MANAGEMENT OF REPORTS

(*Whistleblowing*)

Reviews	Date	Description Edit
0	15/12/2023	First adoption
1	11/03/2026	Removal to the email reporting channel

Purpose 2
Definitions 2
Addressees and scope of application 3
Subject of the report 4
PROHIBITED REPORTS 4
BONA FIDE REPORTS 5
REPORTS IN BAD FAITH 5
ANONYMOUS REPORTS 5
REPORT channels 6
Description of proceedings 7
SENDING THE REPORT 7
Online platform (priority reporting tool) 7
Ordinary/recorded mail 7
SENDING THE ALERT TO A PARTY OTHER THAN THE OPERATOR 8
MANAGEMENT OF POSSIBLE CONFLICTS OF INTEREST 8
VERIFICATION OF THE VALIDITY OF THE REPORT 9
SUBSEQUENT ACTIVITIES 10
CONSERVATION 10
CORRECTIVE AND MONITORING ACTIONS 11
Protections for the reporter 12
PROTECTION OF CONFIDENTIALITY 12
PROTECTION FROM RETALIATION 13
LOSS OF PROTECTIONS AND LIABILITY OF THE REPORTER 14
RESPONSIBILITY OF THE THIRD PARTY REPORTER 15
Processing of personal data 16
Adoption and updating of the procedure 17
Information and training 17

Purpose

This procedure provides tools and operational indications for the transmission, receipt and analysis of reports as defined below, in compliance with the relevant legislation and guidelines:

- Article 6, paragraph 2-bis of Legislative Decree No. 231/2001 (as amended by Law No. 179/2017 and amended by Legislative Decree 24/2023), which provides for the indication, within the Model adopted pursuant to Decree No. 231, of the internal reporting channel defined by the entity, the prohibition of retaliation against the reporter and an adequate disciplinary system;
- Legislative Decree 24/2023, which transposed EU Directive 2019/1937 concerning the protection of persons who report breaches of national or EU regulatory provisions, which harm the public interest, the integrity of the public administration or the private entity, of which they have become aware in the context of their work, whether public or private;
- ANAC Guidelines (Resolution No. 311 of 12 July 2023);
- Confindustria Guidelines 'New discipline Whistleblowing - Operational guide for private entities' - October 2023;
- EU Data Protection Regulation 2016/679 ('GDPR')

Definitions

Company/Entity	Flow-meter S.p.A.
Report	Written or oral communication of information on violations, including reasonable suspicions that violations may have been committed within the Company as well as elements concerning conduct aimed at concealing such violations.
Reporter	Individuals who report violations acquired in the course of their work or in the course of collaboration or business relations with the Company, including collaborators, interns, consultants, customers, agents, suppliers and *business partners.*
Reported	Person mentioned in the report, understood as the person to whom the breach is attributed or as a person otherwise implicated in the reported breach.
Facilitator	Person assisting the reporter in the r e p o r t i n g process, operating within the same work context.

Report Manager and/or Manager	This is the person appointed by the Company, autonomous and specifically trained, in charge of managing the reports made through the internal reporting channel, identified in the Supervisory Board (SB) appointed pursuant to Legislative Decree No. 231/2001.
Model 231	Organisational, Management and Control Model adopted by the Company, i.e. a structured and organic system of principles, internal rules, operating procedures and control activities, adopted for the purpose of preventing conduct liable to give rise to the types of offences and crimes provided for in Legislative Decree 231/2001.
Platform	*A web* platform that complies with the regulations set out in Legislative Decree 24/2023, as well as EU Regulation 2016/679 (GDPR), which allows the whistleblower to make reports and which guarantees the confidentiality of the identity of the whistleblower, the reported person, the content of the report and the related documentation.
Not relevant report	Any communication concerning conduct that does not constitute a violation. All those communications that, on the basis of the vagueness of their contents, do not allow for adequate verification are also considered as non-relevant reports.
Reporting in bad faith	Any communication that proves to be unfounded on the basis of objective elements and that proves, again on the basis of objective elements, to have been made solely for the purpose of causing harm to the reported person and/or the Company.

Addressees and scope of application

This procedure applies to:

a) **top management**, members of corporate bodies and control bodies of the COMPANY;

b) **the REPORT MANAGER** appointed by the COMPANY for the management of REPORTS (hereinafter also the 'REPORT MANAGER' or the 'MANAGER');

c) **employees** of the COMPANY irrespective of their contractual classification (even if in probationary period) and to persons who are even only temporarily in working relations with the COMPANY although they are not employees (e.g.: volunteers and trainees - paid and unpaid),

d) **those who cooperate and collaborate** with the COMPANY - in any capacity - in the pursuit of its objectives (e.g. self-employed workers, agents, freelancers and consultants in the performance of their work),

e) the addressees of the MODEL 231 adopted by the COMPANY (in addition to the

subjects mentioned in the previous points) also **customers, suppliers, business** partners and any further categories of subjects that the administrative body in agreement with the Supervisory Body may establish in relation to the legal relations established by the COMPANY).

The REPORT can be made:

- when the legal relationship is ongoing;
- when the legal relationship has not yet started, in the event that the REPORTER has become aware of a breach during the selection process or at other pre-contractual stages;
- after the termination of the legal relationship, in the event that the REPORTER becomes aware of violations before the termination of the relationship (e.g. pensioners).

Subject of the report

The REPORT can concern behaviours, actions or omissions that damage the integrity of the COMPANY, in particular **illicit conducts relevant to the Legislative Decree 231/2001**; as well as behaviours or situations, also not directly constituting a crime, however contrary to the Model 231 of the COMPANY, to the Ethical Code, or to regulations, directives, *policies* and internal procedures adopted by the COMPANY and relevant to the Legislative Decree 231/2001.

Both violations committed and violations not yet committed that the REPORTER reasonably believes could be committed on the basis of concrete elements may be reported. Elements concerning conduct aimed at concealing the above violations may also be reported.

PROHIBITED ALERTS

REPORTS are prohibited and therefore considered irrelevant and not actionable:

- relating to disputes, claims or **demands linked to an interest of a personal nature on the part of** the REPORTER that relate exclusively to his/her individual work relations with colleagues or superiors (e.g. labour disputes, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker or hierarchical superiors);
- **based on mere suspicions** or rumours concerning personal facts not constituting an offence, or in any case manifestly unfounded and/or acquired only on the basis of unreliable indiscretions or rumours (so-called "rumours");

- having a **purely defamatory** or slanderous **purpose** (e.g. reporting information to discredit a person's reputation);
- having insulting tones or containing **personal offences or moral judgments**, intended to offend or harm the honour and/or personal and/or professional decorum of the person or persons to whom the reported facts are referred (e.g. reports containing derogatory/offensive words);
- relating to information that is **already fully in the public domain** (e.g. information reported in the media - newspapers, websites - and judgments);
- of violations already **regulated** in **European Union** directives and regulations and in the implementing provisions of the **Italian legal system** that already guarantee **specific reporting procedures** (e.g. violations in the banking sector. The Consolidated Banking Act provides for *ad hoc* internal reporting systems for violations and the Procedure for reporting to the Supervisory Authorities).

REPORTS that are considered irrelevant, and therefore inexecutable, will be archived.

BONA FIDE REPORTS

The REPORTER is invited to make REPORTS that are as circumstantial as possible and offer as many elements as possible, in order to allow due verification and adequate feedback.
After having made a REPORT, the REPORTER who detects any errors may immediately inform through the same channel to which the REPORT was made.

REPORTS IN BAD FAITH

REPORTS shall be deemed to have been made in bad faith if they prove to be deliberately futile, false or unfounded, with defamatory content, or in any case with deliberately erroneous or misleading information, for the sole purpose of damaging the COMPANY, the REPORTED or other persons concerned by the REPORT.
In such a case, the COMPANY reserves the right to implement appropriate actions - including through the adoption of appropriate disciplinary sanctions - against the REPORTER.

ANONYMOUS REPORTS

Anonymous REPORTS are permitted and considered admissible provided they are adequately substantiated and detailed.
These reports limit the possibility of carrying out an effective investigation, as it is impossible to establish a smooth information channel with the REPORTER. Therefore, the REPORTS MANAGER considers, among the relevant factors for assessing the anonymous report, the seriousness of the reported breach, the credibility of the facts represented and the possibility of verifying the truthfulness of the breach from reliable sources.
All whistleblowers are also encouraged to declare their identity to ensure greater credibility and effectiveness than an anonymous report.
Should the REPORTER choose to indicate his or her personal details, confidentiality is nevertheless guaranteed, as further specified below.

REPORT channels

The channels are as follows:

1. Computer platform: https://flowmeter.cpkeeper.online/keeper/available-configuration-links
2. Ordinary/recorded mail - for the attention of the Supervisory Board at the Company's registered office in Via del Lino 6, 24040 Levate (BG) - Italy.
   In this case, the Report should be placed in two sealed envelopes, including: i) in the first one, the identification data of the person making the report, together with an identity document (should not wish to remain anonymous); ii) in the second one, the subject of the report. Both envelopes must then be placed in a third envelope bearing, on the outside, the words "confidential to the Supervisory Board".

The PLATFORM is to be considered the priority and preferred internal channel.

The REPORTER may also request, through the channels indicated above, a confidential meeting with the MANAGER of the alerts, who must ensure that it takes place (in a suitable place to allow the confidentiality of the REPORTER) within a period of 15 days. With the REPORTER'S consent, the meeting may be recorded by a device suitable for storage and listening. Alternatively, the meeting is documented by means of minute which the REPORTER may verify, rectify and confirm. A copy of the minute is handed over to the REPORTER.

.

Description of proceedings

SENDING THE REPORT

Online platform (priority reporting tool)

The PLATFORM allows reports to be made in **writing or orally, with the possibility of recording voice messages** and guaranteeing the confidentiality of the identity of the REPORTER and the content of the REPORT.

To make a report, the reporting REPORTER goes to the link https://flowmeter.cpkeeper.online/keeper/available-configuration-links and fills in the fields provided, taking care to enter all the mandatory information required so that the report is as comprehensive and clear as possible, attaching any supporting documentation where appropriate.

The system is designed to allow the sending of reports without the need to register or declare one's personal details. The REPORTER can, in fact, leave a message through the page anonymously and need not provide an e-mail address or telephone number.

Upon completion of the Report Form, the **REPORTER must note down the Unique Identification Code and Password (which uniquely identifies the REPORT), which is** automatically generated by the PLATFORM and cannot be retrieved or duplicated in any way. These credentials will enable the REPORTER to monitor the processing status of its REPORT and, if necessary, interact with the MANAGER of the reports.

Within 7 days after receipt of the REPORT, the MANAGER shall send the REPORTER an acknowledgement of receipt of the REPORT.

Ordinary/recorded mail

If it is not possible to use the *online* platform, the report can be sent via:

- Ordinary/recorded mail - for the attention of the Supervisory Board at the Company's registered office in Via del Lino 6, 24040 Levate (BG), in three envelopes. The REPORT must be placed in **two sealed envelopes**, including: i) in the first, the identification data of the REPORTER, together with an identity document (in the event that he/she does not wish to remain anonymous); ii) in the second, the subject of the report. Both **envelopes** must then be placed in a **third envelope marked "reserved for the REPORT MANAGER" on the outside**.

It is recommended to clearly indicate in the subject line of the REPORT that it is a report for which you intend to keep your identity confidential and benefit from the protections provided for in the event of any retaliation suffered as a result of the REPORT. This specification allows, where the REPORT is mistakenly received by a person who is not competent or through a channel other than those specifically provided for, the timely transmission by the latter to the person authorised to receive and manage *Whistleblowing* reports.

SEND OF REPORT TO A ENTITY OTHER THAN THE MANAGER

Any person who receives a REPORT, in whatever form (oral or written), falling within the scope of this procedure, which is not addressed to him or which has been sent erroneously, shall promptly, and in any event within 7 days of its receipt, forward it to the MANAGER OF REPORTS, through the internal reporting channel and in the manner set out in this paragraph, simultaneously notifying the REPORTER (if known) of the transmission.

The addressee of the erroneous REPORT may not retain a copy of the original and must delete any copies in digital format, refraining from undertaking any independent analysis and/or investigation.

It is however bound by the confidentiality of the identity of the REPORTER, of the persons involved and/or in any case mentioned in the REPORT, of the content of the SIGN and of the relevant documentation.

Failure to report a received REPORT, as well as breach of the duty of confidentiality, constitutes a breach of this procedure and may result in disciplinary action being taken by the COMPANY.

MANAGEMENT OF POSSIBLE CONFLICTS OF INTEREST

In the event that the MANAGER of the REPORT coincides with the REPORTER or is otherwise a person involved or affected by it, the SIGNAL shall be addressed to the Chairman of the Board of Directors in order to guarantee its effective, independent and autonomous management, in compliance with the confidentiality obligation provided for by the applicable regulations.

VERIFICATION OF THE VALIDITY OF THE REPORT

The MANAGER OF THE REPORTS shall verify the validity of the circumstances represented in the REPORT in compliance with the principles of impartiality and confidentiality by carrying out any activity deemed appropriate, including the personal hearing of the REPORTER and of any other person who may report on the facts reported.

As a precautionary measure, the MANAGER assesses the existence of the essential requirements of the REPORT in order to assess its admissibility and thus be able to grant the REPORTER the envisaged protections (specified below).

The MANAGER must therefore verify that

a) the REPORTER is a person entitled to make the REPORT.
   If the requirement does not exist, the REPORT will be taken into consideration by the MANAGER, but the protections provided for by Legislative Decree 24/2023 and in particular the protection of the confidentiality of the REPORTER will not be guaranteed.
b) the subject of the REPORT falls within the scope of the discipline. Should the requirement not be met, the MANAGER shall proceed to file the REPORT received.

Based on the results of the preliminary verifications, the MANAGER:

1. may decide not to exercise its investigative powers (by filing the REPORT) if it is manifestly unfounded due to the absence of factual elements justifying further investigation, if the general content of the REPORT is such that it does not allow the understanding of the facts, or if it considers that the nature and content of the REPORT is irrelevant according to the reference legislation, or if it does not contain elements of risk for the COMPANY and its *stakeholders*, informing the REPORTER and the Chairman of the Board of Directors of the outcome;
2. may decide to exercise its investigative powers according to the level of urgency resulting from the assessment of the risks that may arise from the nature of the REPORT and inform the REPORTER of the outcome.

The exercise of investigative powers may provide for the carrying out of in-depth investigations with the involvement of persons inside or outside the COMPANY who are competent in the matter.

Should what has been reported not be adequately substantiated, the MANAGER may request additional elements from the REPORTER through the dedicated channel, or even in person, if the REPORTER has requested a direct meeting.

In the event of the involvement of other structures/functions/third parties for the performance of investigative activities, they will be informed only of the content of the

REPORT, excluding all references from which it is possible to trace, even indirectly, the identity of the REPORTER. Those involved in support of the REPORTER MANAGER are burdened with the same duties of conduct aimed at ensuring the confidentiality of the REPORTER.

SUBSEQUENT ACTIVITIES

If the outcome of the checks carried out establishes the admissibility and justification of the REPORT, the Supervisory Board shall provide feedback to the REPORTER, giving an account of the measures envisaged or adopted or to be adopted to follow up the REPORT and the reasons for the choice made.
The REPORTER shall be informed of the outcome of the REPORT within a period of three months from the date of the acknowledgement of receipt or, in the absence of such notice, within three months from the expiry of the period of seven days from the submission of the REPORT.
Therefore, upon expiry of the three-months period, the REPORT MANAGER may notify the REPORTER:

- the filing of the REPORT, stating the reasons therefor;
- the establishment of the validity of the REPORT and its transmission to the competent internal bodies;
- the activity carried out so far and/or the activity it intends to carry out (feedback on the nature of the investigation, if still ongoing).

In addition, the REPORTING MANAGER shall forward his opinion to the Chairman of the Board of Directors so that he can identify the most appropriate measures to be taken as a consequence of the incident, including - if the prerequisites are met - disciplinary measures against the perpetrators of the offences and/or irregularities, already provided for by the CCNL.
Likewise, the MANAGER shall ensure to it, by forwarding an appropriate report to the Chairman of the Board of Directors, if he ascertains that the REPORT, which has proved to be unfounded following the appropriate investigations, appears to have been forwarded on account of a conduct of the REPORTER vitiated by wilful misconduct or gross negligence, so that the appropriateness of taking the appropriate disciplinary measures against the same may be assessed.

CONSERVATION

The REPORT and its documentation are kept by the MANAGER OF THE REPORTS (on the PLATFORM for

Reports received via this channel or in dedicated archive for reports received by ordinary mail), in order to ensure complete traceability of the process of handling the REPORT and the activities carried out.

All documentation shall be kept for as long as necessary for the management of the REPORT and, in any case, for no longer than five years from the closure of the REPORT, unless a judicial or disciplinary action is instituted against the REPORTED or the WHISTLEBLOWER who made false or defamatory statements. In this case, the report and the relevant documentation shall be kept until the conclusion of the proceedings and the expiry of the time limit for lodging an appeal.

After the expiry of the aforementioned time limits, the REPORT and its documentation will be deleted or anonymised.

The access credentials to the PLATFORM are known only to the MANAGER OF THE REPORT or by expressly authorised persons.

Any paper documents are stored at an identified location whose access is permitted only to the MANAGER or to expressly authorised persons. ORAL REPORTS and those made through face-to-face meetings are:

- documented in writing by means of a detailed transcript of the conversation. The REPORTER may verify, rectify and confirm the contents of the transcript. A copy of the signed transcript is given to the reporter;
- stored, with the consent of the REPORTER within a device suitable for the conservation and listening.

CORRECTIVE AND MONITORING ACTIONS

If the analyses on the areas and business processes examined reveal the need to formulate recommendations for the adoption of appropriate remedial actions, it is the responsibility of the Chairman of the Board of Directors to assess and define, together with the Functions concerned and the Managers of the areas/processes subject to verification, a plan of corrective actions for the removal of the critical issues detected; as well as to ensure their implementation within the defined timeframe, informing the MANAGER who monitors the status of implementation of the actions.

Periodically, the MANAGER verifies that all the REPORTS received have been processed, duly forwarded to the appropriate recipients and reported in accordance with this procedure.

Protections for the reporter

The protections afforded to the REPORTER can only be guaranteed by the COMPANY if the indications contained in the present procedure are complied with. No protection is granted to the REPORTER in the event that he/she has contributed to the commission of the unlawful conduct.

The protections afforded to the REPORTER are also extended:

- to the FACILITATOR;
- persons in the same work environment as the REPORTER with a stable emotional or kinship link up to the fourth degree;
- to the REPORTER's work colleagues with whom they have a regular and current relationship

PROTECTION OF CONFIDENTIALITY

The COMPANY, in setting up and implementing its internal reporting channel, guarantees the confidentiality of the identity of the REPORTER, the REPORTED and of any other persons involved, as well as of the content of the REPORT and of the related documentation.

REPORTS may not be used beyond what is necessary to adequately follow them up. Confidentiality is also guaranteed in the case of reports made orally via telephone lines or, at the REPORTER's request, via a direct meeting with the REPORT MANAGER. Confidentiality is also guaranteed to whistleblowers before the commencement or after the termination of employment, or during the probationary period, if such information was acquired in the context of employment or in the selection or pre-contractual phase.

The breach of the obligation of confidentiality may lead to the imposition of administrative fines by ANAC against the person concerned, as well as to the adoption of disciplinary measures by the COMPANY, in line with the provisions of the disciplinary system of the 231 Organisational Model.

It is only possible to disclose the identity of the REPORTER with the latter's express consent and after written notification of the reasons for such disclosure, in the following cases (expressly provided for in Legislative Decree 24/2023)

- in disciplinary proceedings, where the disclosure of the identity of the REPORTER is indispensable for the defence of the person charged with the disciplinary offence;
- in proceedings instituted following alerts where such disclosure is also indispensable for the defence of the person concerned.

Therefore, the AWARENESS MANAGER guarantees the confidentiality of the identity of the BEARER and of the SUBJECT, except where strictly necessary for the exercise of the investigative power and except, for example, in cases where: (i) there is an express legal provision or a public authority order requiring the disclosure of the identity of the SUBJECT or (ii) during the preliminary investigation phase - due to the features of the investigations to be carried out

- the MANAGER OF THE REPORT needs to communicate the personal details of the NOTIFIED person to other structures/internal functions/third parties; (iii) it is necessary to involve the head of the corporate function in charge of disciplinary proceedings if the REPORT is deemed well founded in order to assess the appropriate disciplinary actions.

PROTECTION FROM RETALIATION

In any event, no disciplinary proceedings may be commenced in the absence of precise and objective evidence that the REPORT is well-founded.

Furthermore, any conduct, act or omission, even if only attempted or threatened, occurring at work by reason of the REPORT and causing or likely to cause the REPORTER, directly or indirectly, unjust damage is prohibited.

Prohibited retaliatory measures include, but are not limited to:

- dismissal, suspension or equivalent measures;
- downgrading or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- demerits or negative references;
- adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;

- damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- early termination or cancellation of the contract for the supply of goods or services;
- cancellation of a licence or permit

To enjoy protection from retaliation, it is necessary that:

- the REPORTER has reasonable and well-founded grounds to believe that the REPORT is true (mere supposition or rumour is not sufficient) and falls within the objective scope of the regulation;
- the REPORT was made in the manner described in this procedure;
- there is a close connection (relationship of consequentiality) between the REPORT and the adverse act/behaviour/omission suffered by the REPORTER.

Alleged retaliation, even if only attempted or threatened, must be reported exclusively to ANAC, which is entrusted with the task of ascertaining whether it is a consequence of the REPORT.

Where the REPORTER proves that he/she has carried out a REPORT and that he/she has suffered retaliation because of it, the burden of proof lies with the person who has carried out such retaliatory conduct and acts. It is the latter, therefore, who must prove that the action taken is in no way connected to the REPORT.

If the Authority ascertains the retaliatory nature of acts, measures, behaviour, omissions adopted, or even only attempted or threatened, this will result in their nullity and the application of a pecuniary administrative sanction.

Liability is also incurred by the person who has suggested or proposed the adoption of any form of retaliation against the REPORTER, thereby producing an indirect negative effect on his position.

LOSS OF PROTECTIONS E LIABILITY OF THE REPORTER

At the time of the report, the REPORTER must have reasonable grounds to believe that the information reported is true. The protections provided for by Legislative Decree 24/2023, in fact, do not apply when the criminal or civil liability of the REPORTER is established for offences of defamation or slander, or in any case for the same offences committed with the reporting to the judicial or accounting authorities, committed with malice or negligence

serious. In the event of a loss of protection, in addition to the application of disciplinary sanctions, an administrative sanction of between EUR 500 and EUR 2,500 is envisaged by ANAC.

The aforementioned protections should not be understood as a form of impunity of the REPORTER: the criminal and disciplinary liability of the employee REPORTER remains valid in the event of REPORT carried out in bad faith or with gross negligence, as well as the obligation to compensate (*pursuant to* Article 2043 of the Civil Code) for any damage caused by the aforementioned unlawful conduct. Any form of abuse of this procedure, such as manifestly opportunistic REPORTS and/or those made for the sole purpose of damaging the REPORTED PERSON or other persons, and any other hypothesis of improper use or intentional exploitation of the institution covered by this procedure, shall also give rise to liability in disciplinary and other competent fora.

By way of example only, the following penalties may be imposed on the REPORTER in the event of negligence:

- verbal reprimand, written warning, financial penalty, suspension from service, dismissal for managers;
- verbal warning, written warning, fine, suspension from service, dismissal with or without notice for employees.

Specifically, in the event that, at the end of the process of ascertaining the REPORT, objective elements emerge proving the sending of reports in bad faith or with gross negligence, the MANAGER shall promptly inform the Chairman of the Board of Directors and the competent corporate functions so that they can take the appropriate measures.

At the same time, the REPORTED shall be made aware of the presence of such breaches so that, where appropriate, he/she may be in a position to exercise his/her right of defence and, if necessary, to take appropriate action against the NOTIFIER.

RESPONSIBILITY OF THE THIRD-PARTY REPORTER

The criminal and civil penalties resulting from the offences and abuses referred to in the preceding paragraph shall also apply to third parties other than the COMPANY.

Moreover, any offence or abuse of this procedure committed by third parties with whom the COMPANY entertains contractual relationships (such as customers, suppliers, consultants/external collaborators, commercial *partners,* etc.), is sanctioned according to what is provided for by specific contractual clauses included in the relevant contracts. Such clauses may provide, by way of example only, for the right to

termination of the contract and/or payment of penalties. Penalties may also entail the prohibition of establishing new contractual relationships with the parties concerned.

In addition to the sanctions provided for by Leg. Decree 24/2023, the non-compliance with the principles, behavioural rules and control measures contained in this procedure entails the application of the disciplinary system contained in the Organisation, Management and Control Model adopted by the COMPANY pursuant to Leg. Decree 231/2001.

Processing of personal data

The processing of personal data acquired during the management of REPORTS shall be carried out in accordance with Regulation (EU) 2016/679 (GDPR) and Legislative Decree no. 196 of 30 June 2003 (ss. mm. and ii.).

The data collected are exclusively those necessary for the management of the REPORT. The data shall be kept in a form that enables the identification of the persons concerned for the time necessary for the processing of the specific REPORT and in any case no longer than five years from the date of the communication of the final outcome of the REPORT procedure.

Personal data that are manifestly not useful for the processing of a specific REPORT shall not be collected or, if accidentally collected, shall be deleted immediately.

The processing of personal data relating to the receipt and management of REPORTS is carried out by the COMPANY as data controller, in compliance with the principles set out in Articles 5 and 25 of the GDPR, providing appropriate information to the REPORTER and the persons involved pursuant to Articles 13 and 14 of the GDPR, as well as adopting appropriate measures to protect the rights and freedoms of the persons concerned. In particular, the specific purposes of data processing are explained in the information notice made available to anyone accessing the PLATFORM to make the REPORT (CP Keeper portal).

The COMPANY has specifically appointed and instructed authorised persons to process personal data, also in accordance with Articles 5, 24, 29 and 32 of the GDPR and Article 2-quaterdecies of Legislative Decree No. 196 of 30 June 2003.

Furthermore, the COMPANY, in line with the provisions of Article 13 of the *Whistleblowing* Decree, as well as in compliance with the provisions of Articles 24 and 32 of the GDPR, identifies suitable technical and organisational measures to guarantee a level of security appropriate to the specific risks arising from the processing performed, on the basis of a data protection impact assessment (so-called DPIA), regulating the relationship by contract or other legal act

with external suppliers that process personal data on its behalf in the capacity of data controller (Centro Paghe S.r.l., Supervisory Board).

Adoption and updating of the procedure

This procedure is adopted by resolution of the Board of Directors of the COMPANY.

The COMPANY shall periodically review and, if necessary, update this procedure, in order to ensure its constant alignment with corporate practice and reference regulations.

Information and training

This procedure is disseminated by means of publication on the Internet site, company intranet and any other tool deemed most appropriate by the COMPANY.

The COMPANY promotes communication, information and training activities regarding this procedure, in order to ensure the most effective application of the same and the widest knowledge of the rules on REPORT, the functioning of and access to internal REPORT channels, as well as the measures applicable in the event of violations.