NOTICE: This document is an English courtesy translation provided for informational purposes only. The original in Italian version remains the sole legally valid and binding text. In case of discrepancies between this translation and the original, the original version shall prevail, as it is the sole legally valid and binding version.

POLICY

WHISTLEBLOWING SYSTEM FOR THE MANAGEMENT OF REPORTS

27/05/2026	8.0	Risk and Compliance	Whistleblowing Committee Board of Directors
Date of last issue	**Version**	**Document verified by**	**Document approved by**

DOCUMENT HISTORY

Date	Event	Version
April 2019	Document adoption	1.0
18/03/2021	Update	2.0
27/03/2023	Update (formal aspects: brand identity, company name)	3.0
27/11/2023	Update (entry into force of Legislative Decree No. 24/2023)	4.0
25/06/2024	Update (entry into force of FIGC Guidelines)	5.0
13/01/2025	Implementation of changes to the composition of the Whistleblowing Committee, as per the Board of Directors' resolution of 17/10/2024	6.0
25/11/2025	Update following the achievement of Gender Equality Certification which also includes the Whistleblowing channel among the reporting methods.	7.0
27/05/2026	Update (publication of updated version of ANAC Guidelines)	8.0

Contents

1. Definitions and Acronyms

The expressions, terms and acronyms used in this document have the meanings set out below:

ANAC	National Anti-Corruption Authority
Self-employed	persons who have a self-employed working relationship with the Company as referred to in Title III of Book V of the Civil Code, including the persons referred to in Chapter I of Law No. 81 of 22 May 2017
Candidates	individuals participating in a selection process for a salaried position with the Company
Managing Director	The Managing Director identified as the employer
Code of Ethics	the code of ethics adopted by the Company
Code of Sports Justice	The Code of Sports Justice approved by the National Executive Committee of C.O.N.I. by Resolution No. 258 of 11 June 2019
Collaborators	persons who have a collaborative relationship with the Company as referred to in Article 409 of the Code of Civil Procedure and Article 2 of Legislative Decree No. 81 of 2015
Safeguarding Committee	The internal committee entrusted with the functions of the Officer responsible for combating abuse, violence and discrimination as referred to in Article 5(2) of the F.I.G.C. (C.U. 87/A of 31 August 2023)
Whistleblowing Committee	the internal committee responsible for managing the internal reporting channel
Consultants	persons who have contractual relationships with the Company for the provision of consultancy services
Employees	persons who have an employment relationship with the Company, including those whose employment relationship is governed by Legislative Decree No. 81 of 15 June 2015, or by Article 54-bis of Decree-Law No. 50 of 24 April 2017, No. 50, converted, with amendments, by Law No. 96 of 21 June 2017
Public Disclosure	the act of making information on violations public through the press or electronic media or, in any case, through means of dissemination capable of reaching a large number of people
Legislative Decree No. 196/2003	Legislative Decree No. 196 of 30 June 2003 containing the *"Personal Data Protection* Code"

Legislative Decree No. 231/2001	Legislative Decree No. 231 of 8 June 2001 on *"Regulation of the administrative liability of legal persons, companies and associations, including those without legal* personality"
Legislative Decree No. 24/2023	Legislative Decree No. 24 of 10 March 2023 on *the "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions on the protection of persons reporting breaches of national* law"
Facilitator	the natural person who assists a Whistleblower in the reporting process, working within the same workplace, and whose assistance must be kept confidential
F.I.G.C.	the Italian Football Federation
Suppliers	entities, both public and private, which have contractual relationships with the Company for the supply of goods or the provision of services
Safeguarding Framework	The Framework established by the Company to protect the welfare of minors and to prevent harassment, gender-based violence and any other form of discrimination
GDPR	Regulation (EU) No 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
ANAC Guidelines	the guidelines adopted by ANAC pursuant to Article 10 of Legislative Decree No. 24/2023
F.I.G.C. Guidelines	the guidelines on the protection of minors and the prevention of harassment, gender-based violence and any other form of discrimination referred to in Circular 87/A published on 31 August 2023
Freelancers	persons, other than Consultants, who have contractual relationships with the Company for the provision of intellectual services
Model	the organisation, management and control model adopted by the Company pursuant to Legislative Decree No. 231/2001
Prevention Model	the organisational, management and control framework designed to prevent acts contrary to the principles of loyalty, fairness and integrity, adopted by the Company in accordance with Article 7 of the F.I.G.C. Articles of Association
Guarantee Body	the Guarantee Body established by the Company pursuant to Article 7 of the F.I.G.C. Statutes

Supervisory Body	the supervisory body established by the Company pursuant to Legislative Decree 231/2001
Administrative Body	the Company's administrative body (board of directors or sole director, as the case may be)
Platform	the *web-based* application used by the Company for the receipt and management of Internal Reports
Person Involved	the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the breach is attributed or as a person otherwise implicated in the breach reported or publicly disclosed
Reporting Person	the natural person who makes the report or publicly discloses information on breaches discovered within their work context
Report	the communication, whether written or oral, of information concerning breaches committed or that may be committed within the organisation with which the Reporting Person has a legal relationship
External Report	a Report submitted via the external reporting channel
Internal Report	a Report submitted via the internal reporting channel
Trade Unions	the company trade union representatives (RSU/RSA) or, where no company trade union representatives (RSU/RSA) have been established, the delegates – regional or national, as the case may be – of trade union organisations that are comparatively representative at national level
Company	ACF Fiorentina S.r.l.
Members	the Club's registered members
TFEU	the Treaty on the Functioning of the European Union

2. Introduction

On 15 March 2023, Legislative Decree No. 24/2023 was published in the Official Gazette, transposing into Italian law the *whistleblowing* provisions laid down by Directive (EU) 2019/1937 and amending Legislative Decree No. 231/2001.

Article 4 of Legislative Decree No. 24/2023 requires private-sector entities that have adopted an organisational, management and control model pursuant to Legislative Decree No. 231/2001 or which, although not having adopted such a model, operate in certain sectors or have employed an average of at least fifty employees over the past year, to establish an internal reporting channel and to entrust its management to a person or a dedicated, independent internal office with staff specifically

trained to manage the reporting channel, or to an external entity, which is also independent and has staff specifically trained for this purpose.

Through the internal reporting channel, employees, collaborators, suppliers, consultants and other parties may report violations, even merely potential ones, of the Italian and European legal provisions referred to in Legislative Decree No. 24/2023, as well as of the code of ethics and the organisational, management and control model that may have been adopted.

Like the previous regulations, the new regulations also protect the whistleblower from any acts of retaliation carried out as a result of the report. Furthermore, under certain conditions, it is possible to make reports via the external reporting channel, which is operated and managed by ANAC.

That said, it should be noted that the 'guidelines' referred to in Article 7(5) of the Federal Statute also stipulate that clubs adopting an organisational, management and control model, including for the purposes of applying Article 7 of the Code of Sports Justice, must define and describe the process for handling reports from anyone who becomes aware of conduct contrary to the ethical principles of loyalty, fairness and integrity, and of breaches of the code of ethics and prevention models, as well as the safeguards put in place to protect whistleblowers and those reported.

Similarly, the F.I.G.C. Guidelines published in Official Communication No. 87/A of 31 August 2023 require sports clubs to establish a system for reporting conduct that breaches measures adopted to protect minors and to prevent harassment, gender-based violence and any other form of discrimination and, in general, to report cases of abuse, violence and discrimination occurring in the course of sporting activities, ensuring the confidentiality of the whistleblower's identity, the timely and effective handling of reports and the protection of whistleblowers against any form of secondary victimisation.

The Company, in the spirit of giving concrete effect to Article 6(2-bis) of Legislative Decree No. 231/2001, as amended by Legislative Decree No. 24/2023, the guidelines referred to in Article 7(5) of the Federal Statutes and the F.I.G.C. Guidelines, allows Reporting Persons to make Internal Reports via the Platform.

3. Purpose of the policy and intended audience

This document provides information on the channel, rules and conditions for making Internal Reports and External Reports, pursuant to Article 5(1)(e) of Legislative Decree No. 24/2023, as well as on the measures to protect the Reporting Person referred to in Chapter III of Legislative Decree No. 24/2023.

The Internal Reporting channel described in this document also implements the obligation set out in Article 6(2-bis) of Legislative Decree No. 231/2001, to which the Company is subject by virtue of having adopted an organisational, management and control model in accordance with Legislative Decree No. 231/2001, and the provisions of the Prevention Model and the Safeguarding Framework.

The rules described in this document apply to the Company.

Internal reports may be made regarding information on material breaches pursuant to **Legislative Decree No. 23/2023**, including – inter alia – the commission (or attempted commission) of the offences referred to in Legislative Decree
No. 231/2001 or, in any case, acts, conduct and omissions not in line with the provisions of **the Code of Ethics**, the **231 Model**, and the **Diversity, Equity and Inclusion (DEI) Policy,** by persons falling into the following categories:

- Candidates, limited to information on breaches acquired during the selection process or in other pre-contractual stages;
- Employees, including those on probation;

- former Employees, limited to information on breaches acquired during the employment relationship;
- Self-employed persons;
- Contractors;
- workers, both employees and self-employed, and contractors working for Suppliers;
- Freelancers;
- consultants;
- volunteers and trainees, whether paid or unpaid, who carry out their work at the Company;
- persons who perform administrative, managerial, supervisory, oversight or representative functions, whether de jure or de facto, within the Company; and
- Members.

In addition to persons falling within the categories identified above, internal reports regarding breaches of **the Code of Ethics** may also be made by persons not falling within the above categories who are subject to the provisions of the Code of Ethics itself.

Internal reports of breaches of **the Prevention Model** *and* ***the Diversity, Equity and Inclusion (DEI) Policy*** may also be made by business partners, intermediaries, supporters and, in general, by anyone who has dealings with the Company.

As for Internal Reports of breaches **of the Safeguarding Framework**, these may be made by anyone who has suffered a breach, witnessed one, or become aware of facts relating to a breach, even if only potential.

The rules described in this document do not apply to Internal Reports made by persons other than those listed above in relation to the various types of breaches. Should a person other than those listed above make an Internal Report, the decision as to whether to act on such a report and, if so, how to do so, is left to the Whistleblowing Committee.

Internal Reports may relate exclusively to conduct, acts or omissions consisting of:

- breaches of the Code of Ethics or the Model and/or unlawful conduct as defined under Legislative Decree No. 231/2001;
- offences falling within the scope of application of the European Union or national acts listed in Annex 1 to Legislative Decree No. 24/2023 or of national acts implementing the European Union acts listed in the Annex to Directive (EU) 2019/1937, even if not listed in Annex 1 to Legislative Decree No. 24/2023, relating to the following sectors: public procurement; services, products and financial markets; and the 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; the protection of privacy and personal data, and the security of network and information systems;
- acts or omissions affecting the financial interests of the European Union as referred to in Article 325 of the TFEU, as specified in the relevant secondary legislation of the European Union;
- acts or omissions relating to the internal market as referred to in Article 26(2) of the TFEU, including infringements of European Union competition and State aid rules, as well as infringements relating to the internal market connected with acts that breach the rules on

corporate tax or mechanisms designed to obtain a tax advantage that undermines the object or purpose of the applicable corporate tax legislation;

- acts or conduct that undermine the object or purpose of the provisions set out in the European Union acts referred to in the points above;
- breaches of the Prevention Model and/or unlawful conduct relevant under sports law or otherwise contrary to the ethical principles of loyalty, fairness and integrity;
- breaches of the Safeguarding Framework or, in general, instances of abuse, violence or discrimination (as defined within the Safeguarding Framework) occurring in the course of sporting activities;
- conduct resulting in forms of secondary victimisation against Members who file or express the intention to file a complaint with the judicial authorities or an Internal Report regarding information on breaches of the Safeguarding Framework or, in general, cases of abuse, violence or discrimination occurring in the course of sporting activities; who assist other Members in filing a complaint or an Internal Report regarding the same information; who act as witnesses in proceedings concerning abuse, violence or discrimination; or who take action in relation to safeguarding policies;
- breaches of the Company's Diversity, Equity and Inclusion (DEI) Policy and the gender equality management system.

Internal Reports may also cover information regarding:

- conduct aimed at concealing the violations indicated above;
- unlawful activities not yet committed but which the Reporting Person reasonably believes may occur in the presence of specific, concrete and consistent evidence;
- reasonable grounds for suspicion, taking into account the definition of reasonable grounds for suspicion set out from time to time by ANAC in its Guidelines.

It is left to the Whistleblowing Committee to decide whether to act on, and if so, how to act on, Internal Reports concerning information on breaches other than those listed above.

Internal Reports must be based on precise and consistent factual elements, set out the information they concern in as much detail as possible and, where appropriate, be accompanied by suitable supporting documentation.

Internal Reports with generic content or lacking the necessary elements to act upon them are immediately deleted by the Whistleblowing Committee.

Similarly, where technically feasible, personal data contained in the Report that is irrelevant for the purposes of its proper handling shall be deleted immediately.

Internal Reports should ideally contain the identifying details and contact details of the Reporting Person, which in some cases may be essential for the assessments falling within the remit of the Whistleblowing Committee referred to in paragraph 5.2 below.

In any case, the Reporting Person is permitted to make Internal Reports anonymously, which are treated by the Whistleblowing Committee in the same way as other Internal Reports.

4. Objective

The objective of the broader "Whistleblowing System" is to safeguard the integrity of the Company.

In general, the Company encourages its employees and collaborators to resolve any workplace disputes, where possible, through dialogue, even informal, with their colleagues and/or

their line manager. Reports must be made in a spirit of responsibility, be in the public interest, and fall within the categories of non-compliance for which the system was implemented.

5. Management of the Internal Reporting Channel

The management of the Internal Reporting Channel is entrusted to an internal committee known as the Whistleblowing Committee, composed of the Chair of the Supervisory Body and the external member of the Company's Guarantee Body[1] .

Upon taking up their posts, the members of the Whistleblowing Committee sign a specific declaration certifying that they are not in any situation of conflict of interest or, in any case, in situations (for example, marital relationships, de facto cohabitation, kinship up to the sixth degree or affinity up to the fourth degree with persons exercising administrative, managerial, control, supervisory or representative functions, including de facto functions, within the Company; significant financial or economic relationships with the Company; etc.) such as to limit or otherwise affect their autonomy and independence.

The Whistleblowing Committee may be assisted by one or more assistants, appointed by the Company as persons authorised to process data and bound by the same obligations of confidentiality and secrecy imposed on the members of the Whistleblowing Committee. The assistants receive adequate and specific training on how to manage the channel.

The activities carried out by the Whistleblowing Committee at each stage of the Internal Report's handling are documented in minutes, signed by the Committee and stored in a dedicated electronic archive.

Where the Internal Report concerns information on breaches relevant to the 231 Model and the Prevention Model, the Whistleblowing Committee shall promptly involve the Supervisory Body and the Guarantee Body, respectively.

If, on the other hand, the Internal Report concerns information on breaches of the Safeguarding Framework or, in general, on cases of abuse, violence or discrimination (as defined in the Safeguarding Framework), the Whistleblowing Committee shall promptly involve the Safeguarding Committee.

Where an internal report concerns information regarding breaches of the Diversity, Equity and Inclusion (DEI) Policy, the Whistleblowing Committee shall promptly involve the Gender Equality Committee.

5.1. The whistleblowing platform

To make an Internal Report, you must log in to the Platform, which can be accessed at **https://whistleblowing.acffiorentina.it**

Access to the Platform is subject to a 'no-log' policy; this means that the company's IT systems are unable to identify the point of access to the portal (IP address) if access is made from networks external to the organisation's own networks (for example, via a mobile phone network or via a connection from a home computer).

[1] If the person reported is a member of the Reporting Committee, the report is handled by the other member of the Reporting Committee. If, however, the Reporting Committee (or its sole member in the aforementioned case) is unable to perform its duties (e.g. due to absence or illness), the Chair of the Board of Statutory Auditors shall act as a substitute for the activities set out in this procedure, limited to the handling of that specific report.

After logging into the Platform, the Reporting Person will be guided through the completion of a questionnaire consisting of open-ended and/or closed questions that will enable them to provide the details characterising the report (facts, timeframe, financial implications, etc.).

Upon submission of the report, the Platform will issue the Reporting Person with a unique identification code (ticket). This number, known only to the Reporting Person, cannot be retrieved in any way if lost. The ticket will enable the Reporting Person to access their Internal Report via the Platform in order to: i) add further details to substantiate the Internal Report; ii) provide their personal details; iii) respond to any follow-up questions. The Platform allows for a virtual conversation (chat) between the reporting person and the Whistleblowing Committee.

The Platform also allows Internal Reports to be submitted orally by recording a voice message. The original voice message, which in some cases may allow the reporter to be identified, will remain accessible only to members of the Whistleblowing Committee.

5.2. The stages of report handling

Immediately upon receipt, or in any event within 7 days of the date of receipt of the Internal Report, the Platform issues the Reporting Person with an acknowledgement of receipt of the Internal Report.

Each Internal Report is assigned an identification code.

The Internal Report is automatically recorded within the Platform in a dedicated electronic register containing the identification code, the information provided by the Reporting Person when submitting the Internal Report, the date of receipt, the deadline by which the Internal Report must be processed, and its status.

Upon receipt of the Internal Report, the Whistleblowing Committee assesses the relevance and validity of the Internal Report, based on its content.

If, following this assessment, the Whistleblowing Committee decides not to act on the Internal Report on the grounds that it is irrelevant, manifestly unfounded due to the absence of factual elements sufficient to justify an investigation, or so vague as to prevent an understanding of the facts, it shall inform the Reporting Person within 3 months of the date of the acknowledgement of receipt and, at the same time, update the status of the Internal Report. The Whistleblowing Committee’s decision not to act on the Internal Report and the reasons given in support of the decision are documented in minutes kept in a dedicated electronic archive.

If, on the other hand, the Whistleblowing Committee considers further investigations necessary, it shall initiate a preliminary investigation and, at the same time, update the status of the Internal Report.

During the investigation, the Whistleblowing Committee may:

- interview the Reporting Person, the Person Involved and any other persons mentioned in the Internal Report;
- request from any Employee, without the need for prior notification to their line manager, the information and documents necessary to carry out the relevant investigations;
- request the engagement of external parties from the Managing Director, who shall be responsible for assessing and acting upon the request, without prejudice to the Company’s liability in the event of failure to comply with the obligations set out in Legislative Decree No. 24/2023.

The Whistleblowing Committee shall conclude the preliminary investigation in good time to inform the Reporting Person that the Internal Report has been closed or to allow the Managing Director to define and communicate to the Whistleblowing Committee the measures envisaged or adopted by the Company to follow up

the Internal Report and to inform the Reporting Person thereof within the time limit indicated below.

Once the investigation is concluded, the Whistleblowing Committee, if it decides to close the Internal Report due to insufficient evidence or other reasons, shall inform the Reporting Person within 3 months of the date of the acknowledgement of receipt.

If, on the other hand, it ascertains one or more breaches or finds it impossible to ascertain the breaches covered by the Internal Report due to the reticence of the Person Involved or any persons interviewed, it shall communicate the findings of the investigation to the Managing Director, together with any supporting documents, and shall simultaneously request, within no later than 3 months from the date of the acknowledgement of receipt, information on the measures planned or adopted by the Company to follow up on the Internal Report; it shall then, within the same timeframe, inform the Reporting Person. The Managing Director shall then forward the information and documentation received from the Whistleblowing Committee to the relevant company departments to assess the application of any disciplinary measures, or, in the event that the established breaches concern parties other than Employees, Members and Collaborators, the adoption of the measures provided for in the contract between the perpetrator of the breach and the Company. He or she shall then inform the Whistleblowing Committee of any disciplinary sanctions imposed or measures adopted in good time to enable the Whistleblowing Committee to respond to the Reporting Person within three months of the date of the acknowledgement of receipt.

Internal Reports and the related documentation are archived by the Whistleblowing Committee in dedicated archives, both paper-based and electronic, managed in a manner that ensures their confidentiality. In particular, digital archives are stored on servers external to the Company so as to prevent access by system administrators.

Internal Reports, the related documentation and the personal data contained therein are processed for the time necessary to follow up on the reports themselves and subsequently retained for the period determined on a case-by-case basis by the Whistleblowing Committee in relation to the nature of the report and the consequent need to monitor the recurrence of similar reports over time and/or assess the validity of related reports, in any event for no longer than five years from the date of notification of the final outcome of the reporting procedure.

In the event that, following an Internal Report, the Company decides to initiate disciplinary proceedings or to bring legal or administrative proceedings, or to initiate arbitration or conciliation proceedings, the Internal Reports and related documentation shall be retained for a period equal to the duration of the proceedings or the limitation period for the rights for the establishment, exercise or defence of which such retention is necessary, even if this exceeds the retention periods indicated above.

6. External Reports

Pursuant to Article 6 of Legislative Decree No. 24/2023 (the essential content of which is reproduced in this paragraph), whistleblowers falling within the categories of persons referred to in Article 4 of Legislative Decree No. 24/2023 may make External Reports via the External Reporting channel established by ANAC in accordance with the procedures described on its website, provided that one or more of the following conditions apply:

- the Whistleblower considers that the Internal Reporting channel established by the Company does not
  complies with the provisions of Article 4 of Legislative Decree No. 24/2023;
- the Reporting Person has already made an Internal Report and no action has been taken on it;
- the Reporting Person has reasonable grounds to believe that, if they were to make an Internal Report, it would not be effectively followed up or that the Internal Report could lead to a risk of retaliation;

- the Reporting Person has reasonable grounds to believe that the Breaches covered by the Report may constitute an imminent or obvious danger to the public interest.

7. Protection of whistleblowers

In accordance with the provisions of Chapter III of Legislative Decree No. 24/2023 (the essential content of which is reproduced in this paragraph), it is prohibited for anyone acting in the name of or on behalf of the Company to take retaliatory action as a result of an Internal Report, an External Report, Public Disclosure or a report to the judicial and accounting authorities against:

- Whistleblowers;
- the authors of Public Disclosures;
- those who have filed a complaint;
- Facilitators;
- persons who are part of the Company's organisation and who are related to Whistleblowers, authors of Public Disclosures and those who have filed a complaint by a stable emotional bond or kinship up to the fourth degree;
- colleagues of the Reporting Persons, the authors of Public Disclosures and those who have filed a complaint who have a regular and ongoing relationship with them;
- entities owned by the Reporting Persons, the authors of Public Disclosures and those who have filed a complaint, or for which they work, as well as entities operating within or on behalf of the Company.

Retaliatory action means any conduct, act or omission, even if merely attempted or threatened, carried out as a result of the Report, the complaint to the judicial or accounting authorities, or the Public Disclosure, and which causes or may cause the Reporting Person or the person who filed the complaint, directly or indirectly, unjust harm and, in particular, by way of example and without limitation:

- dismissal, suspension or equivalent measures;
- demotion or failure to be promoted;
- a change of duties, a change of workplace, a reduction in salary, or a change in working hours;
- suspension of training or any restriction on access to it;
- negative performance reviews or negative references;
- the imposition of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion;
- the 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 the loss of economic opportunities and loss of income;
- inclusion on blacklists based on a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in that sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the revocation of a licence or permit;
- a request to undergo psychiatric or medical examinations.

Any person or entity who believes they have been subjected to an act of retaliation may report this to ANAC, which will inform the National Labour Inspectorate so that it may take the measures within its remit. In the event that the judicial authorities establish a breach of the prohibition on retaliation, the person or entity that has suffered the act of retaliation shall be entitled to the protective measures provided for in Article 19 of Legislative Decree No. 24/2023.

Whistleblowers falling within the categories of persons referred to in Article 4 of Legislative Decree No. 24/2023 may also request from the third sector organisations listed by ANAC

for information, assistance and advice free of charge on reporting procedures, protection against retaliation, the rights of the Person Involved, and the terms and conditions for accessing legal aid.

The protection and support measures indicated above are not guaranteed in respect of the Whistleblower and any person who has filed a complaint where criminal liability for the offences of defamation or slander, or civil liability on the same grounds, has been established, even by a first-instance judgment, in cases of wilful misconduct or gross negligence.

Specific protection measures against any form of secondary victimisation are provided to Members who have:

- filed a complaint with the judicial authorities or an Internal Report;
- expressed their intention to file a complaint with the judicial authorities or an Internal Report;
- assisted or supported another member in filing a complaint with the judicial authorities or an Internal Report;
- given evidence or attended a hearing in proceedings concerning abuse, violence or discrimination;
- taken any other action or initiative relating to or concerning safeguarding policies.

8. Responsibility of the whistleblower

It is the responsibility of the Reporting Person to make reports in good faith. Reports that are manifestly false or entirely unfounded, opportunistic and/or made for the sole purpose of harming the person reported or any other parties affected by the report will not be taken into consideration.

9. Training and information

The Company promotes the dissemination and understanding of the entire “Whistleblowing System” (which may be delivered via e-learning) through training courses designed to raise awareness of and facilitate the understanding and implementation of the reporting system. The organisation of these aspects is the responsibility of HR & Organisation.

10. Protection of Personal Data (Articles 13 and 14 of EU Regulation 2016/679)

Given that this document already provides, as a whole, detailed information on the purposes and methods of personal data processing following the submission of an Internal Report and its subsequent handling, this paragraph sets out further details and additional information in accordance with the principle of transparency and safeguarding the rights of data subjects.

The data processed, the provision of which by the data subject is obviously optional, may concern the Reporting Person and other natural persons involved in the subject matter of the report and will consist of:

- data/documents provided by the data subject;
- data acquired during the subsequent stages of the report’s handling and necessary for its assessment;
- data from public registers, lists, records or documents accessible to anyone, provided such data is necessary in accordance with the provisions of this policy;
- other data from sources lawfully accessible in relation to the purposes pursued.

The data mentioned above may also include, only if relevant and necessary in relation to the purposes set out in this document, data relating to criminal convictions and offences and/or special categories of personal data [defined in paragraph 1 of Article 9 of EU Regulation 2016/679 as

belonging to “special categories” *“personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning health or a person’s sex life or sexual* orientation”].

To summarise what has already been stated in the preceding paragraphs of this policy, the processing of personal data resulting from the submission of a report may serve the following purposes, for each of which the “legal basis” enabling it is indicated in brackets *[the “legal bases” are the conditions that render a purpose lawful in accordance with Articles 6 and 9 of EU Regulation 2016/679]:*

- proper management of the report and application of the provisions set out in this policy, and compliance with obligations arising from laws, regulations or EU legislation *[legal bases: legal compliance – Article 6(1)(c) – legitimate interest consisting of the protection of the Company’s assets and personnel – Article 6(1)(f)];*
- to protect the confidentiality of the Whistleblower’s identity *[legal bases: compliance with a legal obligation – Article 6(1)(c) – legitimate interest consistent with the purpose – Article 6(1)(f)];*
- to protect staff, assets and company property; *[legal basis: legitimate interest coinciding with the purpose – Article 6(1)(f)];*
- to prevent and detect the commission of offences or circumstances conducive to the commission of offences, thereby protecting staff, assets and company property *[legal basis: legitimate interest consistent with the purpose under Article 6(1)(f)]*;
- to identify and pursue conduct subject to disciplinary action *[legal bases: performance of a contract – Article 6(1)(b) and Article 9(2)(b) of EU Regulation 2016/679 – legitimate interest coinciding with the purpose under Article 6(1)(f)]*;
- to assert or defend a right in court or to assess whether there is a right that can be usefully protected in court *[legal bases: coinciding with the purpose – Article 9(2)(f) of EU Regulation 2016/679]*;
- compliance with orders issued by the judicial authorities *[legal bases: legal compliance – Article 6(1)(c) and Article 9(2)(f) of EU Regulation 2016/679].*

In summary, the processing operations in question may be carried out:

- as necessary for the pursuit of a legitimate interest of the Data Controller consistent with the purposes of this document (to safeguard the integrity of ACF Fiorentina);
- as necessary to assert or defend a right in court or to assess whether there is a right that can be usefully protected in court;
- as necessary to comply with obligations arising from laws, regulations or EU legislation.

In addition to the parties already mentioned above, the data may be processed on behalf of the data controllers by:

- any assistants to the Whistleblowing Committee;
- staff responsible for verification, inspection, investigation, expert assessment and evaluation activities, excluding consultation, and staff responsible for the maintenance of IT systems;
- entities (companies/professionals, including those outside the European Union where necessary in relation to the nature of the report or the parties involved) acting as Data Processors pursuant to Article 28 of EU Regulation 679/2016 in connection with such activities, or providing services ancillary to them, such as: legal advice and assistance, expert reports, specialist consultancy, information systems management, audits and investigative activities; in this regard, it should be noted that such parties will always and in any case be bound to fully comply with the rules and procedures aimed at ensuring the widest possible protection of personal data adopted and imposed by the Data Controller, including but not limited to compliance with current legislation.

Personal data may be disclosed or made available to:

- parties indicated by the data subjects themselves
- parties involved in any legal or disciplinary proceedings arising from or related to the report, in accordance with current legislation
- to parties who may access the data pursuant to provisions of law, regulations or EU legislation, within the limits set out in such rules;
- judicial authorities, judicial police;
- parties (companies/professionals, including those outside the European Union where necessary in relation to the nature of the reported incident and/or the parties involved) who participate as Data Controllers in the activities, or who provide services ancillary to them, such as: legal advice and assistance, audits and investigative activities.

Naturally, this is limited to what is necessary for the recipient body/office (which will remain an independent Data Controller for all subsequent processing) to carry out its duties and/or to achieve the purposes related to the disclosure itself.

Personal data will not be disclosed.

Personal data may also be transferred to entities located outside the European Union where this is necessary in relation to the nature of the report and the parties involved; in particular to the country or countries:

- where the parties involved in the report are based;
- in which the subject matter of the report occurred or has its effects.

The transfer will always be carried out in full compliance with the law and exclusively for the purposes referred to above:

- where one of the conditions set out in Article 49 of EU Regulation 2016/679 applies:

  a) the data subject has explicitly consented to the transfer;

  b) the transfer is necessary for the performance of a contract concluded between the data subject and the data controller or for the implementation of pre-contractual measures taken at the data subject's request;

  c) the transfer is necessary for the conclusion or performance of a contract between the data controller and another natural or legal person in favour of the data subject;

  (e) the transfer is necessary for the establishment, exercise or defence of legal claims;

- and/or to entities required to ensure an adequate level of protection, including by signing the standard contractual clauses set out at European level (Commission Implementing Decision (EU) 2021/914 of 4 June 2021), or by adopting and documenting other forms of adequate safeguards as provided for in Article 46 of Regulation (EU) 2016/679; such entities may include, where necessary for the proper handling of the report, the affiliated company Mediacom Communications Corporation, based in the USA, appointed as Data Processor in relation to the services it provides to Fiorentina – the Data Controller is ACF Fiorentina S.r.l., with registered office at Via Pian di Ripoli, No. 5, 50012, Bagno a Ripoli (FI).

ACF FIORENTINA S.r.l. has appointed a Data Protection Officer tasked with monitoring compliance with personal data protection legislation, whose contact details are: rpd@acffiorentina.it

The data subject has the right:

- to request from the Data Controller access to their personal data, and the rectification or erasure of such data, or the restriction of the processing of personal data concerning them, and to object to such processing;
- if the processing is carried out by automated (computerised) means and on the basis of their consent, to receive the personal data concerning them in a structured, commonly used and machine-readable format and/or to have it transmitted directly to another data controller, where technically feasible;
- to withdraw their consent at any time (without prejudice to the lawfulness of processing based on consent prior to withdrawal), obviously in respect of processing carried out on that basis;
- to lodge a complaint with a supervisory authority: Garante per la protezione dei dati personali - Piazza Venezia n. 11 00187 ROME - Switchboard: (+39) 06.696771 - Email:protocollo@gpdp.it - certified emailprotocollo@pec.gpdp.it .

To exercise their rights, the Data Subject may contact ACF FIORENTINA S.r.l. via the email addressinfoprivacy@acffiorentina.it or by sending a registered letter to the address specified above, or by calling +055571259, specifying to the operator the nature of the request or the issue raised, bearing in mind that:

- it will not be possible to respond to requests received by telephone where there is no certainty regarding the identity of the applicant.
- that pursuant to Legislative Decree 196/2003, Article 2-undecies (Limitations on the rights of the data subject), the rights referred to in Articles 15 to 22 of EU Regulation 2016/679 may not be exercised if the exercise of such rights could result in actual and concrete prejudice:
  - the confidentiality of the Whistleblower's identity;
  - to the conduct of defence investigations or the exercise of a right in court.

11. Updating of the Policy

This document and the Platform will be subject to periodic review to ensure ongoing compliance with the legislation, as well as in light of operational requirements and experience gained.

ANNEX NO. 1 – CONFIDENTIALITY UNDERTAKING

Whereas:

(i) ACF Fiorentina has adopted its own Whistleblowing System;

(ii) in the context of managing Reports, the recipient of the report may need to involve third parties – including the relevant company departments as deemed appropriate – for the purpose of ascertaining the facts in question;

(iii) In order to ensure the effectiveness of the investigation, as well as to protect the identity of the person making the Report ("**the** Whistleblower") and/or the person(s) alleged to have engaged in unlawful conduct or breached the Code (the **"Subject** of the Report"), it is necessary to impose strict confidentiality obligations on all those involved in the investigation of the Report;

In view of the above

I, the undersigned [_____], born [_____], resident at [_____], Tax Code [_____], acting in the capacity of [_____] / in my capacity as [_____], having taken note of the above-mentioned documentation:

1. undertakes

   (i) to treat the information received or acquired in the course of supporting the person handling the report, in the verification thereof and/or relating to the identity of the Reporting Party or the Reported Party (the **"Confidential** Information") as strictly private and confidential, and to take all reasonable measures to keep such information confidential;

   (ii) to use the Confidential Information solely for the purpose of assisting the person handling the report in the verification, investigation and assessment thereof;

   (iii) not to disclose, in any manner or form, and without prior written authorisation from the person handling the report, any Confidential Information to third parties (whether internal or external to the Company), unless required to do so by law or by a binding request from the Judicial Authority or its auxiliaries;

   (iv) in the event of a report being closed, to return to the person handling the report all copies of documents in their possession, and to delete or destroy any information stored on a computer or other device owned, held or controlled by the undersigned, which contains Confidential Information.

2. The obligations assumed under this Confidentiality Undertaking do not apply to information which: (i) at the time it is provided is already in the public domain or (ii) after receipt, becomes in the public domain for reasons unrelated to a breach of this confidentiality undertaking.

3. The obligations undertaken under this Confidentiality Agreement shall take effect from the date of signature.

Signature _____

Date _____