Corso Matteotti, 10
20121 Milano
Italia

Info.italy@colliersglobalinvestors.com
www.colliersglobalinvestors.com

Colliers Global Investors

WHISTLEBLOWING PROCEDURE PURSUANT TO ITALIAN LEGISLATIVE DECREE 231/2001

CODE 20

VERSION 1.0

Colliers Global Investors Italy SGR S.p.A.
Capitale sociale € 1.258.748.00 i.v.
Cod fis., P. IVA e iscr.
Reg. Imp. Milano 06817000968

REA di Milano n. 1916983
Iscritta al n. 131 dell'Albo delle
Società di Gestione del Risparmio
Sezione Gestori di FIA

Corso Matteotti, 10
20121 Milano
Italia

Info.italy@colliersglobalinvestors.com
www.colliersglobalinvestors.com

Colliers Global Investors

Contents

A. REGULATORY FRAMEWORK 3
B. PURPOSE AND SCOPE OF APPLICATION 3
C. CONTENT 4
1. Definitions 4
2. Roles and responsibilities 5
2.1. ..... Board of Directors 5
2.2. ..... Whistleblowing Channel Manager 5
2.3. ..... HR Function 6
3. Protection measures 6
4. Reports 7
4.1. ..... Internal reporting channel 7
4.2. ..... Procedure and content 8
4.3. ..... Subject of the report 8
4.4. ..... Receipt of reports and preliminary obligations 9
5. Follow-up of the report 9
6. Internal investigations 9
7. Closure of the investigation 10
8. Outcome of the report 10
9. Closure 10
10. External reporting 10
11. Protection of the Whistleblower 11
D. ANNEXES AND FORMS 11

Colliers Global Investors Italy SGR S.p.A.
Capitale sociale € 1.258.748.00 i.v.
Cod fis., P. IVA e iscr.
Reg. Imp. Milano 06817000968

REA di Milano n. 1916983
Iscritta al n. 131 dell'Albo delle
Società di Gestione del Risparmio
Sezione Gestori di FIA

A. REGULATORY FRAMEWORK

- Article 6 of Italian Legislative Decree 231/2001, as further amended, governing administrative liability of legal entities, companies and associations, including those with no legal personality;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR);
- Italian Legislative Decree 196/2003, as further amended and extended (Personal Data Protection Code);
- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law;
- Italian Legislative Decree 24/2023 and the related Annex 1 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and concerning provisions on the protection of persons who report breaches of Italian national law;
- ANAC Guidelines, approved through resolution No. 311 of 12 July 2023, on the protection of persons who report breaches of Union law and the protection of persons who report breaches of Italian national law.

B. PURPOSE AND SCOPE OF APPLICATION

Italian Legislative Decree 24 of 10 March 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law and concerning provisions on the protection of persons who report breaches of Italian national law (hereafter the "Whistleblowing Decree") supplemented whistleblowing regulations and amended Legislative Decree 231/2001, repealing paragraphs 2-*ter* and 2-*quater* of Article 6.

No amendments were therefore made to the provisions (Article 6, paragraph 2-*bis*, of Legislative Decree 231/01, as amended by Article 24, paragraph 4, of Legislative Decree 24/23) according to which the "231 models" shall provide for whistleblowing channel (adopted pursuant to the new Whistleblowing Decree), the prohibition of retaliation and a disciplinary framework adopted pursuant to Article 6, paragraph 2(e), of Legislative Decree 231/01.

In accordance with the provisions of its Code of Ethics, the Company intends to promote a company culture characterised by proper behaviour and a sound corporate governance system, ensuring a workplace in which employees, collaborators, directors, supervisory and control bodies, professionals and suppliers can report any unlawful behaviour with peace of mind.

Accordingly, the Company, which has always been committed to conducting its business with honesty and integrity, recognises the importance of the whistleblowing system and, pursuant to Article 5 of the Whistleblowing Decree, adopts this Procedure, designed to provide clear information regarding the internal reporting channel, procedural formalities and the requirements for making internal and external reports.

If a recipient of this Procedure has doubts regarding how it is to be interpreted and applied, the Supervisory Board may be contacted to provide the necessary interpretative support.

This Procedure does not cover internal reporting channels for violations governed by Article 4-undecies of the Consolidated Law on Finance (TUF) and by Article 48 of Legislative Decree 231/2007 on the prevention of money laundering and terrorism, for which the specific company procedure1 should be consulted.

c. CONTENT

1. Definitions

Work-Related Context: current or past work or professional activities performed under legal relationships with the Company through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information or if they disclose it to the public or report it to the judicial or accounting authorities.

Recipients: the recipients of this Procedure are all parties which become aware of Breaches in the context of their Work-Related Context and intend to report them, including, in particular:

(i) employees of the Company (including those still in their trial periods) and personnel employed by the Company's suppliers;

(ii) candidates, where information regarding the Breaches that they intend to report has been acquired during the selection process or other pre-contractual phases;

(iii) independent contractors, including those under a coordinated and continuous collaboration contract, workers or collaborators, as well as self-employed professionals, who provide the Company with services, work or labour;

(iv) volunteers, interns, whether paid or unpaid, who render service to the Company;

(v) shareholders and persons with functions of management, directorship, control, supervision or representation, including on a *de facto* basis, within the Company;

(vi) former employees or former collaborators of the Company, where the information regarding the breaches they intend to report was acquired during the employment and/or collaboration relationship.

Person Concerned: a natural or legal person who is referred to in the internal or external report or public disclosure as a person to whom the breach is attributed or as a person who is, in any capacity, involved in the perpetration of the breach that has reported or publicly disclosed.

Reporting Person or Whistleblower: a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities.

Feedback: the provision to the Whistleblower of information on the action taken or that is expected to be taken as follow-up.

Retaliation: any behaviour, act or omission — including where merely attempted or threatened — that is undertaken in view of a report or a complaint with a judicial or accounting authority or of a public disclosure and that causes or may cause the Whistleblower or the person who made the complaint unjust harm, directly or indirectly.

[1] Whistleblowing Procedure No. 14 – Internal whistleblowing systems for regulatory breaches and management of irregularities.

Report: the oral or written communication of information on breaches.

Internal Reporting: the oral or written communication of information on breaches reported using the internal reporting channel.

External Reporting: the oral or written communication of information on breaches reported using the external reporting channel.

Follow-up: any action taken by the party tasked with managing the reporting channel to assess the accuracy of the allegations made in the reports, the outcome of the investigation and any measures adopted.

2. Roles and responsibilities

2.1. Board of Directors

The Board of Directors:

- approves this Procedure and appoints the manager of the internal reporting channel (the "Whistleblowing Channel Manager"), identified in a way that ensures that the Whistleblowing Channel Manager is not hierarchically or functionally subordinate to the Person Concerned and does not have a potential interest relating to the report. This party is also specifically trained to properly managing the reporting channel;
- receives event-based notifications for the most serious breaches and periodic (annual) notifications from the person in charge of the internal whistleblowing system;
- if, in the course of preliminary assessments, the Person Concerned is found to be potentially liable, it is considered whether to begin penalty proceedings.

2.2. Whistleblowing Channel Manager

The management company (SGR) has appointed its Supervisory Board as Whistleblowing Channel Manager, pursuant to Article 4, paragraph 2, of the Whistleblowing Decree, as it meets the necessary independence, autonomy and professionalism requirements. The Supervisory Board will manage the channel in full autonomy, including in term of expenditure. In this regard, the SGR provides the Whistleblowing Channel Manager with a specific annual budget, which may be supplemented at the request of the Whistleblowing Channel Manager and, in any event, is subject to periodic reporting obligations. In urgent cases, the Whistleblowing Channel Manager is authorised to engage the Company's resources also for a greater amount, as per the relevant resolution, subject to prior detailed written notice to the Board of Directors, and always in according with whistleblowing confidentiality requirements.

The Whistleblowing Channel Manager has full authority to make use of the available budget, without the need for authorisation, for proper assessment and management of reports, for example by awarding consulting assignments to external professionals, in accordance with company procedures.

The Whistleblowing Channel Manager is responsible for gathering reports, carrying out a thorough preliminary review of them, giving Feedback to the Person Concerned and following up on reports with the actions deemed appropriate, while ensuring the confidentiality of the Whistleblower, the Person Concerned and reporting documents.

In its capacity as Whistleblowing Channel Manager, the Supervisory Board drafts an annual report2 on the proper functioning of the internal alert procedure, as well as on the outcome of the activity carried out in response to reports received and submits it to corporate bodies.

If a report refers to the Whistleblowing Channel Manager as a Person Concerned or as a person involved in the circumstances reported, and the Whistleblower thus has well-founded reasons to believe that, if s/he makes an internal report in the manner described above, it will not be effectively followed up on, an external report may be sent to Italian National Anti-Corruption Authority (ANAC) pursuant to Article 10 below.

2.3. HR Function

The HR Function ensures that employees are adequately protected against direct or indirect retaliation, discrimination or other unfair behaviour targeting them, ensuring an environment respectful of workers' dignity.

In addition, if the Person Concerned is an SGR employee (intern, employee or quasi-employee), at the indication of the Whistleblowing Channel Manager, and on the basis of the Board of Director's decision to begin penalty proceedings, the HR Function begins the disciplinary procedure.

3. Protection measures

Through this Procedure, the tools adopted and the internal control system, the SGR guarantees the following protection measures:

- responsibility entrusted to a person specifically trained for managing the whistleblowing channel;
- confidentiality of the identity of the Whistleblower, the Person Concerned and any person referred to in the report, as well as of the content of the report and of the related documentation;
- confidentiality of the information from which said identity may be directly or indirectly deduced;
- possibility to report in anonymous form;
- an internal whistleblowing channel for written or oral reports, in addition to physical meetings;
- prohibition of retaliation, in particular toward the Whistleblower and the facilitators;
- sending the acknowledgement of receipt of the report to the Whistleblower within seven days of that receipt;
- providing feedback within three months of the date of the acknowledgement of receipt or, in the absence of such acknowledgement, within three months from the expiry of the seven-day period after the report was made;
- communication and information on the procedures and requirements to submit internal reporting;
- supervision of compliance with the measures adopted through this Procedure, as well as of the risk of breaches of the prohibition of any retaliation.

[2] The outcome may also be reported in a dedicated section of the Supervisory Board's annual report.

4. Reports

4.1. Internal reporting channel

To ensure full implementation of the provisions of the Whistleblowing Decree, the SGR has set up a specific **internal channel** for receiving and managing whistleblowing reports, represented by a cloud-based **IT platform** called "Sibilus", created by Testudo S.r.l., a certified supplier specialised in designing and developing whistleblowing management IT software (the "Supplier"). This channel uses **cryptography** to ensure the confidentiality of the Whistleblower, the Person(s) Concerned and any other parties mentioned in the report (e.g., potential witnesses), as well as of the content of the report and the related appended documentation, in accordance with Article 4 of Legislative Decree No. 24/2023 (the "**Platform**" or the "**Software**").

The Platform operates in the cloud on specific dedicated servers, distinct from those of the SGR, located within the European Union and protected by state-of-the-art IT protection measures. The Supplier also guarantees the physical security of the servers. In addition, the Platform provides for the Whistleblowing Channel Manager access by multiple-factor authentication, following registration made directly by the Supplier. The related credentials for access to the Platform are provided solely to the Supervisory Board in its capacity as internal Whistleblowing Channel Manager during registration of the account and are thus known solely to it.

With regard to the Whistleblower, the Platform is easily accessible from any device using a simple Internet connection, as no registration is necessary. The Whistleblower is progressively guided by the Platform in submitting the report. Once a report has been properly submitted, the Platform automatically and randomly generates a **numerical code** ("**token**") that unambiguously identifies the report. To further ensure the confidentiality of the report, Whistleblowers are also asked to generate a password of their choosing. It should be noted that neither the SGR nor the Supplier can view this data (token and password), nor can they of course recover it. Only the Whistleblower is therefore in possession of the data needed to monitor the status of the report.

Reports may also be sent via the Platform in **written** or **oral** form, or by requesting a **physical meeting**.

Anyone can access it by connecting to the website **https://collierssgr.sibilus.io/** through a specific section dedicated to whistleblowing on the Company's website, which redirects directly to the selected Platform.

If a meeting is requested by the Whistleblower, the Whistleblowing Channel Manager arranges for the activities necessary to enable a meeting within an appropriate timeframe (if possible, within ten days of the request) and in a protected environment that does not jeopardise the confidentiality of the Whistleblower, but facilitates dialogue.

The Whistleblower's statements, made verbally during the meeting with the Whistleblowing Channel Manager, are documented through audio recording and preparation of specific minutes, to be signed by all those present (firstly by the Whistleblower) and to be uploaded to the Platform by the Whistleblowing Channel Manager.

Once the report has been properly submitted, the Platform automatically and randomly generates a **code** ("token") and asks the Whistleblower to assign a **password** to the report; by entering the token and password into another specific section of the Platform ("**Find Report**"), the Whistleblower may:

a) **monitor** the status of the report at any time;

b) **contact**, where desired, the Whistleblowing Channel Manager.

The Whistleblower is strongly advised to **store** and **keep** the report code and password and check the Platform often to respond to any questions or requests for additional information from the Whistleblowing Channel Manager. It bears recalling that the token and password cannot be recovered by either the SGR or the Supplier **in any way**. Accordingly, if they are lost, the Whistleblower will no longer be able to access the report submitted and will be

required, where desired, to submit a new one (to which a new token will be assigned and a new password will need to be indicated).

Where whistleblowing reports are submitted in a way other than use of the Platform, the party who receives the report must promptly enter it into the Platform using the specific section, "**Submit Report**". It should be noted that, where the content of the report is not known to the addressee (e.g., because it is submitted in a sealed envelope), the addressee must immediately deliver the report to the Whistleblowing Channel Manager, who will read it and enter it into the Platform through the "Submit Report" section. Upon receiving a report outside the Platform (e.g., via e-mail), the Whistleblowing Channel Manager immediately enters it into the Platform using the aforementioned "Submit Report" section.

Once the report has been uploaded onto the Platform, the Whistleblowing Channel Manager must provide the Whistleblower with the **acknowledgement of receipt** of the report through the Platform within the following seven (7) days. The party who has received the report outside the Platform is required to maintain the utmost confidentiality regarding the information contained in the report, in particular with regard to the identity of the Whistleblower, the Person Concerned and any persons mentioned in the report, as well as the subject and content of the report.

4.2. Procedure and content

The report, however delivered, must be sufficiently detailed, made in a way that provides, as thoroughly as possible, the information set out below, along with any relevant documentation:

- description of the breach (event, how the Whistleblower became aware of it, date and place);
- company structures/organisational units involved;
- parties involved (Person Concerned and any other parties involved in the events);
- any third parties involved or potentially damaged.

Anonymous reports will also be taken into account, provided that they are duly circumstantiated and detailed.

However, it should be noted that anonymous reports may limit the possibility for the Whistleblowing Channel Manager to further investigate and effectively assess the content thereof. The guarantee of anonymity is limited in the cases provided for by law and whenever it conflicts with the right to a defence of the parties involved.

NOTE: *It is prohibited to send reports for the mere purpose of retaliation against the Company or its employees, collaborators, consultants, customers, suppliers, etc., or for the mere purpose of intimidation. It is also prohibited to misuse the whistleblowing system to engage in acts of defamation or libel against the Person Concern and/or the Company or to submit unfounded reports made with wilful misconduct and/or gross negligence.*

4.3. Subject of the report

The following facts may be reported:

- predicated offences as per Italian Legislative Decree 231/2001;
- breaches of the Organisation, Management and Control Model adopted by the SGR pursuant to Article 6 of Legislative Decree 231/2001;
- breaches falling within the scope of application and concerning the following areas: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and

nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and security of network and information systems;

- acts or omissions affecting the financial interests of the European Union;
- acts or omissions relating to the internal market, of the European Union, including breaches of competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

4.4. Receipt of reports and preliminary obligations

If a report is made via the Software, the Software itself will provide all the confidential protocol numbers, in accordance with applicable legislation.

Once the report is received, in written or oral form, the Whistleblowing Channel Manager will begin the preliminary analysis, and will in particular verify the significance and degree of detail of the report and properly record and storage the report and any appended documentation, also ensuring traceability and proper storage in the subsequent phases.

Within seven days of the date of receipt, the Whistleblowing Channel Manager must submit the acknowledgement of receipt to the Whistleblower.

5. Follow-up of the report

The in-depth assessment and analysis phase takes the form of specific analyses, evaluations and verifications of the reports that make it possible to identify, analyse and assess the elements, seeking to confirm that the reported events are well-founded.

After the preliminary analysis, the following possible actions are taken:

- if the report is significant and sufficiently detailed, it is taken into charge and the activities deemed necessary are carried out, such as, for example, further analyses, requests for information and internal investigations;
- if the report is significant but it is not sufficiently detailed, it is taken into charge and the activities deemed necessary are carried out, such as, for example, acquisition of additional documentation, requests for information and internal investigations;
- if the report is not significant, the Whistleblower is informed and the report is closed;
- if the report has been submitted in bad faith, in concert with the HR Function, it is considered whether disciplinary proceedings should be initiated against the Whistleblower.

6. Internal investigations

The investigation and assessment process must ensure the following elements:

- thorough reconstruction of the facts, supported by documentary evidence;
- application of all rules and precautions to guarantee the confidentiality and/or anonymity of the Whistleblower (retention of documentation, management of the reporting process, records of testimony);
- all those involved in the investigation must be informed of the statements made and the evidence acquired against them, and must be put in a position to be able to respond to them;
- detailed report on the outcome of the investigation;

- ensure that the investigation is thorough and has a reasonable duration.

During this phase, the Whistleblowing Channel Manager may decide, where necessary, to avail itself of the support of external professionals in view of the complexity of the subject of the report, while always ensuring the protection of the confidentiality aspects required by the Whistleblowing Decree.

7. Closure of the investigation

The investigation may end with:

- a **negative outcome**: in this case, the report is closed;
- a **positive outcome**: in this case, the outcome of the checks performed is sent to the Board of Directors in order to allow the Company to adopt the necessary countermeasures and any disciplinary sanctions, while in any case ensuring the confidentiality requirements imposed by the Whistleblowing Decree.

At the end of the investigation, a final report is drawn up that shall:

- summarise the investigation process and the evidence collected;
- illustrate the conclusions drawn;
- provide recommendations and suggest actions to be implemented to remedy the breaches identified and ensure that the latter do not occur in the future.

All the reports will be classified as "restricted", i.e. with the highest degree of confidentiality.

8. Outcome of the report

The measures taken by the Board of Directors are reported to the Whistleblowing Channel Manager to complete the file on the Report.

The Whistleblowing Channel Manager provides a feedback to the report within three months of the date of acknowledgement of receipt or, in the absence of such acknowledgement, within three months from the expiry of the seven-day period after the report was made.

9. Closure

The reports and the related documentation are stored within the Platform by the Whistleblowing Channel Manager for the time needed to process the report and, in any way, for no more than five years from the date of notification of the final outcome of the reporting procedure, in accordance with the confidentiality requirements set out in Article 12 of the Whistleblowing Decree and the principle laid down in Article 5, paragraph 1(e), of Regulation (EU) 2016/679.

10. External reporting

External reports may be sent to ANAC in written form, through the IT platform, or in oral form through dedicated telephone lines or voice messaging systems made available and published on the authority's website (www.https://www.anticorruzione.it/).

The Whistleblower may file an external report if, upon submission, one of the following conditions are met:

- its Work-Related Context does not provide for the mandatory activation of an internal reporting channel or the latter, even if it is mandatory, is not operating or, even it has been activated, does not comply with the provisions of the Whistleblowing Decree;
- the Whistleblower has already filed an internal report and it has not been followed up;

- the Whistleblower has reasons for believing that, if an internal report were filed, it would not be effectively followed up or that the same report could determine the risk of retaliation;
- the Whistleblower has reasons for believing that the breach may constitute an imminent or clear danger to the public interest.

11. Protection of the Whistleblower

If a report has been made in good faith, in accordance with the principles of the Whistleblowing Decree, Code of Ethics, Organisation Model and this Procedure, regardless of the reporting channel used, the Whistleblower is always ensured protection against acts of "retaliation", including merely attempted or threatened retaliation, undertaken due to the report, complaint to a judicial or accounting authority or public disclosure.

The following circumstances, when occurring as a result of a reporting, qualify as retaliation:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work;
- reduction in wages, change in working hours;
- withholding of training or any restriction to access it;
- a negative performance assessment or employment reference;
- adoption of disciplinary measure, other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination or any disadvantageous treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that worker would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for the provision of goods or services;
- cancellation of a licence or permit;
- request for psychiatric or medical referrals.

D. ANNEXES AND FORMS

This procedure does not include any forms and/or annexes.