Whistleblowing Policy (hereinafter "The Policy") for staff members of Capital Dynamics SGR S.p.A.

Main regulatory sources:

- Legislative Decree 231/2001 as further amended and supplemented;
- Legislative Decree 231/2007 as further amended and supplemented;
- Italian Legislative Decree n. 81/2008 as further amended and supplemented;
- UE Regulation n. 679/2016 (GDPR) and Legislative Decree n. 196/2003 as amended and supplemented
- Market Abuse Regulation (EU MAR n. 596/2014);
- Legislative Decree no. 58 of 24 February 1998 (T.U.F.) (artt. 4-undecies and 4-duodecies);
- Bank of Italy Regulation issued on December 5th, 2019 and subsequent amendments (Art. 9, 39 and Annex 4);
- EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law;
- Legislative Decree No. 24 of 10 March 2023, implementing EU Directive 2019/1937 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws' dictated an organic regulation of the matter;
- Guidelines on the protection of persons who report violations of Union law and protection of persons who report violations of national laws. Procedures for the submission and management of external whistleblowing, approved by the National Anti-Corruption Authority (ANAC) with resolution No. 311 of 12 July 2023.

Perimeter of application

A Whistleblower is the natural person who makes a report or public disclosure of violations of which he has become aware in the context of his own work context and/or of the work or professional activities performed in favour of the Company (pursuant to Article 2(1)(g) and (i) of Legislative Decree 24/2023).

Addressees of the Policy (potential Whistleblowers) are all persons who are in possession of information on violations falling within the scope of this Policy and who, as such, benefit from the protection measures provided for therein.

The following may submit a report (the 'Addressees'):

- members of the Board of Directors of the SGR;
- members of the Board of Statutory Auditors of the SGR;
- members of the SGR Management;
- all employees of the SGR;
- collaborators of the SGR;
- self-employed workers;
- self-employed professionals and consultants working for the Company;
- volunteers and trainees, both paid and unpaid, who work for the Company;
- shareholders of the Company.

As provided for in Article 3 (4) of Legislative Decree 24/2023, the protection of the Whistleblower is also guaranteed in the following cases:

- when the legal relationship with the Company has not yet commenced, if the information on violations was acquired during the selection process or in other pre-contractual phases;
- during the probationary period;
- after the termination of the legal relationship with the Company, if the information on breaches was acquired during the course of the relationship.

The protections in favour of the Whistleblower (so-called 'protection measures'), referred to in the following paragraphs, also extend to the following figures:

- facilitators (the persons assisting the reporter in the reporting process);
- persons belonging to the same work environment as the Whistleblower, to whom the Whistleblower is linked by a stable emotional or kinship link;
- work colleagues of the Whistleblower to whom the Whistleblower has a habitual and current relationship;
- entities owned by the whistleblower or for which the protected persons work.

This Policy also applies to suppliers of advisory services when the advice provided is continuous and involves the de facto inclusion, even temporary, of specific persons within the company structure.

All the persons listed above are referred to hereinafter as "addresseses".

Qualifying Disclosure

Anyone who makes a "*Qualifying Disclosure"* (defined herein) of information that is in the public interest has the right not to suffer detriment or victimization because of the disclosure. A Qualifying Disclosure is one, which, in the reasonable belief of the staff members, suggests that one or more of the following has been, is being, or is likely to be committed (each, a "Report"):

- administrative, accounting, civil or criminal offences (under Legislative Decree 231/2001);
- placing the health and safety of any employee in danger (Italian Legislative Decree n. 81/2008 as further amended and supplemented);
- a failure to comply with any legal obligation;
- offences falling within the scope European Union acts relating to, but not limited to, the following areas: public procurement, financial services, products, markets and prevention of money laundering and financing of terrorism;
- damage to the environment;
- possible violation of the anti-money laundering regulation (Italian Legislative Decree n. 231/2007 as further amended and supplemented)
- a miscarriage of justice;
- possible fraud and corruption;
- a violation of the Code of Ethics or other ethical conduct;
- possible violation of the GDPR and related implementing regulation (Italian Legislative Decree n. 196/2003 as amended and supplemented);
- violations of the provisions of the Consolidated Law on Finance ("Testo Unico della Finanza") and its implementing provisions;
- a violation of the Market Abuse Regulation (EU Reg. MAR n. 596/2014);
- deliberate concealment relating to any of the above;
- any other possible violation of the law.

The Reports that will be taken into account are only those that are circumstantiated and well-founded and that concern facts found directly by the Whistleblower, not based on suppositions or current rumours.

Moreover, the reporting system may not be used by the Whistleblower for purely personal purposes, for claims or complaints, which, if anything, fall within the more general discipline of the employment/collaboration relationship or of relations with the hierarchical superior or with colleagues, for which reference should be made to the procedures falling within the competence of the corporate structures.

Reports concerning the following are excluded from the scope of application of the Policy:

- disputes, claims or requests linked to an interest of a personal nature of the person making the report, which relate exclusively to his/her individual work relationships or public employment relationships, or inherent to his/her work relationships or public employment relationships with hierarchically superior figures, unless they are linked to or refer to the violation of rules or internal rules/procedures;
- violations if already mandatorily regulated by European Union or national acts, as indicated in Article 1, para. 2, letter b) of Legislative Decree no. 24/2023 (concerning financial services, products and markets and the prevention of money laundering and the financing of terrorism, transport safety and environmental protection)
- breaches of national security, as well as procurement relating to defence or national security aspects, unless such aspects are covered by relevant secondary European Union law;
- facts or circumstances falling within the application of national or European Union provisions on classified information, forensic or medical secrecy and secrecy of court deliberations, or falling within the application of national provisions on criminal procedure, the autonomy and independence of the judiciary, provisions on the functions and powers of the Consiglio Superiore della Magistratura on national defence and public order and security, as well as on the exercise and protection 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 partners and their right to enter into collective agreements, and the suppression of anti-union conduct.

Please note that:

- Staff members must believe that the disclosure of information is in the public interest, and does not apply to matters relating exclusively to your employment;
- Staff members must believe it to be substantially true;
- Staff members must not act maliciously or make false allegations;

- Staff members must not seek personal gain.

Confidentiality

Every effort will be made by the SGR to treat the complainant's identity with appropriate regard for confidentiality wherever possible. However, there will be circumstances where this is not possible, for example, where the whistleblower is an essential witness, or where we would be unable to investigate a situation further without revealing the whistleblower's identity.
Additionally, depending on the nature of the Qualifying Disclosure, the matter may be escalated to members of senior management or the Board of Directors of the SGR, or external parties or independent bodies/agencies, as appropriate. Any Qualifying Disclosure raised anonymously will be considered but may prove more difficult or impossible to investigate due to the anonymous status. This policy encourages any staff member however to put his/her name wherever possible and, in any case, any concern will be treated on a confidential basis.

The SGR recognizes that the decision to report a Qualifying Disclosure can be a difficult one to make. If what you are saying is true, you should have nothing to fear because you will be doing your duty to your employer and those for whom you provide a service.

The SGR will not tolerate any harassment or victimization (including informal pressures) and will take appropriate action to protect you when you raise a concern, which is in the public interest.

The SGR guarantees the confidentiality of the report and the data of the reporter; in particular, the reported person has no right to know the identity of the whistleblower without its consent. For this reason, anonymous reports are normally not accepted. The documentation relating to reports is confidential and is kept in compliance with the security regulations in force at the SGR by the Whistleblowing Manager (as defined below).

Reporting modes

The ways in which reports of illegal behavior can be made are indicated below. In order to guarantee the confidentiality of the personal data of the Whistleblower and the alleged perpetrator of the violation, reports should normally be sent to the Compliance function of the SGR appointed as Whistleblowing Manager at the following email address: gdipuma@capdyn.com.

The Whistleblowing Manager performs the following tasks:

- is competent to receive reports through the “internal channel” referred to below;
- within 7 days of receipt of the report, he shall provide feedback to the Whistleblower as to whether the report has been taken into account;
- informs the Board of Directors and the Board of Statutory Auditors that the report has been received and taken into account;
- manages the reports with regard to the preliminary investigation activities deemed necessary to verify their grounds, guaranteeing the confidentiality of the identity of the Whistleblower;
- within 3 months of taking charge (unless an exceptional extension is notified to the reporting party), he informs the reporting party of the outcome of the report;
- informs the Board of Directors and the Board of Auditors of the outcome of the report;
- proposes to the Board of Directors to evaluate the application of disciplinary measures against the author of the ascertained violation;
- proposes to the Board of Directors the measures deemed appropriate to eliminate any deficiencies found in the procedures concerning the receipt and management of reports;
- submits an annual report to the Board of Directors on the activity performed and on any corrective measures proposed;
- sets up and updates a Whistleblowing Register in which it records all the relevant information about the report and its related stages of processing;
- keeps the documentation relating to the report in its own custody.

A ‘Confidential’ email is only received by the intended recipient and cannot be intercepted by a third party. Capital Dynamics employs encryption solutions to ensure this. Please see the Capital Dynamics IT handbook for additional detail on encryption and sensitive data.

In cases of urgency, the report is also accepted by means of a signed letter (to be addressed to the Whistleblowing Manager, indicating in the subject line "whistleblowing report").

Anonymous reports are also admissible, provided they are substantiated.

In the case of anonymous reports, those containing facts that are generic, confusing or do not allow the reconstruction of the facts that are the subject of the report shall not be taken into account.

Any Report must be addressed through the confidential reporting guidelines as listed above to the Whistleblowing Manager.

The Whistleblowing Manager is the person in charge of managing the internal reporting systems of the SGR and, by its nature, is in a functional hierarchical position such as not to compromise the investigations.
The Whistleblowing Manager is not involved in the adoption of any decision-making measures that are referred to the relevant departments or corporate bodies.
In alternative, to ensure a back-up of the Whistleblowing Manager ("*Funzione di Riserva*"), the Reports could be addressed to CD Global Compliance Officer Reid Conway (rconway@capdyn.com). The following functions could be involved as well in case of need:

- Group General Counsel, or
- Group Human Resources, or
- Group Chief Executive Officer

REPORTING THROUGH INTERNAL CHANNELS

For the purposes of reporting, the Whistleblower must use the form annexed to this Policy (ALLEGATO 1 - MODULO PER LA SEGNALAZIONE INTERNA DELLE VIOLAZIONI).

In any case, it is essential that the facts are of direct knowledge of the whistleblower and have not been reported by others.

The report is sent by the Whistleblower to the Whistleblowing Manager by one of the following means:

- by sending it to the e-mail address of the Whistleblowing Manager;
- by registered letter (marked as confidential) to the address of the Company to the attention of the Whistleblowing Manager

If that person is the alleged perpetrator of the breach or has a potential interest related to the report such as to compromise impartiality of judgement, the report must be addressed to the Company for the attention of the "Reserve Function" as identified above.

Reports "by internal channel" may also be transmitted orally. The Whistleblower, if he/she deems it appropriate, may also request a direct meeting with the Whistleblowing Manager . In this case, subject to the consent of the Whistleblower, the meeting is documented by the personnel in charge by means of a recording on a device suitable for storage and listening, or by minutes, which the Whistleblower may verify, rectify and confirm by signing.

The process of evaluating internal reports is divided into the following phases:

(a) receipt of the report;

(b) confirmation to Whistleblower about receipt of the report within 7 days;

(c) analysis and evaluation of the report;

(d) information upon completion of the phase (a), (b) and (c) to the Board of Directors of the SGR within 30 days of receipt of the report. Other parties' involvement may be required such as the Global Compliance Officer, Human Resources Department, relevant directors, officers or committees of Capital Dynamics, internal and/or outside counsel, accounting firms, internal or external investigators, regulatory or other government authorities or other appropriate internal personnel or third parties ("Relevant Parties"). The Global Compliance Officer, in consultation with appropriate Relevant Parties, will determine whether to further investigate the issues raised in the Report or not and, if so, the course of any investigation, as well as any internal or external reporting or referrals for further action. Depending on the nature of the concern, the matter may be disclosed to an auditor, the judicial police or another independent body or regulatory authorities;

(e) information to the reporting party of the outcome of the report within 3 months of the date of the report.

Decisions and any remedial action should be clear and fully documented on the investigation log.

The Whistleblowing Manager must record each report in a special register reserved for whistleblowing reports ("ALLEGATO 2 – REGISTRO SEGNALAZIONI WHISTLEBLOWING") assigning a progressive identification code. The Register is kept by the Whistleblowing Manager in electronic and/or paper form and must contain (at least) the following information:

- **Date and means of receipt of the report;**
- **Information relating to the Whistleblower:** name, surname, organizational unit of reference and function covered;

The Whistleblower is required to declare the presence of any private interests linked to the report if any.

- **Information relating to the reported person:** name, surname, organizational unit of reference and function covered;
- **Information about any other persons involved in the Whistleblowing process:** name, surname, organizational unit of reference and function covered;
- **Any counter-deductions of the reported person;**

- **Actions taken;**
- **Final report(s) by the Whistleblowing Manager dated and signed;**
- **Date of closure of the Whistleblowing process**

In line with the principle of proportionality, taking into account the size and complexity of the SGR, the Whistleblowing Manager directly manages all stages of the reporting process mentioned above, i.e. receipt, examination, assessment and communication.

Similarly, should the report concern a member of the Board of Directors, as the person hierarchically supervised by the Whistleblowing Manager, the latter shall promptly inform the Chairman of the Board of Statutory Auditors.

Among the most serious cases are those relating to the violation of labor rights (e.g. mobbing), anti-money laundering and market abuse violations.

All reports are managed by the Whistleblowing Manager with the utmost care and attention. In the event that an initial verification does not reveal sufficient evidence to launch an investigation, the Whistleblowing Manager shall inform the reporting party. If the report is made in bad faith, disciplinary action may be taken against the whistleblower, in compliance with the relevant company procedures

The whistleblower must be protected against any negative repercussions for him or her in the event that, upon verification of the justification of the report, no elements emerge to justify the adoption of measures against him or her. In the event of measures being taken against the person responsible for the reported breach, the person must, in any case, be protected against any further negative repercussions potentially in addition to those which are the subject of the measures taken by the competent bodies.

REPORTING THROUGH AN EXTERNAL CHANNEL TO THE SUPERVISORY AUTHORITIES

The whistleblower may also make a report through an “External Channel” if, at the time of submission, one of the following conditions is met:

- the reporting person has already made a report through the 'internal channel' and the report was not followed up;
- the person making the report has reasonable grounds to believe that, if he/she were to make a report through the “internal channel”, the report would not be effectively followed up, or that the report may give rise to the risk of retaliation;

- - the person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The “external channel” is activated by the National Anti-Corruption Authority (ANAC).
Information on the conditions, forms and methods of submission can be found at: htts://anticorruzione.it/-/whistleblowing.

In addition, the Bank of Italy and CONSOB, pursuant to Article 4-duodecies of the TUF, have respectively implemented the following channels in order to transmit any whistleblowing concerns in relation to any possible regulatory violations or misconducts:

CONSOB (http://www.consob.it/web/area-pubblica/wistleblowing)

There are the following channels to send a report to Consob:

- Phone: +39068411099

- E-mail address: whistleblowing@consob.it (using specific modules to download through the link http://www.consob.it/web/area-pubblica/wistleblowing-ricezione-segnalazioni)

- Confidential postal service envelope addressed to CONSOB, Via G.B. Martini 3, 00198 - ROMA

BANCA D’ITALIA (https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html)

There are the following channels to send a report to Bank of Italy:

- Online Platform “Servizi online” ticking the box “Invia una segnalazione”
- Confidential postal service envelope addressed to Banca d’Italia, Dipartimento Vigilanza bancaria e finanziaria - Servizio RIV – Divisione SRE – Via Nazionale, n. 91 – 00184 Roma.

<u>Reports by public disclosure</u>
Reports may also follow the public disclosure channel, and the Whistleblower is guaranteed the same protections as for reports submitted through the “internal channel” and the 'external channel' if one of the following conditions is met:

- the person making the report has previously made an internal and an external report, or has made an external report directly and no reply has been received in due time;

- the person making the report has justified reason to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the person making the report has justified reason to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be in collusion with or involved in the perpetrator of the breach.

Violation of this Policy is a source of disciplinary liability, without prejudice to other forms of liability provided for by law.

In order to prevent the fear of being subjected to detrimental consequences from inducing people not to report breaches, the identity of the Whistleblower may not be disclosed, without his or her express consent, and all those involved in the handling of the report are required to protect the confidentiality of such information.

Exceptions to this are cases in which the Whistleblower may be held liable for libel and slander under the provisions of the Criminal Code or under Article 2043 of the Civil Code, and cases in which anonymity is not enforceable by law.

The anonymity of the Whistleblower is also guaranteed in disciplinary proceedings when the allegation against the whistleblower is based on investigations separate and additional to the report.

On the other hand, the identity of the whistleblower may be disclosed to the whistleblower, with the whistleblower "s consent, i.e. when the charge is based primarily on the report and knowledge of the identity is therefore absolutely essential for the whistleblower's defence.

Breach of the obligation of confidentiality, including the disclosure of information on the basis of which the identity of the reporter or of the person reported or in any case involved can be deduced, is considered a breach of this procedure and is a source of disciplinary liability, without prejudice to other forms of liability provided for by the law.

In the event that the whistleblower believes he/she has suffered retaliation, even indirectly, in connection with the report made, he/she may refer the matter directly to the National Anti-Corruption Authority - A.N.A.C.

Prohibition of discrimination

Persons making a report under this Policy may not be sanctioned, dismissed (except in cases of established co-responsibility) or subjected to any discriminatory measures affecting working conditions for reasons related to the report. Discriminatory measures include unjustified disciplinary actions, harassment in the workplace and any other form of retaliation leading to intolerable working conditions.

Persons who believe they have suffered discrimination shall report it in detail to the RSIS, which, having ascertained the grounds, shall report the case to the competent Company bodies, so that the necessary measures may be taken to restore the situation and/or remedy the negative effects of the discrimination.

Any form of retaliation or discrimination affecting the working conditions of those who cooperate in the activities of verifying the grounds of the report is also prohibited.

RESPONSIBILITY OF THE WHISTLEBLOWER

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

In order to ensure the reconstruction of the different phases of the reporting process, the Whistleblowing Manager (or the Reserve Function, in case the reports have been received by him) is responsible for ensuring for a period of 5 years following the date of the report;

- the traceability of the reports and the relevant preliminary activities;
- retention of the reports and of the documentation relating to them and to the relevant verification activities, in special archives (paper/electronic).

PRIVACY AND PROCESSING OF PERSONAL DATA

Personal data will be processed in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Legislative Decree No. 196/2003 (Personal Data Protection Code), Legislative Decree No. 51/2018, implementing the Directive on the processing of personal data in police activities and, finally, Regulation (EU) No. 2018/1725 for the communication of personal data by the institutions, bodies, offices or agencies of the European Union.
Personal data acquired in the course of reporting will only be processed for institutional purposes. Reports may not be used beyond what is necessary to follow them up.
The identity of the person making the report and any other information from which this identity may be deduced, directly or indirectly, may not be disclosed, without the express consent of the person making the report, to persons other than those responsible for receiving or following up the reports, who are expressly 12inimizati to process such data. The data controller ensures their proper custody, through the application of appropriate measures to guarantee their secrecy and confidentiality.
In application of the principle of 12inimization, personal data that are clearly not useful for the processing of a specific report will not be collected or, in the event of accidental collection, will be immediately deleted.

The exercise of the data subject's rights under Articles 15 – 22 GDPR (access to data, rectification, deletion, portability, objection…) is precluded when it may result 'n 'actual and concrete prejud'ce' to the confidentiality of the identity of the reporter.

Reports and related documentation are retained only for the time necessary to process the report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure in compliance with confidentiality obligations.

Annual report

In compliance with the provisions of the regulations on the protection of personal data, the Whistleblowing Manager draws up an annual report on the correct functioning of the internal reporting systems, containing aggregate information on the results of the activity carried out following the reports received; the report is approved by the Board of Directors of the SGR and is made available to the staff members (without any personal data).

Whistleblowing training and dissemination of this Policy

All staff members must be made aware of the protection reserved to them in case of a report made in good faith, of the repercussions in case of a report made in bad faith, of the modalities of sending the report, as well as of their rights and duties related to the report itself.

In order to make the staff members aware and correctly inform them, the SGR will:

- send them a copy of this Policy via e-mail;
- update them on the occasion of each revision;
- ensure them appropriate training sessions on whistleblowing.

1. ALLEGATO 1 - MODULO PER LA SEGNALAZIONE INTERNA DELLE VIOLAZIONI

Nome e cognome del segnalante	
Data/periodo in cui si è verificato il fatto	
Descrizione dei fatti oggetto di segnalazione	
Nome/i e cognome/i del/dei soggetto/i segnalato/i	
Nome/i e cognome/i del/dei soggetto/i a conoscenza dei fatti oggetto di segnalazione (eventuale)	
Ulteriori informazioni che possono fornire utile riscontro circa la sussistenza dei fatti oggetto di segnalazione (eventuale)	
Allegati pertinenti (eventuali)	

IL SOTTOSCRITTO……DICHIARA L'ASSENZA DI QUALSIASI INTERESSE PRIVATO COLLEGATO ALLA SEGNALAZIONE.

OPPURE

IL SOTTOSCRITTO……..DICHIARA LA SUSSISTENZA DI UN INTERESSE PRIVATO COLLEGATO ALLA SEGNALAZIONE, DI SEGUITO DESCRITTO

……..……..……..…

……..……..……..……

……..……..……..…..

Luogo e data

……

Firma

2. ALLEGATO 2 – REGISTRO SEGNALAZIONI WHISTLEBLOWING

Codice segnalazione	Data segnalazione	Modalità di ricezione	Dati Whistleblower	Dati segnalato	Alti soggetti coinvolti nel processo	Controdeduzioni del segnalato	Azioni intraprese	Data chiusura processo e Conclusioni

-