REITHERA S.R.L.

REGULATION ON THE INTERNAL SYSTEM OF REPORTING OF INFRINGEMENTS (WHISTLEBLOWING)

Pursuant to Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and additions

Approved on 27/03/2024

INDEX

1. PREMISES

Legislative Decree no. 24 of 10 March 2023 transposed Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report violations of national legislation[1]. The Decree entered into force on 30 March 2023, but the provisions contained in it are effective from 15 July 2023.

The new legislation aims, on the one hand, to ensure the expression of freedom of expression and information, which includes the right to receive or communicate information, on the other, is a tool to counter (and prevent) corruption, maladministration and the prevention of violations of law in the public and private sectors. The purpose of this Regulation is to define the system adopted by the Company, in line with the time-by-time provisions in force, regarding internal systems for reporting violations, to facilitate the submission of reports that may lead to the emergence of illegal behavior and violations of rules and regulations by the staff.

In particular, the document defines criteria and modalities for the reception, analysis and processing of reports of breaches, ensuring adequate confidentiality and protection of the personal data of the reporting entity and the reported entity. In addition, the precautions taken to protect the alerter, such as the protection of anonymity and the fight against any possible discrimination or retaliation against him, thus removing possible factors that could prevent or make difficult the reporting of unlawful conduct. The offences reported under this Regulation are indicated in the following paragraph. 4.1.

2. DEFINITIONS

Channel	Physical means of communication of the alert
Ethical Code	Adopted Ethical Code
Model 231	The organization, management and control model adopted by the Company pursuant to Legislative Decree no. 231 of 8 June 2001 and s.m.i.
O.d.V.	The Supervisory Body appointed by the Board of Directors pursuant to Legislative Decree no. 8 June 2001, n. 231 and s.m.i.

[1] The Decree was published in the Official Journal, General Series No. 63 of 15 March 2023.

Corporate Bodies	Board of Directors, Board of Statutory Auditors and Shareholders' Meeting
Personnel	a) Violations attributable to the Activity: employees and those who, in any case, operate based on relationships that determine their inclusion in the corporate organization, even in a form other than the employment relationship. b) Violations attributable to D.Lgs. n. 24/2023: employees and those who, in any case, operate on the basis of relationships that determine their inclusion in the corporate organization, even in a form other than the employment relationship pursuant to art. 3, paragraph 3, from lett. c) to lett. h) of D.lgs. n. 24/2023".
Responsabile	The Head of the Company's Internal Breach Reporting System.
Reports	• *Internal reports:* any communication, nominative received by the Company made by a recognized person as belonging to the Staff of the Company having as its object facts or behaviors (of any nature, even merely omitting) Personnel placed in violation of laws or regulations. • Report ex D.lgs. n. 24/2023: o Written Internal Report: the communication, in written form, of information on infringements submitted through an internal reporting channel. o Internal oral reports: internal reports via telephone lines or voice messaging systems or, at the request of the signaler, through a direct meeting fixed within a reasonable time. o External reporting: communication, written or oral, of information on violations, via an external reporting channel activated by ANAC.
Defamatory report or in "bad faith"	Notification that, at the end of the investigation phase, is found to be unfounded and carried out in bad faith, however, for the sole purpose of defaming or causing any damage to the injured person or company

SISV or System	The Company's Internal Abuse Reporting System
ANAC	National Anticorruption Authority
Public disclosure	Make publicly available information on infringements through the press or electronic means or otherwise **publicly disseminate** through media capable of reaching large numbers of people.

3. SOURCES OF LAW

Below are the main reference sources of the matter.

Directive 2013/36/EU of 26 June 2013 (Capital Requirements Directive - CRD IV)	Article 71 "Reporting on violations"
Norms on protection of personal data	Regulation (UE)
GDPR	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 the free movement of such data and repealing Directive 95/46/EC.
Law n. 179/2017	Provisions for the protection of whistleblowers who become aware of crimes or irregularities in the context of a public or private employment relationship.
D.Lgs. n. 231/2001 s.m.i.	Administrative responsibility of companies and entities
	Implementation of EU Directive 2015/849 (c.d. Fourth Anti-Money Laundering Directive) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. *Amendments and additions to legislative decrees 25 May 2017, n. 90 and n. 92, implementing Directive*

D.lgs. n. 90/2017 e d.lgs. n. 125/2019	*(EU) 2015/849, as well as the implementation of Directive (EU) 2018/843 amending the Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.*
D.lgs. n. 24/2023	Legislative decree concerning the protection of persons who report violations of Union law and laying down provisions concerning the protection of persons who report violations of national regulatory provisions.
Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019	Protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national legislation.

4. REPORTS OF VIOLATIONS

4.1 Scope

The Company's SISV provides staff, as defined in Chapter 2 of these Regulations, with the possibility to report:

a) Conduct, acts or omissions that may constitute a violation of the rules governing the Activity, including potential or actual breaches of the provisions on the prevention of money laundering and the financing of terrorism and of the rules on investment services and market abuse and on the distribution of insurance products.

b) conduct, act or omission consisting in: [2]:

1) administrative, accounting, civil or criminal offences;
2) relevant unlawful conduct of D. Lgs. n. 231/2001 or violations of the MOG;
3) offences falling within the scope of European Union or national acts [3];

[2] Cfr. art. 2, comma 1, lett. a, point 1, nn. da 1 a 6, D. Lgs. n. 24/2023

[3] Offences falling within the scope of the acts of EU or national law shall mean:
- offences falling within the scope of European Union or national acts in the following areas: public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product security and conformity; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems.

4) acts or omissions affecting the financial interests of the Union.
5) acts or omissions relating to the internal market.
6) acts or behavior which nullify the subject-matter or purpose of the provisions of Union acts in the areas referred to in points 3, 4 and 5.

Reporting is allowed in all those circumstances in which the reporting agent, at the time of Reporting, has a reasonable certainty of the correctness of the information provided. The mechanisms for protecting the reporting agent are therefore not applicable where information is provided that the reporting agent knows is incorrect, inaccurate, or misleading (i.e. "bad faith").

Reporting is allowed in all those circumstances in which the reporting agent, at the time of Reporting, has a reasonable certainty of the correctness of the information provided. The mechanisms for protecting the reporting agent are therefore not applicable where information is provided that the reporting agent knows is incorrect, inaccurate or misleading (i.e. "bad faith").

Alerts must be detailed, qualified and suitable to prevent and/or suppress unlawful conduct. It is necessary, therefore, that the alert is as detailed as possible in order to allow the determination of the facts by the competent entities to receive and manage the alerts. In particular, it is necessary to be clear:

- The circumstances of the time and place of the occurrence of the incident referred to in the report;

- The description of the fact;

- Particulars or other particulars identifying the person to whom the facts reported should be attributed.

It is also useful to attach documents that can provide evidence of the facts being reported, as well as the indication of other subjects potentially aware of the facts.

4.2 Recipients

This Regulation is addressed to all Company Personnel, as indicated below. The category here defined of the "Recipients" refers to the group of "reporting" subjects.

Included in the definition of Personnel are "employees and those who, in any case, operate on the basis of relationships that determine their inclusion in the company organization, even in a form different from the employment relationship" (4).

Pursuant to Legislative Decree No. 24/2023, "Recipients" in the private sector are the following categories of subjects:

- employees of private sector subjects, including workers whose employment relationship is governed by Legislative Decree No. 81 of 15 June 2015 or Article 54-bis of Decree-Law No. 50 of 24 April 2017, converted, with amendments, Law no. 96 of 21 June 2017; the self-employed, including those indicated in Chapter I of Law No. 81 of 22 May 2017, as well as the holders of a collaborative relationship referred to in Article 409 of the Code of Civil Procedure and Article 2 of Legislative Decree No. 81 of 2015, working with public or private sector entities;
- workers or collaborators who carry out their work with private sector entities providing goods or services or carrying out works in favor of third parties.
- freelancers and consultants working in the private sector.
- i tirocinanti che prestano la propria attività presso soggetti del settore privato.
- shareholders and persons with managerial, managerial, supervisory or representational functions, even where such functions are performed merely as a matter of fact, by private sector entities.

The protection of reporting persons applies, in accordance with Legislative Decree no. 24/2023. even if the report, the report to the judicial or accounting authority or the public disclosure of information takes place in the following cases:

a) Where the legal relationship has not yet started, if the information on infringements has been acquired during the selection process or at other pre-contractual stages;

b) During the trial period;

c) After the legal relationship has been terminated if the information on the infringements has been acquired in the course of the relationship.

4.3 Protection of the signaler

The Company ensures the confidentiality and protection of the personal data of the reporting person in order to mitigate the risk of retaliation and/or discrimination against him; the documentation relating to the Reports is strictly confidential.

All parties involved in the process have the obligation to ensure the confidentiality of the information received and, in particular, the identity of the reporting agent. The violation of the obligation of confidentiality is a source of disciplinary liability, without prejudice to any other form of liability provided for by law.

The identity of the alerter shall be protected except where:

- The Report is made for damaging or otherwise causing damage to the person reported (i.e. "bad faith" report) and constitutes a liability for slander or defamation in accordance with the law;
- Anonymity is not legally enforceable (e.g. criminal investigations, inspections of supervisory bodies, essential defense requirements);
- In the Report are revealed facts and/or circumstances such that, although outside the sphere of the company, make appropriate and/or due reporting to the Judicial Authority.

Alerts may not be sanctioned, dismissed, or subjected to any discriminatory measure on grounds relating, directly or indirectly, to the alert, except as specified in Point 4.5 and Point 7.

Discriminatory measures shall mean unjustified disciplinary action, harassment in the workplace and any other form of retaliation.

The D.lgs. n. 24/2023 provides, for the protection of the signaler, the prohibition of retaliation defined as "*any conduct, act or omission, even if attempted or threatened, carried out by reason of the report, the report to the judicial or accounting authority or public disclosure and which may cause or may cause an unjustifiable harm to the person being slandered or the person who has made the complaint."*[4].

It is reiterated that, in order to constitute retaliation and, consequently, to qualify for protection, a close link between reporting, disclosure and reporting and unfavorable behavior/act/omission suffered is necessary, directly or indirectly, by the reporting person, the complainant or the public disclosure person.

The signaler who considers that he has suffered a retaliation must give detailed notice to the

[4] It is therefore a broad definition of the concept of retaliation that can consist both in acts or measures but also in behaviors or omissions that occur in the workplace and that cause harm to the protected subjects.

The new rules, refers only to retaliation, overcoming the division between discriminatory measures and retaliation present in L. n. 179/2017, and greatly expands the list of cases that constitute retaliation, although this is not exhaustive. In addition to those expressly indicated in Legislative Decree no. 24/2023 may constitute retaliation, for example, also the claim of results impossible to achieve in the ways and times indicated; an assessment of the performance artatamente negative; an unjustified dismissal of assignments; an unjustified failure to confer assignments with simultaneous attribution to another subject; the repeated rejection of requests (e.g. leave, leave); the unjustified suspension of patents, licenses, etc.

President of the Board of Statutory Auditors in order to enable him to assess its validity and adopt possible appropriate actions.

The persons protected can inform ANAC of any retaliation they feel they have suffered, whether it is retaliation already carried out against them or retaliation attempted, even if the conduct has not been carried out in a complete manner, and only those envisaged.

In case of retaliation, the D. Lgs. n. 24/2023 provides for a protection regime whose application requires that the reporting, public disclosure, and denunciation by one of the entities identified by the legislator meet certain conditions and requirements; in particular, to enjoy protection:

- The notifiers or complainants must reasonably believe, also in the light of the circumstances of the specific case and of the data available at the time of the reporting, public disclosure, or complaint that the information on the reported infringements, disclosed or reported are true. Instead, simple assumptions or rumors as well as public information are not enough.
- On the other hand, for the purpose of protection, the fact that the subject has reported, made public disclosures or complaints while not being certain of the actual occurrence of the reported or denounced facts and/or the identity of the author of the same or also reporting inaccurate facts due to a genuine error.
- Similarly, any person who makes a report, public disclosure or complaint is entitled to protection if he has acted on well-founded grounds, which reasonably suggest that the information on the reported infringements, disclosed or denounced are relevant as part of the offences considered by the legislator.
- Public reporting or disclosure must also be made based on the provisions of Chapter II of the Decree. It is recalled that in the case of alerts sent to an entity other than the competent one, the latter must transmit them immediately to the entity authorized to receive and manage the alerts, giving the simultaneous notification of the transmission to the reporting person. To allow such timely transmission, the reporting agent should clearly indicate in the subject of the report that it is a whistleblowing alert.
- there must be a close link between the reporting, public disclosure, and the complaint and the unfavorable behavior/act/omission suffered directly or indirectly by the reporting or reported person, for them to be considered retaliatory and, as a result, the entity is eligible for protection.

Art. 17 of D.lgs. n. 24/2023 also provides for a probative regime in favor of the reporting agent; in fact, in the context of judicial or administrative proceedings (including extrajudicial) related to the

reporting: in particular, the retaliatory nature of the behavior adopted (by the counterparties) because of the alert, considered ex lege as a reaction to the report or disclosure or complaint, is presumed. Consequently, the burden on those who have carried out the abovementioned behaviors is on those who have shown that they have been motivated by reasons unrelated to reporting or disclosure or complaint (reversal of the burden of proof); in the event of a claim for compensation, a similar favorable regime is provided for in respect of the finding of damage which is presumed to be a consequence of reporting or disclosure.

The protection measures provided for in Chapter III of Legislative Decree no.24/2023 also apply [5]:

a) to facilitators [6];
b) persons in the same working environment [7] of the reporting person [8], the person who has made a complaint to the judicial or accounting authority or the person who has made a public disclosure and who is linked to them by a stable emotional or family relationship by the fourth degree;
c) work colleagues of the reporting person or of the person who made a complaint to the judicial or accounting authority or made a public disclosure, who work in the same working environment and have a habitual and current relationship with that person;
d) institutions owned by the reporting person or the person who has made a complaint to the judicial or accounting authority or who has made a public disclosure or for whom the same persons work, as well as entities operating in the same working context [9].

[5] Cfr. art. 3, comma 5, D.Lgs. n. 24/2023.

[6] "Facilitator" means a natural person who assists a reporting person in the reporting process, operating within the same working environment and whose assistance must be kept confidential (cf. art. 2, paragraph 1, lett. h, D. Lgs. n. 24/2023).

[7] "Work context" means the work or professional activities, present or past, carried out in the framework of the reports referred to in Article 3, paragraphs 3 or 4, through which, regardless of the nature of those activities, a person acquires information on the infringements and in the context of which he or she could face retaliation in the event of a report or public disclosure or a complaint to the judicial or accounting authority. The term "persons in the same working environment as the reporting agent" therefore refers to persons who are linked by a network of relationships arising from the fact that they have been or have been operating in the same working environment as the reporting agent or complainant, such as colleagues, ex-colleagues, collaborators (cf. art. 2, paragraph 1, lett. i, D. Lgs. n. 24/2023).

[8] "Reporting person": The natural person who makes the report or the public disclosure of information on violations acquired within their business context (cf. art. 2, paragraph 1, lett. g, D. Lgs. n. 24/2023).

[9] The concept of ownership entities may include: either cases where a person is the owner of an entity exclusively or in partnership with a majority of third parties; the entities with which the complainant, complainant or public disclosure works; entities operating in the same business environment as the complainant, complainant or public disclosure entity.

4.4. Regularity of the reporting

Alerts must be nominative, and the signaler is asked to submit his identification details in order to be recognized and, if necessary, contacted. The legislation requires, however, that the Company identifies the reporting entity as a subject belonging to its Staff.

The process adopted and defined in this regulation guarantees, however, from the moment the Report is sent, confidentiality at all stages of the procedure; in particular, the identity of the reporter will not be disclosed to third parties. However, it may be necessary to communicate the identity of the alerter to the competent entities involved in the investigations or any subsequent judicial proceedings, which may be initiated following the verification carried out as part of the reporting procedure.

Anonymous reporting, where substantiated, for ANAC is treated as ordinary reporting and in this case considered in its "ordinary" supervisory procedures. According to the Anac Guidelines [10] public and private sector entities that receive alerts via internal channels consider anonymous alerts as ordinary alerts to be processed according to the criteria set out in their respective legal systems. In any event, the anonymous complainant or complainant, subsequently identified, who informed ANAC that he had been retaliated may benefit from the protection afforded by the decree in the event of retaliatory measures. Public or private sector entities that receive alerts through internal channels and the Authority itself are, therefore, required to record anonymous alerts received and to keep the relevant documentation no later than five years from the date of receipt of such alerts, thus making it possible to trace them, in the event that the reporting agent, or who made the complaint, inform ANAC that it has been retaliated for that anonymous report or complaint. However, subject to point 3.1 above, within the framework of disciplinary proceedings, the identity of the reporting person cannot be disclosed where the challenge of the disciplinary charge is based on separate and additional findings with respect to the report, even if they are a consequence of the report.

Where the dispute is based, in whole or in part, on the alert and knowledge of the identity of the reporting person is indispensable for the defense of the accused, the alert shall be usable for disciplinary proceedings only if the reporting person has given his or her express consent to the disclosure of his or her identity. In this case, the notifier shall be informed in writing of the

[10] The "Guidelines on the protection of persons who report violations of Union law and the protection of persons who report violations of national regulatory provisions. Procedures for the submission and management of external reports" were approved with Resolution no. 311 of 12 July 2023.

reasons for disclosure of the confidential data, and in the internal and external signaling procedures referred to in this Chapter when the disclosure of the identity of the reporting person and the information referred to in paragraph 2 is also indispensable for the defense of the person involved. Moreover, pursuant to paragraph 9 of art. 12 of D.lgs. n. 24/2023, in the internal and external signaling procedures referred to in this Chapter, the person involved can be heard, or, at his request, is heard, also by means of a written procedure through the acquisition of written observations and documents.

4.5 Responsibility of the reporting agent

The reporting agent must not use the System described here for purely personal purposes or to make work claims against hierarchical superiors or the Company in general, as for these purposes reference must be made to the specific procedures already in place.

Any improper or incorrect use of the System, such as manifestly opportunistic Alerts, those made for the sole purpose of damaging the reported or other subjects, as well as any other form of misuse or intentional exploitation of this System, are subject to sanctions and disciplinary measures.

The reporting agent shall provide initial information relating to a reasonable belief, or reasonable suspicion, that an illegal activity has occurred or is in progress. The reporting agent must provide evidence of acts, facts or omissions that may constitute a violation of the rules governing the activity of the Company, supporting them with as detailed information as possible. However, it is not the responsibility of the reporter to prove the truth of his assertions.

The investigation cannot, however, be undertaken without adequate verifiable evidence about the Report carried out.

The complainant will not be immune from disciplinary action if he or she is found to be in bad faith or involved in the reported offences.

4.6 External Reporting Channel (ANAC)

The National Anti-Corruption Authority (ANAC) has published the new Guidelines as well as the Regulation for the management of external reports and for the exercise of the sanction power

of ANAC itself. In implementation of Legislative Decree 10 March 2023, n. 24[11] which will ensure, including through the use of cryptography, the confidentiality of the identity of the reporting person, the person involved and the person mentioned in the alert, as well as the content of the alert and its documentation. The signaler may send an external alert to ANAC if one of the following conditions is met ([12]):

a) it is not foreseen, within the working context of the signaler, the mandatory activation of the internal reporting channel or this channel, even if mandatory, is not active or, even if activated, is not in compliance with the provisions of D. Lgs. n. 24/2023 for internal signaling channels;

b) the reporting person has already issued an internal alert and has not been followed up;

c) the reporting person has reasonable grounds to believe that, if he made an internal alert, it would not be effectively followed-up or that the same alert could lead to the risk of retaliation;

d) the reporting person has reasonable grounds to believe that the infringement may constitute an imminent or manifest danger to the public interest.

4.7 Public Disclosure

The signaler, pursuant to art. 15 of D. Lgs. n. 24/2023, can directly carry out a public disclosure in cases where:

- has previously issued an internal and external alert or has directly issued an external alert and has not been acknowledged within the time limits set for the measures planned or taken to follow up alerts;
- the reporting person has reasonable grounds to believe that the infringement may constitute an imminent or manifest danger to the public interest;
- the reporting person has reasonable grounds to believe that the external alert may involve the risk of retaliation or may not have effective follow-up due to the specific circumstances

[11] Le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" sono state approvate con Delibera n. 311 del 12 luglio 2023; il "Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio dell'ANAC in attuazione del Decreto Legislativo 10 marzo 2023, n. 24" è stato adottato con Delibera n. 301 del 12 luglio 2023.

[12] Cfr.art. 6 del D.Lgs. n. 24/2023.

of the particular case, such as those in which evidence may be concealed or destroyed or where there is a reasonable fear that the person receiving the report may be colluding with the offender or involved in the infringement itself[13].

4.8 Sanctions and measures within the competence of ANAC

ANAC, according to art. 21 of D. Lgs. n. 24/2023 may apply a series of administrative fines to subjects, public or private, in case of violation of the rules established by the decree itself. In particular, there is a penalty of 10,000 to 50,000 Euros in the event of retaliatory conduct or conduct impeding the detection of the report or if the obligation of confidentiality has been violated. Penalties of the same amount are also provided for the non-installation of reporting channels or when procedures for the management of alerts have not been adopted or these do not comply with the requirements of Articles 4 and 5 of Legislative Decree no. 24/2023[14].

For these behaviors, within the private sector, Article 21 of the decree provides that entities and legal persons referred to in Article 2, paragraph 1, letter q), n. 3, that is, with less than 50 employees but who have established an organizational model pursuant to the discipline referred to in Legislative Decree no. 231/2001, provide in it disciplinary sanctions against those who ascertain that they are responsible for such offences.

The same decree also provides that ANAC may apply a financial penalty from 500 to 2,500 euros against the reporting agent, where it is established that it is liable for the offences of defamation or slander in the event of intent or gross negligence, unless there has already been a conviction for the same offences or in any case for the same offences committed by reporting them to the judicial or accounting authority.

5. ROLES AND RESPONSABILITIES

5.1 Corporate Bodies

The Board of Directors of the Company approves these Regulations defining the characteristics of the System adopted.

The Board of Directors is responsible for identifying the actions to be taken in the light of the feedback received from the investigation.

[13] Cfr. art. 15 del D.Lgs. n. 24/2023.

[14] Please note that Articles 4 and 5 of Legislative Decree No. 24/2023 concern, respectively, the internal signaling channels and the management of internal signaling channels.

In addition, the Board of Directors:

- Analyses, evaluate and approve the periodic information (annual report of the Manager) on the management of SISV also in order to define possible improvements to SISV and the overall system of internal controls;

- Define any amendments to be made to the SISV;

- Shall be promptly informed of the Reports which, by reason of the importance of the facts, may give the Company exposure to high risks of a capital, operational or reputational nature.

The Board of Statutory Auditors shall verify the adequacy of the adopted System, the proper performance of the tasks and the appropriate coordination of the functions involved, promoting any corrective action of the deficiencies and irregularities detected. In carrying out this task, it may use internal operating structures or external consultants within the limit of the Supervisory Body's own expenditure.

The Chairman of the Board of Statutory Auditors receives analyses and evaluates any Reports involving members of the Board of Directors, the Chief Executive Officer/General Manager and the Head of SISV.

The Board of Statutory Auditors takes note of the Annual Report drawn up by the Manager and is promptly informed of any Reports that, due to the importance of the facts, may result in the Company being exposed to high risks of a financial nature, operational and reputational.

5.2 Responsible of the system of violations reports

The Company identifies the Responsible for the System in the Responsible for the Prevention, Corruption and Transparency Society, which ensures the proper conduct of the proceedings and, in its Annual Report, reports directly to the Corporate Bodies of the Company the information reported, for approval. In particular, that annual report on the proper functioning of the internal reporting systems shall contain aggregated information on the findings of the activity carried out following the reports received, in compliance with the rules on the protection of personal data.

The Manager, in line with the principle of proportionality, can directly manage the phases of reception, examination and evaluation of the Reporting process or can make use of internal resources.

The Manager ensures the management of the System according to the canons of confidentiality of the information received and provides timely information to the Corporate Bodies regarding

particular reporting cases that could expose the Company to significant risks of patrimonial nature, operational or reputational.

The Manager draws up an annual report on the proper functioning of the System, containing aggregate information on the results of the activity carried out following the Reports received.

As a rule, the Staff Reports are addressed to the Manager through the transmission methods provided for in Chapter 6 below.

In case of unavailability of the Manager (for holidays, illness, missions, etc.) this is replaced by a delegate to be appointed within the Internal Audit Function that assumes, for the period of replacement, the role and responsibility of the Manager.

5.3 Other Functions and Directions involved

The other Functions involved in the management process of the Reports as provided for in these provisions are:

Managing Director/General Manager

- ensure the implementation of the SISV in accordance with the rules and consistent with this Regulation;
- take appropriate measures to protect the signaller, if necessary in agreement with the Personnel Directorate provided for in Articles 16 and 19 of D. Lgs. n. 24/2023[15];
- receives the information of the Manager;
- deliberates possible measures and sanctions as far as competence.

Personal Direction

• ensures the training activity, in agreement with the Manager;

• take appropriate measures to protect the reporting agent, if necessary in consultation with the Chief Executive Officer/General Manager;

• implement any measures and sanctions decided by the competent bodies.

[15] Art. 16 and art. 19 of D. Lgs. n. 24/2023 concern, respectively, the "Conditions for the protection of the reporting person" and "Protection from retaliation".

In the event of disciplinary action, the Personnel Department shall implement the necessary measures by activating the Disciplinary Affairs Committee of the Company referred to in the current Staff Regulations.

5.4 Control on violation system

Controls on the violations system are assured:

- by the Manager who continuously monitors the proper functioning of the SISV and reports annually to the Corporate Bodies on its functioning;

- by the Board of Statutory Auditors, which supervises the adequacy, completeness, functionality and reliability of SISV with the possible help of internal resources or independent external consultants.

5.5 Relations with the Supervisory Body

If during the investigation, it is found alleged or found violations of the offences referred to in D. Lgs. n. 231/2001 will be provided appropriate information to the Supervisory Body in compliance with the principles of confidentiality and confidentiality of the information of the reporter and any reported.

5.6 Processing of personal data in whistleblowing reports

Regarding the processing of personal data for whistleblowing reports, the data controller is:

ReiThera s.r.l. - Via di Castel Romano n. 100 – Roma

In compliance with the provisions of the legislation on the protection of personal data, the aforementioned data controllers have individually designated the company DigitalPA s.r.l. - Via San Tommaso D'Aquino 18/a - 09134 Cagliari provider of whistleblowing reporting software, responsible for the processing of personal data pursuant to art. 28 of the GDPR and the Prevention, Corruption and Transparency Manager as subjects authorized to process data for the reports in question.

The personal data of Whistleblowers and of all the parties involved in the Report are processed

in accordance with current legislation on the protection of personal data.

- In particular, it is evident in this context that: the processing activities underlying the management of the Report are carried out in compliance with the principles dictated by art. 5 GDPR.
- the Reporting Entity - is within the limits and in the ways provided for by law, the reported

subject and all the persons involved - will receive an information pursuant to art. 13 and 14 of the GDPR which specifies the purposes and methods of the processing of personal data and the period of storage thereof, the conditions of lawfulness on which the processing is based, the categories of recipients to whom data may be transmitted as part of the management of the Report and the rights granted to the Reporting Agent by the Regulation;

- The reporting system provides that the personal data processed (potentially, even the particular data referred to in art. 9 GDPR) are adequate, relevant and limited to what is necessary with respect to the purposes for which they are collected.

  In addition, personal data will be processed for the time necessary to achieve the purposes that justify the collection (eg: evaluation and management of the report); once the purpose of processing is exhausted, the personal data will be stored on the basis of the criteria and for the periods indicated in the information on data processing provided to the data subject and subsequently deleted or anonymized;
- In addition, personal data will be processed for the time necessary to achieve the purposes that justify the collection (eg: evaluation and management of the report); once the purpose of processing is exhausted, the personal data will be stored on the basis of the criteria and for the periods indicated in the information on data processing provided to the data subject and subsequently deleted or anonymized;
- the exercise of rights by the Signaler or the Reported ("interested parties" pursuant to the law on the protection of personal data), in relation to personal data processed as part of the Whistleblowing process, may be limited, pursuant to and for the effects referred to in Article 2-undecies of Legislative Decree No. 196/2003 and s.m.i., in the event that such an exercise could result in an effective and concrete prejudice to other interests protected by specific legislation, with the clarification that under no circumstances can the Reported person be allowed to use their rights to obtain information on the identity of the Signaler;
- access to personal data is granted only to authorized persons who are entitled to receive such Reports, limiting the transfer of confidential information and personal data only where this is necessary and where required by law.
- the personal data are kept only for the appropriate and proportionate time limits to allow the execution of the Whistleblowing Procedure.

6. INFRIGMENT REPORTS AND MANAGEMENT PROCESS

The internal reporting process of the Company's violations is structured in the following steps:

6.1 Channel and mode of transmission of signals

Communication channels

The Company has identified as the person responsible for receiving, examining and evaluating the Report, Responsible for corruption prevention and transparency (RPCT) on the assumption that it can meet the following requirements:

a) is not hierarchically or functionally subordinate to any reported entity.

b) is not himself liable for the infringement.

c) does not have a potential interest related to the alert that would compromise its impartiality and independence of judgment.

The methods of use of the Platform are reported in the appropriate operational documentation.

Media

The Platform adopted is able to ensure the confidentiality and protection of the information transmitted; in particular, it ensures:

- the confidentiality of the identity of the reporting person.

- the confidentiality of the person involved and of the person otherwise mentioned in the alert.

- the confidentiality of the content of the alert and the related documentation.

Following the insertion of the Report, the Platform automatically forwards a notice to the Head of the SISV for the start of the subsequent stages of investigation.

Verbal Reports may also be represented to the Data Controller by means of a personal interview; in this case, the Report must always be recorded and signed by the reporting agent.

The Manager shall carry out the following activities:

1) Issue the reporting person with acknowledgement of receipt of the report within seven days from the date of receipt (activity automatically managed through the Platform used);

2) Maintain contacts with the reporting person and be able to request additions from the reporting person if necessary (activities also supported by the Platform in use);

3) diligently follow up reports received.

4) provide feedback to the alert within three months of the date of the acknowledgement of receipt or, failing that, within three months of the expiry of the seven-day period following the submission of the alert. The Platform in use supports Responsible through specific notification/alerting functions.

6.1 Receipt of the alert

The reporting agent must necessarily be recognised as a person belonging to the Company's Personnel, as defined in paragraph 4.2 above.

The Manager is obliged to guarantee the confidentiality of the information received, including the identity of the reporter, and ensures that the Report received has the required contents. If not, contact the complainant, through the Platform, to request the missing information; in the event that this is not provided and this prevents the continuation of the investigation, The Data Controller shall file the Report and the related information after having kept a record of it for statistical purposes only.

The Platform guarantees the recording of individual reports and the attached documentation.

6.2 Oral Reports

The D.lgs.n. 24/2023 provides for the possibility of making oral reports "using telephone lines or voice messaging systems or, again, through a direct meeting set within a reasonable time".

For this purpose, at the request of the reporting person, the report is made orally during a meeting with the SISV Manager, it, with the consent of the reporting person, it shall be documented by the personnel involved either by recording it on a device suitable for storage and listening or by drawing up a report signed by the signaler.

6.3 Exam on report

The examination of the Report is carried out based on the information acquired as part of the activity of receiving the Report. The Manager, using the support of any internal and/or external resources for the purpose, carries out the examination of the documentation acquired and carries out the verifications of the case.

The subjects for this purpose, Members, verify the existence of eligibility requirements, carry out a preliminary analysis of the Alert to assess the characteristics, timing and methods of investigation as well as potential impacts and, finally, carry out an investigative activity.

The purpose of the preliminary analysis is not to reach a definitive conclusion on the incident or responsibilities, but to make a "verification of eligibility" and a preliminary assessment of the evidence available to determine whether there is sufficient evidence to justify further investigation and the degree of relevance/risk.

The "eligibility check" must determine whether the Alert has all the characteristics necessary to make it eligible; in particular, the eligibility of the reporting agent must be verified, the admissibility of the reported act/fact and the presence of any conflicts for the subject responsible for the examination.

The Manager in a special document must record the results of the preliminary analysis (Preliminary Analysis Findings uploaded to the Whistleblowing Platform) in which it is established whether or not a formal investigation should be carried out and the further investigation that at the moment seem to be to be conducted.

To this end, the following factors, among others, should be considered:

- information provided in support of the Report.

- current procedures in force relating to the facts reported.

- previous alerts having the same subject and already examined.

- facts or situations in respect of which public authorities are already investigating.

Based on the findings of the preliminary analysis, in the document it will also be necessary to determine whether the Report can be considered "relevant" and, as such, an "emergency procedure" (Cfr. § 6.5 - Management of relevant alerts) should be initiated.

The Investigation has, finally, the purpose of exploring in detail the facts/ acts reported in the Report, ascertaining the existence or acquiring evidence in support of the acts or facts reported and related responsibilities. The investigative activity must also gather useful elements to determine the actual relevance and scope for the Company of the reported violations. For this purpose, any activity deemed appropriate might be carried out also through the involvement of any competent Business Departments and/or reporting entity.

If the report is classified as "ineligible", the reporting agent is informed via the Platform.

6.4 Management of relevant reports

The System must allow to identify and communicate without delay to the Corporate Bodies the

Reports deemed "relevant". For "relevant reports" are to be understood, in addition to those concerning members of the Corporate Bodies, the Reports for which, even after an initial preliminary analysis, one or more of the following situations is considered possible:

- a significant budgetary impact;
- a significant reputational impact;
- violation of the Organizational Model ex D.Lgs. n. 231/2001;
- a significant deficiency/deficiency of the Internal Control System.

In the event of "relevant reports", the Manager shall promptly inform the President of the

Board of Statutory Auditors, also for the purposes of a possible convocation of the Board of Directors.

In case of "relevant reports" or, in any case, related facts reported on which are being investigated by public authorities, the Legal and Corporate Affairs Department must be involved in the examination and evaluation activities.

In the case of "relevant alerts", and in any situation where it is conceivable that illegal actions are still taking place, emergency procedures shall be in place to enable rapid definition and implementation of measures to resolve or mitigate the effects.

The Manager determines, based on the feedback received (Preliminary Analysis or Preliminary Investigation), whether it is appropriate to start an emergency procedure, giving clear reasons. In this case, the Manager activates the appropriate emergency measures on the basis of the instructions received from the Corporate Bodies previously informed; these measures can be taken even before the reported person is informed of the Report. The process must, however, continue along the normal path and responsibilities defined for it.

6.5 Evaluation on reports

In the evaluation phase, it may be necessary to carry out further investigations and to collect further information. In the evaluation process, the Manager can rely on the collaboration of other SISV reference figures within the Company (Members of the Board of Statutory Auditors, Head of Personnel Management).

Before the end of this phase, except in cases of emergency procedure, the person who has been alerted must be informed of the subject of the Alert against him, for the purposes referred to in the previous par. 4.3 ("Protection of the reporting agent") and may counter within the deadline

indicated in the communication.

At the end of this phase, the Responsible carries out, in a special document ("Findings of the Investigation and Evaluation") the description of the facts and their assessment (also in the light of any counter-deductions of the reported) defining their relevance, the possible effects/consequences for the Company, as well as clarifying the reasons that led to the evaluation.

This document shall be sent promptly to the Board of Directors for the subsequent evaluations and decisions.

The alert shall be acknowledged within three months of the date of the acknowledgement of receipt or, in the absence of such acknowledgement, within **three months** of the expiry of the period of seven days from the submission of the alert[16].

6.6 Actions

The decision phase is up to the Board of Directors with the possibility of delegating to the Chief Executive Officer within the limits allowed by the Statutes ([17]).

The competent bodies may:

a) to initiate disciplinary proceedings, or other useful decisions, against the reported entities recognized as liable.

b) initiate the sanction procedure against the person who acted with intent and/or gross negligence.

c) not to carry out any action and to order the archiving of the Report.

The final decision is communicated to the signaler, if he has expressed a desire to know it, to the reported, in a confidential way, and to his manager. The same must then be protected storage object.

In view of the evidence obtained, if it is considered appropriate or in the event of the discovery of facts and circumstances that by law must be the subject of a complaint to the competent authority, further action may be taken such as:

- alerts to the competent judicial authority.
- reporting to supervisory bodies.
- definition of possible prevention and mitigation actions.

[16] Cfr. art. 5 del D.Lgs. n. 24/2023.

[17] In case of a report concerning a member of the board, the same must obviously refrain from participating in the decision-making phase under consideration.

The Company assesses, even if the acts/facts are ascertained but not attributable to duly identified subjects, any measures to mitigate the risks involved and to prevent the recurrence of the violations that occurred.

6.7 Reporting

The evaluation processes of the Reports are the subject of a special annual report to the Board of Directors. The reporting activity contains a summary of the main aggregated statistical data (number of reports, number of sanctions adopted with distinction of disciplinary measures applied, number of subjects reported, corporate functions involved, etc.).

This report is approved by the Board of Directors and made available to the Staff on the Corporate Intranet.

6.9 Storage, conservation, and traceability of reports

The Manager shall ensure:

- The traceability of reports and related analysis, evaluation and decision-making activities;

- the proper preservation of the documentation relating to the Reports and the related verification activities.

The storage, traceability and archiving of Reports must be carried out in compliance with the requirements of confidentiality and confidentiality provided by the legislation on the protection of personal data.

The alerts and related documentation shall be kept for the time necessary to process the alert and in any event not later than five years from the date of notification of the final outcome of the reporting procedure, in compliance with the obligations of confidentiality referred to in Article 12 of this Decree and the principle referred to in Articles 5, paragraph 1, letter e), Regulation (EU) 2016/679 and 3, paragraph 1, letter e), Legislative Decree No. 51 of 2018[18].

To keeping oral reports, paragraphs 2, 3 and 4 of art. 14 of Legislative Decree no. 24/2023 (cf. also par. 6.3) apply.

6.10 Training

[18] Cfr. art. 14 del D.Lgs. n. 24/2023.

In order to ensure the necessary effectiveness of the System, it is essential that the principles laid down in this Regulation are disseminated to all recipients and transposed into appropriate operational procedures that provide a clear description of the activities envisaged and the tools used for this purpose.

The Company undertakes to ensure the dissemination of this Regulation to all Personnel through publication on the Company's Intranet. The contents of this Regulation will also be brought to the attention of each employee at the time of recruitment, as well as of interested parties ex D.lgs. n. 24/2023.

Personnel shall be given specific information about the fact that the legal provision under which the alleged controller has the right to obtain, inter alia, the indication of the origin of the personal data (in accordance with the provisions of current legislation on the protection of personal data), does not apply with regard to the identity of the reporting agent, which can be revealed only with his consent or when knowledge is essential for the defense of the reported.

For those who, for the purposes of this Regulation, fall into the category of Staff, the same training and information requirements apply as described above, although, in relation to the type and duration of the relationship with the Company, may be subject to different procedures and timetables compared to the employees.

External collaborators must also be defined a specific contractual clause, to be included in contracts or agreements governing the provision of activities or collaboration of the same in favor of the Company, establishing the subjection of such external collaborators to the internal rules on "reporting of violations".

6.11 Assessment of the internal infringement reporting system

The assessments and considerations of competence regarding the compliance of SISV with the relevant legislation are contained in the annual report on the proper functioning of the reporting systems (cf. point 5.2 above).

The adequacy assessment shall consider the following plant aspects:

- compliance of internal regulations and compliance with applicable external rules.

- clarity and completeness of the operating instructions for the use of the system by potential Signallers;

- existence of adequate information and internal notes to support the parties involved in the process;

- the existence of appropriate training activities and awareness-raising campaigns for potential signallers.

The Data Controller, if applicable also with the support of the other corporate functions, verifies the existence of adequate procedures for the management of the processing of personal data. To verify the correct functioning of the System, the Manager must carry out checks both on the actual

compliance with the defined plant, and with reference to its real effectiveness.

In particular, the following aspects shall be assessed:

- full and correct application of the relevant internal provisions.
- compliance with the timetable;
- compliance with the principles of confidentiality and protection of information and with the personal data of the alerter and the alerter.
- adequacy of the dissemination activities of the Regulation.

The analysis and evaluation of the SISV can be carried out, in addition to the Manager, also in response to specific requests for verification by the Board of Statutory Auditors that, for this purpose, can make use of competent company resources.

7. SANCTIONS AND MEASURES

All employees must comply with the provisions of these Regulations. Any failure to comply with or breach of the rules set out here may result in the activation by the employer of disciplinary initiatives, with the procedures and guarantees provided by law, contracts, and company regulations in force, without prejudice to any civil, administrative and/or criminal liability.

In the relationship that governs the contract of external collaborators, the measures that the Company may take in the event of violations provided for by these Regulations; for contracts in existence at the date of approval of these Regulations, the provisions of the previous paragraph shall apply when renewing contracts.