action plan necessary for the implementation of the relevant control procedures, also ensuring the monitoring of the implementation of the relevant activities put in place;
b) agreeing with the functions concerned on possible steps to be taken to protect the interests of the entity (e.g. legal action, suspension/cancellation of suppliers);
c) request the initiation of disciplinary proceedings against the whistleblower, in the case of reports in respect of which it is established that the whistleblower is acting in bad faith and/or has a purely defamatory intent, which may also be confirmed by the unfounded nature of the report.

Also in this case the Operator shall inform the Whistleblower.

In the event that the report concerns the majority of the members of the administrative body, the Operator shall inform the Board of Auditors or the Monocratic Control Body, if applicable, for the assessment of the action to be taken.

8) PROTECTIVE MEASURES FOR THE WHISTLEBLOWER AND OTHER ACTORS INVOLVED

The following specific safeguards must be ensured in the handling of the report:

- the person concerned shall have the right to be heard or, at his/her request, to be heard by means of a written procedure through the filing of written submissions and documents;
- the confidentiality of the whistleblower, of the persons involved in or referred to in the report, of the other persons mentioned in § 5, as well as of the contents of the report and of the relevant documentation, must always be guaranteed;
- it is prohibited to disclose the identity of the whistleblower without his/her express consent;
- the Italian and European legislation on the protection of personal data (EU Reg. 679/2016, Legislative Decree 196/2003) must be fully respected.

With specific reference to the obligation of confidentiality with regard to the identity of the whistleblower and the content of the report, the identity of the whistleblower must be protected in any context subsequent to the report, with the exception of cases in which liability for libel and slander can be established pursuant to the provisions of the Criminal Code or Article 2043 of the Civil Code and cases in which anonymity cannot be enforced by law (e.g. criminal, tax or administrative investigations, inspections by supervisory bodies). Therefore, subject to the exceptions mentioned above, the identity of the whistleblower cannot be disclosed without his/her express consent and all those who receive or are involved in handling the report are required to protect the confidentiality of that information. Violation of the confidentiality obligation is a source of disciplinary liability, without prejudice to further forms of liability provided for by the law. Specifically:

- the identity of the whistleblower and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the whistleblower himself/herself, to persons other than those competent to receive or follow up the reports, expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196/2003;
- In criminal proceedings, the identity of the whistleblower is covered by secrecy in the manner and to the extent provided for in Article 329 of the Code of Criminal Procedure;

- In the context of disciplinary proceedings, the identity of the whistleblower may not be disclosed, where the disciplinary charge is based on investigations which are separate from and additional to the report, even if consequent to it. If the accusation is based, in whole or in part, on the report and knowledge of the identity of the whistleblower r is indispensable for the accused's defence, the report can only be used for the purposes of disciplinary proceedings if the whistleblower has expressly consented to the disclosure of his/her identity. In the latter case, the whistleblower will be notified in writing of the reasons for the disclosure of the confidential data;
- the whistleblower shall be notified by written communication of the reasons for the disclosure of the confidential data even if the disclosure of his/her identity and of the reported information is indispensable for the defence of the person concerned;
- the identity of the persons involved and of the persons mentioned in the report will be protected until the conclusion of the proceedings initiated as a result of the report in compliance with the same guarantees provided for in favour of the whistleblower.

Moreover, with regard to the **specific protection of the whistleblower and of the other persons referred to in § 5 from retaliation/discrimination**, no form of retaliation or discriminatory measure, direct or indirect, affecting working conditions for reasons directly or indirectly linked to the report is allowed or tolerated against the employee who makes a report under this procedure. Discriminatory measures include unjustified disciplinary actions, harassment in the workplace and any other form of retaliation leading to intolerable working conditions. Protection is limited to cases where both the reported person and the whistleblower are employees of the entity. Any employee who believes that he/she has suffered discrimination for having reported an offence is required to give detailed notice of the discrimination to the Operator, which, having preliminarily assessed the existence of the elements, reports the hypothesis of discrimination to the administrative body. The latter must, after verification, adopt any consequent measure necessary or appropriate to restore the situation and/or to remedy the negative effects of the discrimination, not excluding the initiation of disciplinary proceedings against the employee who has discriminated. Retaliatory measures include, but are not limited to:

- dismissal, suspension or equivalent measures;
- relegation in grade or non-promotion;

- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion on improper lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for the supply of goods or services;
- cancellation of a licence or permit;
- request to undergo psychiatric or medical examinations.

9) RESPONSIBILITY OF THE WHISTLEBLOWER

This procedure is without prejudice to the criminal and disciplinary liability of the whistleblower *in the* event of a libellous or defamatory report under the Criminal Code and Article 2043 of the Civil Code.

Any form of abuse of this procedure, such as reports that are manifestly opportunistic and/or made with the sole aim of harming the whistleblower or other persons, and any other hypothesis of improper use or intentional exploitation of the institution covered by this procedure, shall also give rise to liability in disciplinary and before other competent authorities.

Moreover, without prejudice to the above-mentioned provisions concerning any disciplinary measures falling within its competence, if, at the end of the proceedings,

the Operator, on the basis of the elements acquired, has evidence that the whistleblower's report also constitutes an offence of defamation and/or slander against the reported person, it shall grant the latter, upon request, access to the records of the internal investigation concluded, in order to enable him/her to exercise his/her rights.

The entity will be able to protect itself in the event of criminal or civil offences committed by the whistleblower through the forms provided for by law.

However, a person who discloses or disseminates information about breaches covered by the obligation of secrecy, other than the obligation of secrecy concerning classified information, forensic and medical professional secrecy, secrecy of court deliberations, or relating to the protection of copyright or the protection of personal data, or discloses or disseminates information about breaches that offend the reputation of the person involved or reported, shall not be punishable when, at the time of the disclosure or dissemination, there were reasonable grounds for believing that the disclosure or dissemination of the same information was necessary to disclose the breach and the public disclosure or denunciation was carried out in accordance with this procedure and the applicable provisions of law. In this case, any further liability, including civil or administrative liability, is also excluded.

Moreover, unless the act constitutes a criminal offence, no liability, including of a civil or administrative nature, is incurred for the acquisition of or access to information on violations. Nevertheless, criminal liability and any other liability, including of a civil or administrative nature, is not excluded for conduct, acts or omissions that are not connected with the reporting or denunciation to the judicial authority or public disclosure or that are not strictly necessary to disclose the breach.