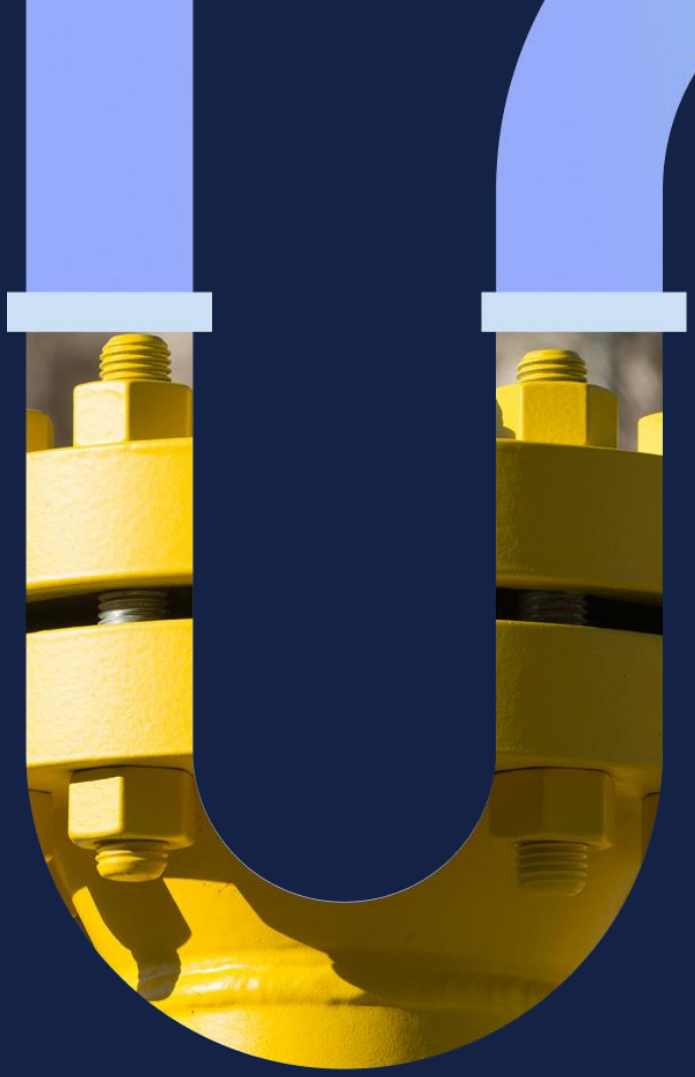


Società Gasdotti Italia

MODEL OF ORGANIZATION, MANAGEMENT AND CONTROL

Annex C
Protocol for reporting wrongdoing

- c.d. *Whistleblowing* -

Last update: March 2024

Index

INTRODUCTION AND ESSENTIAL REFERENCE STANDARDS

The concept of the whistleblower or whistleblower on wrongdoing was first introduced in Italy with Law No. 190 of Nov. 6, 2012, which provided for the inclusion of Article *54-bis* in Legislative Decree No. 165 of March 30, 2001 on the protection of a public employee who decides to report wrongdoing committed within the entity in which he or she works.

The *whistleblower* is the worker who, during the course of his or her work activity (thus as an *insider*) "discovers" a wrongdoing, possible fraud, danger or other serious risk that could cause concrete harm to third parties (e.g., consumers, customers) or to the company/company itself (e.g., damage to its image) and decides to report it, exposing himself or herself, however, to the risk of harassment, retaliation or harassment.

These endogenous whistleblowers represent an effective tool of "diffuse control" that provides an internal protection mechanism within the public or private apparatus by creating a kind of organic immune system. However, in order for such whistleblowers to be encouraged, it is necessary that the one who reports the wrongdoing be protected from retaliation or harassment, if only in terms of the work climate in which he or she offers his or her services.

Initially, in Italy, the reporting of wrongdoing of which the employee had become aware through his or her *insider* status was an eventuality reserved for those employed in the public sector. With Legislative Decree No. 90 of May 25, 2017, the Italian state implemented the first European directive on the subject, specifically Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and amended other transposed provisions by providing, among other things, that *procedures aimed at incentivizing internal reporting of potential or actual violations of anti-money laundering provisions by employees* should be adopted in the system being regulated. Ultimately, the regulation of *whistleblowing* was definitively extended to the entire private sector.

Following the entry into force of Law No. 179 of Nov. 30, 2017 (on *Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship*), the legislature has, among other things, amended Art. 6

co. 2- *bis* of Legislative Decree No. 231 of June 8, 2001 (entitled *Protection of the employee or collaborator who reports wrongdoing in the private sector*), on the subject of the administrative liability of entities for crime.

The 2017 law had required companies with an organizational and management model pursuant to Art. 6 co. 1 lett. a) Legislative Decree No. 231/2001 to provide ways for both top management of the entities and individuals under their management or supervision to submit reports of unlawful conduct or violations of the organizational model and, at the same time, ensure the confidentiality of the reporter's identity.

In the face of known difficulties in implementing protocols that are adequately effective in terms of both preventive functionality and protection of the confidentiality of *whistleblowers*, the European Union has again intervened with more detailed *whistleblowing* requirements.

LEGISLATIVE DECREE MARCH 10, 2023, NO. 24: SCOPE OF APPLICATION

On October 23, 2019, the European Parliament and the Council adopted Directive (EU) 2019/1937, on "the *protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws.*" The directive introduced a set of common minimum standards aimed at ensuring a high level of protection of both public and private "whistleblowers" in order to standardize the different regulations adopted by member states.

Despite the fact that Article 26 of EU Directive 2019/1937 had stipulated an obligation for member states to implement the directive by Dec. 17, 2021, Italy only transposed the *body of* EU law with **Legislative Decree March 10, 2023, no. 24, which** came into force on March 30 and whose provisions took effect as of July 15, 2023, with the exemption provided for the private sector for entities that employed an average of no more than 249 workers in the last year, for which the obligation to establish the internal reporting channel will take effect as of Dec. 17, 2023.

The national legislature intended to gather in a single regulatory text the entire discipline of reporting channels and protections accorded to whistleblowers in both the public and private sectors, seeking to ensure maximum harmonization: as a result of the provisions of the decree, both Art. *54-bis* of Legislative Decree 165/2001 (T.U.P.I.) for public entities and Art. 6, paragraphs *2-ter* and *2-quater* of Legislative Decree 231/2001 for private entities, while Art. 6 paragraph *2-bis* was amended[1] .

In light of the requirements introduced by the implementing decree, as far as the area of interest is concerned, the obligations falling on private entities have become more substantial, and the subjective and objective scope of reporting protocols has been expanded.

Regarding the **subjective scope of application**, compared to the previous legislation that limited *whistleblower* protection to workers or collaborators of entities that had adopted the 231 organizational model, there is a significant expansion of the category of private entities subject to the *aforementioned* legislation, which are identified on the basis of different criteria (size of the staff,

[1] Which currently reads, "the *models referred to in paragraph 1(a) provide, pursuant to the legislative decree implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, the internal reporting channels, the prohibition of retaliation, and the disciplinary system adopted pursuant to paragraph 2(e).*"

performance of activities in the sectors governed by European law; adoption of the organizational and management models provided for in Legislative Decree No. 231/01).

Significantly, these are the entities that:

- ⇒ have employed, in the last year, an average of **at least fifty** employees with permanent or fixed-term employment contracts (Art. 2(*q)*(1));
- ⇒ although they have not employed an average of at least fifty employees with permanent or fixed-term employment contracts in the last year, nevertheless, they fall within the scope of application of the Union acts referred to in Parts I.B and II of Annex 1 to Decree No. 24/2023 (cf. Annex 1 "List of EU Acts and National Implementing Provisions Relevant to the Scope of Legislative Decree No. 24 of 2023") in the **area of financial services, products and markets and prevention of money laundering and terrorist financing, environmental protection and transport safety** (Art. 2, para. 1(*q)*(2));
- ⇒ which, other than those indicated in the aforementioned Art. 2, para. 1, letter *q)* no. 2, fall within the scope of application of Legislative Decree no. 231/2001, **adopt organization and management models** provided *therein*, if in the last year they have employed an average of **at least fifty** subordinate **workers** with permanent or fixed-term employment contracts;
- ⇒ who, other than those indicated in the aforementioned Art. 2, para. 1, lett. q) no. 2, fall under the scope of Legislative Decree No. 231/2001, **adopt the organization and management models** provided *therein*, even if in the last year **they have not reached an average of at least fifty employees** with permanent or fixed-term employment contracts (Art. 2, para. 1, lett. q), no. 3). In essence, such entities are required to comply with the *whistleblowing* provisions, even if they employ fewer than fifty employees, but only if they adopt the organization and management models already provided for in Article 6 of Legislative Decree No. 231/2001[2] .

The range of private-sector individuals, then, who are assured protection in the new decree is much broader than in the previous legislation and includes:

[2] This, as clarified in the Explanatory Report to the outline of Decree No. 24/2023, was provided in order not to undermine the protections in this matter already provided even to entities with fewer than fifty employees under the 231 regulations.

⇒ **employed workers** (Art. 3, co. 3 lett. c), including: workers whose employment relationship is governed by Legislative Decree No. 81/2015[3] ; workers who perform occasional services (whose employment relationship is governed by Art. *54-bis* of Legislative Decree No. 50/2017, conv. with mm.ii. by Law No. 96/2017);

⇒ **self-employed workers** (Art. 3, para. 3 lett. d), who carry out their work activities with entities in the private sector, including: self-employed workers indicated in Chapter I of l. No. 81/2017[4] ; holders of a collaboration relationship referred to in Article 409 of the Code of Civil Procedure[5] ; holders of a collaboration relationship referred to in Article 2 of Legislative Decree No. 81/2015[6];

⇒ **freelancers and consultants** (Art. 3, para. 3(e)), who work for private sector entities;

⇒ **volunteers** and **trainees**, (art. 3, para. 3 lett. f), paid and unpaid, working in private sector entities[7];

⇒ **shareholders** (Art. 3, para. 3(h)), individuals who hold shares in one of the private sector entities, where the latter take on a corporate form.

⇒ **persons with functions of administration, management, control, supervision or representation**, (Art. 3, para. 3 lett. h), even if these functions are exercised on a de facto basis, at entities in the private sector[8] .

The protection applies not only if the reporting, whistleblowing or public disclosure takes place during the constancy of the employment or other legal relationship, but also during the probationary period

[3] These are, for example, part-time, intermittent, fixed-term employment relationships.

[4] These are workers with self-employment relationships governed by Title III of Book V of the Civil Code, including work contracts under Article 2222 of the same Civil Code. These include, for example, self-employed workers in the intellectual professions for the exercise of which registration in special registers or lists is required such as psychologists, architects, surveyors etc.

[5] We are referring to the relationships indicated in No. 3 of the provision, i.e., agency, commercial representation and other collaborative relationships that result in the provision of continuous and coordinated, predominantly personal work, although not of a subordinate nature. For example, lawyers, engineers, social workers who perform their work for a private sector entity by organizing it independently (parasubordinate relationship).

[6] These are-according to co. 1 of the aforementioned provision-collaborations organized by the principal that result in exclusively personal and continuous work, the manner of performance of which is organized by the principal also with reference to "the time and place of work" (so-called "hetero-organization").

[7] These are individuals who may be in a privileged situation as witnesses to wrongdoing and who are nevertheless at risk of retaliation for reporting violations. Retaliation against these individuals could take the form of, for example, no longer using their services, giving them negative work references, or otherwise damaging their reputation or career prospects.

[8] These may be, for example, members of boards of directors, even without executive positions, or members of Supervisory Boards (SBs).

before (e.g., in the pre-contractual stage) or after the establishment of the legal relationship (Art. 3(4)).

In addition, the new legislation (Art. 3(5)) expands the group of persons-other than the whistleblower[9] -against whom the protection measures the prohibition of retaliation apply, including:

⇒ the so-called **facilitator**[10] , i.e., the physical person who assists the reporter in the reporting process, operating within the same work environment and whose assistance must be kept confidential;

⇒ persons in the same work environment as the reporter who are related to them by a stable **emotional or kinship relationship** within the fourth degree;

⇒ **co-workers** of the whistleblower, who work in the same work environment as the whistleblower and have a regular and current relationship with said person;

⇒ **entities** owned-exclusively or in majority third-party ownership-by the reporter; entities at which the reporter works; entities that operate in the same work environment as the reporter.

Regarding the **objective scope**, the new legislation has a broader scope than the scope outlined in the European Directive: it includes not only the violations of Union law indicated in Article 2(2) of the Directive, but also those of national law. Reports, in order to fall within the scope of Legislative Decree 24/2023, must relate to "*violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity***,**" knowledge of which occurred in the "work *context.*"[11] .

[9] This is an absolute novelty, as it is a hypothesis that the previous Law 179/2017 did not foreshadow.

[10] The definition of "facilitator" in the decree refers to an individual who provides advice and support to the reporter. It also refers to a person operating in the same work environment as the reporter. By way of example, the facilitator could be a colleague in a different office from that of the reporter who assists the reporter in the reporting process on a confidential basis, that is, without disclosing the information learned. The facilitator could be a colleague who also holds the title of trade unionist if he or she assists the reporter in his or her name and on his or her behalf, without expensing the trade union acronym. It should be noted that if, on the other hand, he or she assists the whistleblower by using the union acronym, he or she does not play the role of facilitator. In this case, the provisions on the consultation of union representatives and the repression of anti-union conduct under Law No. 300/1970 remain applicable.

[11] While excluded from the new discipline are objections, claims or requests related to an interest of a personal nature of the reporter or pertaining exclusively to his/her individual labor or public employment relationships, or inherent to his/her labor or public employment relationships with hierarchically superordinate figures; reports of violations where they are already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to the Decree or by national acts that constitute implementation of the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, albeit not indicated in Part II of the Annex to this Decree; reports of violations relating to national security, as well as procurement

In particular, taking into account the breadth of cases that can be reported, the legislature has typified the offenses, acts, behaviors or omissions that can be reported, referring to Article 2 (*Definitions*) to define what qualifies as a violation:

- ⇒ with regard to violations of national law, in addition to **civil** and **administrative offenses**, which were already included in the scope defined by the previous legislation, together with **unlawful conduct relevant under Legislative Decree No. 231/2001** and violations of organization and management models, what is new is the extension of the object of reporting to all **criminal offenses** and **accounting offenses** (not only those relevant under Legislative Decree No. 231/2001), while mere irregularities are no longer included among violations of national law;
- ⇒ with regard to **violations of European Union law, these are** all offenses committed in violation of the EU legislation listed in Annex 1 to Legislative Decree No. 24/2023 and all national provisions implementing it (even if the latter are not expressly listed in the said Annex) (Art. 2, co. 1(a) no. 3); all acts or omissions affecting the financial interests of the European Union within the meaning of Article 325 of the T.F.U.E. as identified in EU regulations, directives, decisions, recommendations and opinions (Art. 2, co. 1(a) no. 4); all acts or omissions concerning the internal market that undermine the free movement of goods, persons, services and capital (Art. 26(2) TFEU), as well as violations concerning the internal market related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law (Art. 2, co. 1(a) No. 5); acts or conduct that frustrate the object or purpose of the provisions of the European Union in the areas of Nos. 3, 4 and 5 (Art. 2, co. 1(a) No. 6).

There is to emphasize that, subject to the general rules, a specific delimitation of the objective scope applies in the private sector, based on the different subjective qualification of the entity mentioned in the previous paragraph:

relating to defense or national security aspects, unless such aspects are covered by the relevant secondary law of the European Union (Art. 1 para. 2).

⇒ for private entities that have adopted an organizational model and have fewer than the average number of employees in the last year of 50, the objective scope is still limited to only those reports pertaining to violations of the 231 regulations or the 231 organizational model and only through the internal channel;

⇒ while entities that have adopted an organizational model but have an average of more than 50 employees, it is also possible to make internal, external, public disclosures or reports to the judicial or accounting authorities of violations of national legislation implementing EU acts on public procurement, services, financial products and markets, and prevention of money laundering and terrorist financing, transportation safety, environmental protection, public health, consumer protection, privacy and personal data protection, and network and information system security.

LEGISLATIVE DECREE NO. 24 OF MARCH 10, 2023: THE REPORTING CHANNELS

The decree, in implementing the directions of the European Directive, provided for a diversified system of reporting:

⇒ first, it stipulated that appropriate **internal channels** should be arranged within the entities to which the regulations apply to receive and process reports;

⇒ secondly, it identified the possibility for reporters, where specific conditions apply, to have recourse to an **external channel** activated at A.N.A.C.

⇒ at the same time, also provided for the possibility of making a **public disclosure**, if special conditions are met in this case as well;

⇒ Finally, the decree, in incorporating the indication contained in the European legislation, stipulates that a **complaint** must be made in cases where Union or national law requires reporting persons to address the competent national authorities, for example, as part of their professional duties and responsibilities or because the violation constitutes a crime.

a. Internal reporting channels

The decree prescribes the obligation to activate its own system of internal reporting channels[12] :

⇒ that ensures, including through the use of encryption tools, the confidentiality of the identity of the reporting person, the person involved and the person in any way mentioned in the report, as well as the content of the report and related documentation;

⇒ to be managed by a dedicated autonomous internal person or office with specifically trained personnel to manage the reporting channel, or by external personnel, provided they are autonomous and specifically trained;

[12] Keep in mind, however, that private entities that have employed an average of no more than 249 employees in the past year may share the internal reporting channel and its management (Art. 4 Paragraph 4).

⇒ which provides for the formulation of the report in writing, including by computer, or orally, or, at the request of the reporter, including through a face-to-face meeting set within a reasonable period of time;

⇒ stipulating, in the case of a report submitted outside the modalities referred to in the preceding paragraph, that it shall be forwarded within seven days of receipt to the competent person, at the same time giving notice of the transmission to the reporting person.

As part of the management of the internal reporting channel, the person or internal office or external party entrusted with the management of the channel shall:

⇒ Issue the reporting person with an acknowledgement of receipt of the report within seven days from the date of receipt;

⇒ Maintain interlocutions with the reporting person and, if necessary, request additions;

⇒ Diligently follow up on reports received;

⇒ Provide acknowledgement of the report within three months from the date of the acknowledgement of receipt or in any case within three months from the expiration of the seven-day period from the date of receipt;

⇒ Make available clear information on the channel, procedures and prerequisites for making reports (possibly, also on the appropriate section of the *website*).

It is essential that the institution make it clear to those interested in making a report that they should clearly indicate in the subject line of the report that it is a report for which they intend to keep their identity confidential and benefit from the protections provided in the event of any retaliation suffered as a result of the report.

This specification allows, where the report is mistakenly received by a non-competent person or through a channel other than those specifically provided for in the decree, for timely transmission by the latter to the person authorized to receive and handle *whistleblowing* reports.

Such information must be clear and easily accessible, including, as far as possible, to persons who, although not attending workplaces, are legitimately entitled to submit *whistleblowing* reports. It should be displayed, for example, in the workplace in a visible place, accessible to all such persons as well as

in a special section of the institution's institutional website and also be included in ethics and integrity courses and trainings.

b. The external reporting channel

Without prejudice to the preference for the internal channel, the decree provides for the possibility of reporting through a so-called external channel, managed by the National Anticorruption Authority. Access to this channel, however, is allowed only under certain conditions expressly provided for by the legislature. Specifically, the reporting person may make an external report if, at the time of its submission:

⇒ the internal channel despite being mandatory, is not active or, even if activated, does not comply with the provisions of the decree with reference to the subjects and methods of submission of internal reports, which must be able to guarantee the confidentiality of the identity of the reporter and other protected subjects;

⇒ the reporting person has already made an internal report and it has not been followed up;

⇒ the reporting person has reasonable grounds to believe that if he or she were to make an internal report it would not be effectively followed up or that the report itself might result in the risk of retaliation;

⇒ the reporting person has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest.

External reports are made in written form through the IT platform or orally through telephone lines or voice messaging systems or, at the request of the reporting person, through a face-to-face meeting set within a reasonable period of time. An external report submitted to a person other than ANAC shall be forwarded to ANAC, within seven days from the date of its receipt, giving simultaneous notice of the transmission to the reporting person.

c. Public disclosure

With public disclosure, information about violations is brought into the public domain through the press or otherwise through means of dissemination capable of reaching a large number of people, including *social networks* and new communication channels (e.g., *facebook, twitter, youtube, instagram*) that constitute a rapid and interactive means of transmitting and conveying information and exchanges between networks of people and organizations. Public disclosure of violations must take place in compliance with the conditions set by the legislature so that then the person making the disclosure can benefit from the recognized protections. Therefore, protection will be recognized if one of the following conditions is met at the time of disclosure:

(i) an internal report, which was not responded to by the entity regarding the measures planned or taken to follow up the report within the timeframe, was followed up by an external report to ANAC, which, in turn, did not provide feedback to the reporter within a reasonable timeframe;

(ii) the person directly makes a public disclosure because on the basis of reasonable grounds grounded in light of the circumstances of the particular case, he or she believes that the violation may pose an imminent or obvious danger to the public interest;

(iii) the person directly makes a public disclosure because on the basis of reasonable grounds grounded in the light of the circumstances of the particular case, he or she believes that the external report may pose a risk of retaliation or may not be effectively followed up because, for example, he or she fears that evidence may be concealed or destroyed or that the person who received the report may be colluding with or involved in the perpetrator of the violation.

d. The anonymous tip

Legislative Decree 24/2023 does not specifically indicate the fate of anonymous reports, nevertheless the ANAC Guidelines have confirmed that anonymous reports, where substantiated, are equated with ordinary reports and in that case considered in their "ordinary" supervisory procedures: public sector and private sector entities that receive reports through internal channels consider anonymous reports as ordinary reports to be treated according to the criteria established in their respective regulations.

In any case, the anonymous reporter or whistleblower, subsequently identified, who has notified ANAC that he or she has suffered retaliation may benefit from the protection that the decree guarantees against retaliatory measures. Entities that receive reports through internal channels and the Authority itself are, therefore, required to record anonymous reports received and keep the relevant documentation no later than five years from the date of receipt of such reports, thus making it possible to trace them, should the reporter, or whistleblower, notify ANAC that they have suffered retaliatory measures because of that anonymous report or complaint.

LEGISLATIVE DECREE NO. 24 OF MARCH 10, 2023: THE PROTECTIONS

The protection system provided by Legislative Decree No. 24/2023 consists of the following types of protection:

⇒ The **protection of the confidentiality** of the reporter, the facilitator, the person involved, and the persons mentioned in the report;

⇒ **protection from any retaliatory measures** taken by the entity by reason of the report, public disclosure or denunciation made with related benefit of reversal of the burden of proof in favor of the person who suffers any retaliatory or potentially retaliatory conduct;

⇒ **limitations on liability with respect to the** disclosure and dissemination of certain categories of information that operate under certain conditions;

⇒ The provision of **support measures by** Third Sector entities included in a special list published by ANAC.

a. The protection of confidentiality

The obligation to protect confidentiality requires that any disclosure of the identity of the reporting person to persons other than those competent to receive or follow up on reports should always take place with the express consent of the reporting person.

The prohibition of revealing the identity of the reporter is to be referred not only to the **name of** the reporter but also to any **other information or element of the report**, including the documentation attached to it, from the disclosure of which the identity of the reporter can be deduced directly or **indirectly**: the processing of all these elements must therefore be marked by the utmost caution, starting with the obscuring of personal data, especially those relating to the reporter but also of other subjects whose identity under d.lgs. 24/2023 must remain confidential, if, for investigative reasons, other subjects must also be made aware of the content of the report and/or the documentation attached to it.

The protection of confidentiality must also be ensured in **judicial** and **disciplinary proceedings**. Similar to what was already provided for in the previous legislation, Legislative Decree 24/2023 specifies that: in criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure. (closure of investigations); in proceedings before the Court of Auditors, the obligation of investigative secrecy is provided for until the closure of the investigative phase; in the context of disciplinary proceedings, the identity of the reporter cannot be disclosed, where the accusation of the disciplinary charge is based on separate and additional investigations to the report, even if consequent to it.

In cases where the identity of the whistleblower is indispensable to the defense of the person facing the disciplinary charge, it may be revealed **only with the express consent of the whistleblower**. The decree provides two cases in which prior written notice of the reasons behind the disclosure of the identity of the whistleblower and prior express consent of the whistleblower must concur in order to reveal the identity of the whistleblower: the first hypothesis occurs where in the context of a disciplinary proceeding initiated against the alleged perpetrator of the reported conduct, the identity of the reporter is indispensable for the defense of the person to whom the disciplinary charge has been contested; the second hypothesis occurs, on the other hand, where in internal and external reporting procedures the disclosure of the identity of the reporter is also indispensable for the defense of the person involved.

The decree, with a view to extending the system of protections as far as possible, recognized that confidentiality should also be guaranteed to **persons other than the whistleblower**: it expressly provides that identity protection should also be guaranteed to the ***reported natural person***, i.e., to the person to whom the violation is attributed in the public disclosure (c.d. ***involved person***); to the ***facilitator both with regard to*** identity and with reference to the activity in which the assistance takes place; and to ***persons other than*** the person reported but nevertheless implicated insofar as they are mentioned in the report or public disclosure (think, for example, of persons named as witnesses).

The *rationale for the* new discipline is to be found in the need to safeguard the rights of individuals who, as a result of reporting, could suffer damage to their reputation or other negative consequences even before it is proven whether or not they are unrelated to the reported facts. Indeed, the risk is not

only that of creating a negative impression on others, but the much more concrete and afflictive risk of losing trustworthiness. The unveiling of the latter's identity would result in considerable damage both to the individual-in terms of credibility and reliability-and to the company, which, in addition to reputational damage, would also suffer negative economic consequences.

An exception to this duty of confidentiality of the persons involved in or mentioned in the report is the case where the reports are reported to the Judicial Authorities and the Court of Auditors, in order to enable them to proceed with the investigation having a complete picture of the reported fact and acquiring as much information as possible to pronounce on the case in question.

Article 14 of the decree prescribes the **retention of internal and external reports** and related documentation for as long as necessary for their determination and, in any case, for not more than five years from the date of communication of the final outcome of the reporting procedure, subject to confidentiality obligations.

b. The prohibition of retaliation

The decree provides for the prohibition of so-called **retaliation**: "*any conduct, act or omission, even if only attempted or threatened, carried out by reason of the report, report to the judicial or accounting authority, or public disclosure and which causes or may cause the reporting person or the person who made the report, directly or indirectly, unjust damage.*"

In discontinuity with the past, Legislative Decree No. 24/2023 in providing a definition of retaliation also includes therein those "*only attempted or threatened*" (it then becomes the burden of the person who has even only attempted the retaliation or threatened it to prove that the facts attached by the reporter are unrelated to the report, denunciation, public disclosure made) and greatly expands **the list of cases** that constitute retaliation, although this is non-exhaustive in nature:

⇒ dismissal, suspension or equivalent measures;

⇒ Grade demotion 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;

⇒ demerit notes or negative references;

⇒ Adoption of disciplinary measures or other sanction, including fines;

⇒ coercion, intimidation, harassment or ostracism;

⇒ discrimination or otherwise unfavorable treatment;

⇒ failure to convert a fixed-term employment contract to a permanent employment contract where the employee had a legitimate expectation of said conversion;

⇒ Non-renewal or early termination of a fixed-term employment contract;

⇒ damage also to the person's reputation, particularly on *social media*, or financial economic harm, including loss of economic opportunities and loss of income;

⇒ inclusion on improper lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;

⇒ Early termination or cancellation of the contract for the provision of goods or services;

⇒ Cancellation of a license or permit;

⇒ Request for submission to psychiatric or medical examinations.

In order for retaliation to occur and, consequently, for the person to be eligible for protection, a close connection is required between the reporting, disclosure, and whistleblowing and the unfavorable behavior/act/omission suffered, directly or indirectly, by the person reporting, whistleblowing, or making the public disclosure.

To enjoy the protection:

⇒ Whistleblowers or whistleblowers must reasonably believe, including in light of the circumstances of the particular case and the data available at the time of reporting, public disclosure, or whistleblowing, that the information about the reported, disclosed, or whistleblowing violations is true. On the other hand, mere assumptions or rumors as well as news in the public domain are not sufficient. This is an essential safeguard against damaging or offensive reporting and ensures that those who, have deliberately and knowingly reported, publicly disclosed, or denounced erroneous, patently unsubstantiated, or misleading information do not enjoy protection.

⇒ On the other hand, the fact that the person reported, made public disclosures or complaints while being uncertain of the actual occurrence of the facts reported or denounced and/or the identity of the author thereof or even reporting inaccurate facts due to genuine error is not relevant to the protections.

For the purposes of protection, however, no relevance is attached to the personal and specific reasons that led individuals to make the report, public disclosure or complaint.

The protection provided in the event of retaliation does not apply in the event of a finding by a judgment, even if not final of first instance against the reporter of criminal liability for the crimes of slander or defamation or otherwise for the same crimes related to the complaint, or civil liability, for having reported false information reported intentionally with malice or negligence (see Art. 16, para. 3 Legislative Decree No. 24/2023).

In cases where the aforementioned responsibilities are established, a disciplinary sanction should also be applied to the reporting and whistleblower. Therefore, it is necessary for entities to include this specific sanctionable case in their codes of conduct or 231 Models.

Legislative Decree No. 24/2023 regulates communications to ANAC of retaliation that subjects believe they have suffered as a result of the public reporting, whistleblowing or disclosure made. Element of novelty is that the new discipline includes among the subjects who can communicate to ANAC the retaliatory measure also those who having a qualified connection with the reporter, whistleblower or public discloser suffer retaliation because of said connection. These are: facilitators, people in the same work context, co-workers, and even legal entities in cases where they are entities owned by the whistleblower, whistleblower, public discloser or entities in which he or she works or entities that operate in the same work context. Excluded from the possibility of reporting to ANAC, in discontinuity with the past, are the most representative labor organizations in the administration/entity where the retaliation took place.

The possibility for the whistleblower to report retaliatory measures directly to the Labor Inspectorate has also been eliminated (see Article 6, paragraph *2-ter*, of Legislative Decree No. 231/2001): the sole competence of ANAC has been provided for in the private sector as well. The involvement of the Inspectorate can only take place through ANAC, which remains the only entity competent to assess

the elements acquired and the possible application of administrative sanctions under Article 21 of the Decree.

In continuity with the past, on the other hand, the easing of the evidentiary burden on the retaliating party has also been maintained in the new regulatory framework: indeed, Art. 17, expressly prescribes, "*In the context of judicial or administrative proceedings or otherwise extrajudicial disputes having as their object the ascertainment of the conduct, acts or omissions prohibited under this article against the persons referred to in Article 3, paragraphs 1, 2, 3 and 4, it shall be presumed that the same have been put in place as a result of the reporting, public disclosure or complaint to the judicial or accounting authority. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting, public disclosure or complaint shall be on the person who put them in place.*"

c. Limitations of liability

To the set of protections recognized by the discipline to the reporter, whistleblower or person making a public disclosure must also be ascribed the limitations of liability with respect to the disclosure and dissemination of certain categories of information, for example, covered by secrecy, authorial prerogatives or protected by data protection regulations, or offending the reputation of the person involved or reported. These are limitations (*rectius of* a scrimination of a general nature) that operate when two certain conditions are met, in the absence of which there would be consequences in terms of criminal, civil, and administrative liability:

(i) at the time of disclosure or dissemination there are reasonable grounds to believe that the information is necessary for the breach to be discovered.

The person, therefore, must reasonably believe, and not on the basis of mere inferences, that that information must disclose itself because it is essential to bring out the violation, to the exclusion of superfluous information, and not for additional and different reasons (e.g., vindictive, opportunistic, or scandalous purposes);

(ii) the reporting, public disclosure or denunciation was made in compliance with the conditions set forth in Legislative Decree No. 24/2023 to benefit from the protections.

This is without prejudice only to criminal liability in cases where the acquisition of or access to information about violations constitutes a crime. The applicability of the exemption is, on the other hand, excluded for conduct that is not strictly necessary to disclose the violation or, in any case, unrelated to public reporting, whistleblowing or disclosure.

d. Support measures

To further strengthen the protection of the whistleblower, the legislature for the first time provides for the possibility for ANAC to enter into agreements with Third Sector entities so that they provide support measures to the whistleblower. In particular, these entities, included in a special list published by ANAC on its institutional website, provide assistance and advice free of charge on how to report; on the protection from retaliation recognized by national and European Union regulatory provisions; on the rights of the person involved; and on the terms and conditions of access to legal aid.

LEGISLATIVE DECREE NO. 24 OF MARCH 10, 2023: THE PENALTIES

Without prejudice to other profiles of responsibility, ANAC, when it ascertains at the outcome of the investigation that ***(i)*** retaliatory measures were taken, or the report was obstructed or attempted to be obstructed, or the obligation of confidentiality was violated, applies administrative pecuniary sanctions (from 10,000 to 50,000 euros) to the person responsible.

Administrative pecuniary sanctions (EUR 10,000 to EUR 50,000) are also provided for the failure to establish reporting channels, in the event that procedures for forwarding and handling reports have not been adopted or the adoption of such procedures does not comply with those provided for internal channels, as well as when it determines that the verification and analysis of the reports received has not been carried out ***(ii)***.

Finally, ANAC applies a fine of 500 to 2,500 in the case referred to in Art. 16, paragraph 3 ("when the *criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority or his civil liability, for the same title, in cases of wilful misconduct or gross negligence*") is *established*, unless the reporting person has been convicted, also at first instance, for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority ***(iii)***.

Entities in the private sector shall provide in the disciplinary system adopted pursuant to Legislative Decree No. 231/2001, disciplinary sanctions against those found to be responsible for the offenses referred to in points ***(i),*** (***ii)*** and ***(iii)*** above.

SUMMARY FRAMEWORK FOR PRIVATE ENTITIES: THE REGULATIONS APPLICABLE TO S.G.I. S.P.A.

In light of the complex regulatory framework introduced by Legislative Decree 24/2023l, it was deemed necessary to summarize the regulations specifically applicable to the current organization of S.G.I. S.p.A., in the outline below.

S.G.I. S.p.A. falls into the category of "*private entities*" referred to in Article 2, paragraph 1, letter q) of Legislative Decree No. 24/2023: these are entities other than those falling under the definition of public sector entities that have employed, in the last year, an average of at least fifty subordinate workers with permanent or fixed-term employment contracts.

Protection is provided for persons referred to in paragraphs 3 or 4 of Art. 3, i.e., employees (Art. 3, co. 3 lett. c); self-employed (Art. 3, co. 3 lett. d) freelancers and consultants (Art. 3, co. 3 lett. e), volunteers and trainees, (Art. 3, co. 3 lett. f), shareholders (art. 3, co. 3 lett. h), persons with functions of administration, management, control, supervision or representation, with extension also to persons other than the reporter for whom protection is provided (see *supra*), who make internal or external reports, public disclosures or reports to the judicial or accounting authorities of information violations referred to in Art. 2 co. 1 lett. *a)* n. 2), 3), 4), 5),6), i.e., illegal conduct relevant under Legislative Decree No. 231 of June 8, 2001, or violations of the organization and management models provided therein and violations of national legislation implementing EU acts or Euro-Union legislation as exemplified above[13] .

Therefore, the Company that has chosen to adopt an Organization, Management and Control Model pursuant to Legislative Decree No. 231/2001 must have multiple internal reporting channels that comply

[13] With reference to the type of violations that can be the subject of internal/external reporting, public disclosure or denunciation to the authority, it should be pointed out that the new version of Art. 3, para. 2 (b), does not mention violations under Art. 2(1)(a)(1) (*i.e.* conduct that harms the public interest or integrity of the public administration or entity and that consists of administrative, accounting, civil or criminal offenses that do not fall under numbers 3), 4), 5), and 6) of Art. 2(1)(a)). In fact, the provision under comment refers exclusively to the violations "referred to in *Article 2, paragraph 1 (a), number 2)*" and "*violations referred to in Article 2, paragraph 1 (a), numbers 3), 4), 5), and 6).*"
The previous version of Art. 3(2)(b), on the other hand, stipulated that for entities with MOG 231, the provisions of the Scheme applied to persons who make internal reports or public disclosures or reports to the judicial or accounting authorities of information on violations under Art. 2(1)(a) (thus including all cases, including that covered in No. 1) of the same article.

with the conditions prescribed by Legislative Decree No. 24/2023 regarding information clarity (*i.e.* information on the *website* of the internal reporting protocol, but also of the conditions of reporting of possible retaliation of the whistleblower or other persons protected by the legislation to the National Anticorruption Authority) and protective measures (see *above)* and ensures the necessary information in training regarding the other reporting channels (external, public disclosure, whistleblowing).

The company must also have a disciplinary system, which covers any violation of the 231 Model and the procedures for handling *whistleblowing* indicated in this protocol. With reference to the disciplinary system, Legislative Decree No. 24/2023, in addition to the general configuration, imposes for the entities to which S.G.I. S.p.A. belongs, specifically:

⇒ to prepare a specific disciplinary sanction against those found to be responsible for violating the duty of confidentiality in handling reports;

⇒ to prepare a specific disciplinary sanction against the reporting person when he/she is convicted by a judgment (including non-final first-degree judgment) that has established criminal liability for the crimes of slander or defamation in reference to the facts that are the subject of the report or civil liability, for intentionally reporting false information with malice or negligence;

⇒ to prepare specific disciplinary sanctions against those who have taken retaliatory measures, obstructed reporting, or violated the duty of confidentiality;

⇒ to set up specific disciplinary sanctions against *management that has* failed to adopt appropriate reporting channels or failed to adopt procedures for the submission and handling of reports, or failed to verify and analyze reports received.

DEFINITIONS

For the purposes of **this protocol**, the following definitions apply:

Whistleblower or reporting person: an individual who makes a report of information about violations acquired within his or her work context;

Facilitator: an individual who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;

Internal reporting: the written or oral communication of information about violations through the internal reporting channel.

Work context: present or past work/professional activity performed in the context of employment relationships relevant to the regulations (see *above).*

Person involved: the natural or legal person mentioned in the internal report as the person to whom the violation is attributed or as a person otherwise implicated in the reported violation**;**

Violation: behaviors, acts or omissions that harm or are potentially capable of harming the interest and integrity of the entity, based on concrete symptomatic indices and including any conduct that violates the prescriptions and procedures contained in the Organization, Management and Control Model adopted by the Company, as well as any conduct that is relevant-even if only as attempted or threatened-under Legislative Decree No. 231 of June 8, 2001, as a potential predicate offense for the entity's liability or otherwise an offense relevant to the company's civil, accounting and administrative liability.

External reporting: information of the violation of the Euro-Union legislation relevant for the purposes

of Legislative Decree No. 24/2023 and the national implementing legislation, which is transmitted through the external reporting channel arranged by ANAC and accessible at the *link* indicated in this protocol, or which is conveyed through public disclosure under the conditions prescribed by Legislative Decree No. 24/2023 (see *above*).

Follow-up: action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigation, and any measures taken**;**

Acknowledgement: communication to the reporting person of information regarding the follow-up that is given or intended to be given to the report.

Company: Società Gasdotti Italia S.p.A., headquartered in Milan, Via Della Moscova 3, having as its object the transportation, dispatching, distribution and storage of liquid and gaseous hydrocarbons of all kinds and other gases and gas mixtures of renewable origin; as well as the design, construction and operation of plants for transportation, or other water infrastructure and the provision of services related to the indicated activities.

Recipient: body responsible for receiving reports, identified, in order to ensure the functionality and confidentiality of the procedure, in the Company's Supervisory Board; only alternatively, an external *231 compliance* reference professional.

PURPOSE OF THE *WHISTLEBLOWING* PROTOCOL

The purpose of the document is to remove factors that may hinder or discourage reports of potential wrongdoing detrimental to the Company. With this in mind, the objective pursued by this procedure is to provide the *whistleblower* with clear operational indications in relation, on the one hand, to the subject, content, Recipient and method of transmission of reports and, on the other hand, to outline a sufficiently defined information framework on the forms of protection offered to him or her by the

regulations and the potential liability to which he or she is exposed in the event of abuse of the instrument.

OBJECT OF THE REPORT

The following are the object of internal reporting: unlawful conduct relevant under Legislative Decree No. 231 of June 8, 2001, thus the facts listed in the so-called *predicate offenses* indicated in the General Section of the Organization and Management Model adopted by the Company; any pathological malfunction of the activity within the Company that denotes a violation of the control principals laid down in the Organization and Management Model adopted by the Company or is potentially capable of causing harm to the Company and its personnel.

The subject of the possible external reporting are: violations of European Union law, this is all offenses committed in violation of the EU legislation indicated in Annex 1 to Legislative Decree No. 24/2023 and all national provisions implementing it (even if the latter are not expressly listed in the said Annex) (Art. 2, co. 1(a) no. 3); all acts or omissions affecting the financial interests of the European Union within the meaning of Article 325 of the T.F.U.E. as identified in EU regulations, directives, decisions, recommendations and opinions (Art. 2, co. 1(a) no. 4); all acts or omissions concerning the internal market, which undermine the free movement of goods, persons, services and capital (Art. 26(2) TFEU), as well as violations concerning the internal market related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law (Art. 2, co. 1(a) No. 5); acts or conduct that frustrate the object or purpose of the provisions of the European Union in the areas of Nos. 3, 4 and 5 (Art. 2, co. 1(a) No. 6)[14] .

The information may concern both violations that have been committed and those that have not yet been committed that the *whistleblower* reasonably believes could be committed based on concrete evidence. Those elements that concern conduct aimed at concealing violations (think, for example, of the concealment or destruction of evidence about the commission of the violation) may also be subject to reporting.

They are not eligible for reporting:

[14] Indication by Confindustria - Legislative Affairs (doc. dated April 13, 2023 "*Whistleblowing Decree: the new discipline*"), where it is highlighted that for entities with MOG 231 the use of ANAC's external reporting channel is limited to cases of reports of violations of Union law.

⇒ information that is patently unsubstantiated or information that is already totally in the public domain;

⇒ information acquired only on the basis of poorly reliable indiscretion or rumor (so-called rumors);

⇒ disputes, claims or demands related to an interest of a personal nature of the reporting person or the person making a complaint to the judicial or accounting authority that relate exclusively to his or her individual labor relations, i.e., inherent in his or her labor relations with hierarchically subordinate figures (i.e., are therefore, excluded, for example, reports concerning labor disputes, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker)

⇒ violations where they are already mandatorily regulated by the European Union or national acts specified in Part II of the Annex to the Decree or by national acts that constitute implementation of the European Union acts specified in Part II of the Annex to Directive (EU) 2019/1937, albeit not specified in Part II of the Annex to the Decree.

⇒ violations of national legislation already covered in European Union directives and regulations and in the implementing provisions of the Italian legal system that already guarantee appropriate reporting procedures.

The whistleblower must provide all the elements relevant to the reconstruction of the fact aimed at ascertaining the merits of what was reported. In particular, it is necessary to be clear:

⇒ The generalities, job title or position, place of employment and contact information of the reporter;

⇒ The circumstances of time and place under which the reported event occurred;

⇒ description of the fact;

⇒ generalities or other elements that would allow the person involved to be identified;

⇒ The particulars of any other individuals who may report on the facts being reported;

⇒ Any other information or documentation that may provide grounds for the facts that are the subject of the report.

TRANSMISSION OF INTERNAL REPORTING

In compliance with national and European regulatory requirements, the Company has adopted an **internal reporting** channel, which allows the reporter to forward the communication to the Recipient either in an *open form* (in which the reporter gives consent to the disclosure during the investigation of his or her personal details); or in a *confidential form* (in which the reporter discloses his or her name to the Recipient but does not give consent to its disclosure); or in *an anonymous form* (in which the reporter does not disclose his or her name even to the Recipient).

In particular, an initial information channel that can be used for reports intended to remain *confidential* or *open* is established, which allows the reporter to forward from his or her company e-mail address an *e-mail* to the e-mail address of the Recipient odv@sgispa.com, or to contact him or her by telephone from company devices at the following dedicated telephone number: (+39) 0775886098, to make the report orally or request a face-to-face meeting.

The written report must be made by completing both pre-formed forms-attached to this protocol (see Doc. 01, Doc. 02)-which are to be forwarded via *email* with the *personal confidentiality* wording in the subject line and recorded as "*Form 1: data of the reporter*" and "*Form 2: content of the report*," without any other identification.

In order to maximize the protection of the whistleblower's confidentiality, the Company has also provided for the possibility of sending forms by *e-mail* through the *specially* created *e-mail* address segnalazioniodvsgi@gmail.com.

The user name and password to access the *mailbox* are shared with all employees of the Company and included in the *whistleblowing* protocol information to be also transmitted to suppliers/consultants/external collaborators of S.G.I. S.p.A.

This *mailbox* has a "*Flow Crypt"* plugin that exploits a mixed encryption system with three algorithms: the RSA public key system, the IDEA private key system, and the MD5 hashing algorithm. How it works is very simple: if user A wants to send user B a message, PGP encrypts that message using IDEA with a randomly generated key K that will be sent to user B encrypted with his public key with the RSA algorithm, along with the message encrypted with IDEA; thus only B will be able, with his own private

key, to retrieve the key K and use it to read the rest of the message. For reporting purposes, then, through this *mailbox*, the potential reporter can fill out forms and attach them to an e-mail message. The Reporting Recipient, in possession of the previously created private key, will be the only one able to decrypt the contents of the message.

This is without prejudice to the option for the reporter to forward the *confidential* or *open* communication (by checking the box on the corresponding *Form 1*) without taking advantage of the encryption tool and to transmit the message with attachments via unencrypted regular mail. This choice does not preclude the protection of the reporter's confidentiality, as outlined *supra*, and does not affect any subsequent Follow-up fulfillment of the report.

Finally, the *confidential* or *open* reporting can be formulated orally, through different modalities: it can be made by audio recording to be transferred by the same e-mail channel (encrypted or not); by exposing the content of the report directly during the telephone call to the dedicated number (telephone call intended for recording for use exclusively internal to the Recipient's investigative activity) or *de visu* after requesting and arranging the direct meeting with the Supervisory Board. In this case, the Recipient is required to verbalize the content of the conversation, rereading the record at the end of the interview with the reporter so that the latter can confirm its content and, if necessary, sign it.

On the other hand, the reporter who wishes to keep his or her report totally *anonymous* - without prejudice to the need for subsequent identification in order to have access to the protection measures in case of retaliation and the necessary circumstantiality of its content in order to be taken into consideration for the purposes of internal investigation - must forward the communication, filling out only *Form 2: Content of the report* and proceed to send the report following the procedure described above, i.e., using the mailbox segnalazioniodvsgi@gmail.com.

TRANSMISSION OF EXTERNAL REPORTING

In the event that the reporter is in a position to use the so-called external channel, managed National Anticorruption Authority (see *above*), the transmission of the communication must be done by accessing from the following *link* to the Portal made available by ANAC: https://www.anticorruzione.it/-/whistleblowing.

For any External Reporting that is made in the mode of so-called public disclosure (through the press or mass media), the reporter may proceed with it within the limits of the subject matter indicated *supra* (see *Definitions* External Reporting) and upon the occurrence of the following conditions:

⇒ an internal report that was not responded to by the administration/entity within the prescribed timeframe was followed by an external report to ANAC, which, in turn, did not provide feedback to the reporter within reasonable timeframes;

⇒ the person has already directly made an external report to ANAC, which, however, has not responded to the reporter regarding the measures planned or taken to follow up the report within a reasonable time;

⇒ the person directly makes a public disclosure because he or she has reasonable grounds, based on concrete circumstances and thus, not on mere inferences, to believe that the violation may pose an imminent or obvious danger to the public interest;

⇒ the person directly makes a public disclosure because he or she has reasonable grounds to believe that external reporting may pose a risk of retaliation or may not be effectively followed up.

It should be noted that the person making a public disclosure should be considered distinct from the person who constitutes a source of information for journalists. In such cases, the rules on professional secrecy of journalistic practitioners, with reference to the source of the news, remain unaffected.

Finally, it should be noted that the reporter may convey any Violation (see Definitions *above*), which integrates the extremes of unlawful conduct, also by means of a complaint to the judicial authorities.

RECIPIENT OF INTERNAL REPORTING AND RELATED TASKS

To ensure the functionality and confidentiality of the procedure, the report is addressed to the Company's Supervisory Board, which in turn can identify a support in the management of the report, who is a specifically trained figure outside the corporate structure.

In the event that the *confidential* or *open* report reaches the Recipient by communication to the e-mail address odv@sgispa.com, without the use of cryptographic keys, the figure in charge of management accesses the box by means of an alphanumeric *password*, which is subject to periodic updating and knowledge of which is strictly limited to members of the Supervisory Board.

If, then, the reporter has encrypted the content of the report, using the P.G.P. program, the Recipient must download the *software* that manages certificates and provides the interface for encryption, so that the transferred public key can be used to create the private key and decrypt the cipher text of the report. The Recipient shall be assisted by the Company's internal IT department in order to implement the cryptographic key management mechanism.

In both cases, however, the Recipient receiving the communication is required to first open the annex *Form 2: content of the report*, to verify that the subject of the communication is relevant to the institution, then *Form 1* concerning the *data of the reporter.* In the event that the contents of the first annex do not fall within the objective scope, the Recipient is required to assess in each case whether it might be relevant information for the purpose of possible reporting to the governing body or for the purpose of a disciplinary investigation.

In the event that the *confidential* or *open* report has been made orally, via telephone call to the dedicated number, the Recipient is required to verbalize the conversation, specifically indicating whether or not the reporter has given consent to the disclosure of his or her name; he or she is also required to request the reporter to provide an *e-mail* address for subsequent communications.

If the whistleblower has requested a face-to-face meeting, the Recipient is required to schedule it within a maximum period of three months from receipt of the contact and is required-until the time of the meeting-to maximally preserve the confidentiality of the whistleblower by not mentioning the request for the face-to-face meeting via *e-mail* or orally with any corporate personnel resource.

Likewise, upon receipt of the request, it is required to request the reporter to provide an *e-mail* address for subsequent communications.

If the report was made orally by forwarding the audio recording through the e-mail channel, the procedure for handling the report follows the directions provided for the first two scenarios.

In all cases, within seven days of the act of receipt of the report, the Acknowledgement must be sent to the reporter: it may take the form of a response to the *e-mail address* from which the report came to the Recipient's mailbox or a communication to the *e-mail* address provided by the reporter at the time of the oral report and the request for a face-to-face meeting.

In the event that the reporter has decided to use the cryptographic key program, all subsequent interlocutions between the Recipient and the reporter should take place in the same procedural manner.

In addition, the Recipient shall ensure the confidential logging of the report and any other documentation that is received together. Access to the minutes of the report or *e-mail* communications must be preserved with the utmost confidentiality: the preservation of the relevant documentation must take place for the time necessary for the definition of the report and, in any case, for no more than five years from the date of communication of the final outcome of the procedure, in compliance with the obligations of confidentiality *ex* art. 12 of Legislative Decree No. 24/2023 and the principle set forth in Articles 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative Decree No. 51/2018.

Reports made through a recorded telephone line or other recorded voice messaging system shall be documented--with the consent of the reporter--by recording on a device suitable for storage and listening, or by transcription in its entirety (in which case, the reporter must be able to verify, rectify or confirm the content of the transcription by his or her own signature).

Reports made via an unrecorded telephone line or other unrecorded voice messaging system shall be documented in writing by detailed transcript of the conversation (even then, the reporter must be able to verify, rectify or confirm the contents of the transcript by his or her own signature).

In the case of a report made orally - subject to the consent of the reporter - it shall be documented by recording on a device suitable for storage and listening, or by transcription through minutes, and even then, the reporter must be able to verify, rectify or confirm the minutes of the meeting by

his or her signature.

Finally, in the case of an anonymous report coming from the e-mail address segnalazioniodvsgi@gmail.com specifically created by the Company, the Recipient is required to verify the circumstantial nature of the content and to carry out the appropriate internal investigations in order to verify its reliability. Consider, indeed, that - according to the latest ANAC indications - anonymous reports are equated with ordinary reports and in that case considered in their own ordinary supervisory procedures. In any case, the anonymous whistleblower who reports possible retaliation and is subsequently identified, access in *full* the protection that the decree guarantees against retaliatory measures. Thus, the Recipient who receives the anonymous report is required to record it and keep the relevant documentation no later than five years from the date of receipt of such reports, thus making it possible to trace them, in the event that the reporter, communicates that he or she has suffered retaliatory measures because of that anonymous report.

Unless the report is manifestly unfounded or outside the scope of this protocol (see *above)*, the Recipient is required to follow up on the report.

Specifically:

⇒ To initiate, with due caution and in accordance with the utmost confidentiality, the internal procedure for verification of the facts described in the report, investing the relevant structures to carry out the necessary activity to ascertain the facts themselves;

⇒ Order any investigative activities it deems appropriate, including the hearing of persons potentially able to report on the facts reported and indicated by the reporter, colleagues and the facilitator;

⇒ Maintain interlocutions with the reporting person and, if necessary, request additions;

⇒ Provide acknowledgement of the report within three months from the date of the acknowledgement of receipt or in any case within three months after the expiration of the seven-day period from the date of receipt.

In the event that the Recipient considers the report to be well-founded, the Recipient, while respecting the terms of confidentiality of the identity of the reporter where the report was made in *confidence*

(thus, for example, obscuring the signature and *e-mail* address from which the report originated), within the limits of compatibility with the content of the report (for example, omitting communication to the Chief Executive Officer if directly involved by the subject of the report), shall inform the Chief Executive Officer, advising him that within the period of thirty days from receipt of the report he is required to make further verifications

Upon the outcome of these verifications and subject to the time limit just mentioned, the Chief Executive Officer, copying for information to the Supervisory Board for the appropriate control of the terms and procedure, shall do so within ten days:

⇒ to the communication to the Personnel Office, for the purpose of taking appropriate action, including the possible exercise of disciplinary action and sanctions;

⇒ To the submission of the complaint to the judicial authority if the legal requirements are met.

Conversely, in the event that the report turns out to be unfounded due to malicious intent or gross negligence on the part of the reporter, the Recipient, always maintaining the utmost confidentiality on the *confidential* report, shall inform the Chief Executive Officer, advising him or her that he or she has sixty days from the receipt of the report to carry out further verification.

Upon the outcome of these verifications and subject to the deadline just indicated, the CEO:

⇒ communicates the finding to the Personnel Office for the purpose of taking appropriate action, including the possible exercise of disciplinary action and sanctions;

⇒ Submits a complaint to the judicial authority if the legal requirements are met.

The identity of the Persons involved and other persons mentioned in the report is guaranteed until the conclusion of the relevant proceedings, in compliance with the same guarantees provided in favor of the reporter. The Person Involved may be heard, or at his or her request, shall be heard, including by means of paper proceedings through the acquisition of written observations and documents, as part of the investigation of the internal report concerning him or her.

PROTECTION AND RESPONSIBILITY OF THE REPORTER

The first form of protection offered to the reporter is the obligation of confidentiality. The identity of the reporter is protected in every context: from the time of the report, all those who receive or are involved, even accidentally, in the handling of the report are obliged to protect the confidentiality of that information and the identity of the reporter.

Violation of the duty of confidentiality is a source of disciplinary liability, without prejudice to additional forms of liability provided for by law.

The prohibition to disclose the identity of the reporter is to be referred not only to the **name of** the reporter but also to any **other information or element of the report**, including the documentation attached to it, from the disclosure of which the identity of the reporter or even of the other persons whose identity under Leg. 24/2023 must remain confidential, if, for investigative reasons, other persons must also be made aware of the content of the report and/or the documentation attached to it: the Company also ensures confidentiality to the Person involved and the Facilitator both with regard to identity and with reference to the activity in which the assistance takes place. An exception to this duty of confidentiality of the Persons involved or mentioned in the report is the case in which the reports are reported to the Judicial Authorities and the Court of Auditors.

In the event that, as a result of the report, criminal proceedings are initiated, the identity of the reporting person is covered by investigative secrecy *pursuant to* Article 329 of the Code of Criminal Procedure; in the context of accounting proceedings, the identity of the reporting person may not be disclosed until the closing of the investigative phase; in the context of disciplinary proceedings, the identity of the reporting person may not be disclosed, both when the accusation of the disciplinary charge is based on separate and additional investigations to the report, even if consequent to the report, and when it is based exactly on the facts that are the subject of the report. In the event that the identity of the reporter is indispensable to the defense of the person to whom the disciplinary charge has been contested, it may be disclosed only with the express consent of the reporter and after written notice to the reporter of the reasons that make it necessary to disclose his or her particulars.

If the disclosure is indispensable for the defense of the Person involved, notice shall be given to the reporting person by written communication of the disclosure of the confidential data, and it shall be done after obtaining his or her express consent.

Second, the *whistleblower* is protected from retaliation, which can manifest itself in any conduct, even if only attempted or threatened, carried out on account of the report and which is likely to cause the reporting person directly or indirectly unfair harm[15] .

Whether the *whistleblower* believes that he or she has been retaliated against, he or she may apply directly to the labor or criminal judicial authority for the purpose of protection from retaliatory conduct through his or her attorney or union representative, or he or she may use the reporting channel set up by the National Anticorruption Authority to report any retaliatory measures against *whisltleblowers* through an IT platform accessible at the following *link on* the dedicated page on the institutional website: https://www.anticorruzione.it/-/whistleblowing.

Similar to the duty of confidentiality, all those who, having a qualified connection with the reporter, suffer retaliation because of said connection also benefit from the protection against retaliation[16] .

Provision is then made-in the context of judicial proceedings involving retaliatory conduct, but also administrative proceedings or in the case of out-of-court disputes-for an inversion of the burden of proof: where the person proves that he or she has made a report and that he or she has suffered retaliation because of it, the burden of proof is on the person who has engaged in such retaliatory conduct and acts. It is the latter, therefore, who is required to prove that the action taken is in no way related to the report.

Even in the case of a compensatory claim filed with the judicial authority, it is presumed-unless proven otherwise-that the harm suffered resulted from the report, except with respect to Facilitators, co-workers of the reporter, and entities owned by the reporter (on whom the burden of proof rests if they complain of retaliation or harm as a result of the report).

[15] For exemplification of forms of retaliation, see *supra.*

[16] These are the Facilitator, people in the same work context, co-workers, and even legal entities in cases where they are entities owned by the whistleblower, whistleblower, public discloser, or entities in which he or she works or entities that operate in the same work context.

The Company holds responsible for the retaliatory measure the person who took the measure or in any case the person to whom the retaliatory behavior and/or omission is attributable. Liability also arises in the person who suggested or proposed the adoption of any form of retaliation against the *whistleblower*, thus producing an indirect negative effect on his or her position (e.g., proposed disciplinary sanction).

It is then the responsibility of the judicial authority to take all measures, including provisional measures, necessary to ensure protection for the subjective legal situation being asserted, including compensation for damages, reinstatement in the workplace, an order to cease the conduct engaged in in violation of the prohibition against retaliation, and a declaration that the acts taken are null and void.

The protection of the whistleblower cannot be ensured, and the whistleblower's liability remains intact, in the event that the report involves civil or criminal liability: in the event of a finding by a judgment, even a non-final judgment of first instance against the whistleblower of criminal liability for the crimes of slander or defamation, or civil liability, for having reported false information intentionally reported with malice or negligence, not only does the whistleblower not enjoy protection from possible retaliatory measures but a specific disciplinary sanction is applied against him or her. On the other hand, protection of the whistleblower from retaliation is applicable, albeit belatedly, if the first instance judgment, unfavorable to the whistleblower or whistleblower, is not upheld in subsequent levels of judgment.

Similarly, the institution of a criminal trial for the offenses of defamation or slander as a result of the report, public disclosure, or whistleblowing, which is later concluded with a dismissal, does not preclude the application of this protection in favor of the whistleblower. This is because dismissal does not involve any finding of criminal liability.

In addition, taking into account that, with regard to civil liability, the damage resulting from the crime must have been caused by the defendant with malice or gross negligence, the existence of slight negligence, although a source of civil liability ascertained by the court, may not result in the loss of the protection provided in case of retaliation.

Any forms of abuse of this procedure, such as reports that are manifestly opportunistic and/or made for the sole purpose of harming the whistleblower or other subjects, and any other hypothesis of improper use or intentional instrumentalization of the institution that is the subject of this procedure, are also a source of liability in disciplinary and other competent fora. If, as a result of internal investigations, the report is found to be manifestly unfounded and made for the purpose of procuring an advantage for oneself or for the sole purpose of harming the whistleblower or other subjects, disciplinary liability actions against the whistleblower will be assessed, regardless of any criminal or civil liability for libel and slander.

COMMUNICATION, TRAINING, CONFIDENTIALITY AND MANAGEMENT OF PERSONAL DATA

This procedure, in addition to providing for the widest dissemination of this document, promotes effective awareness-raising and training on the rights and obligations relating to the reporting of violations within the Company: the widest publicizing of the *policy* is ensured, with specific indication of the content and prerequisites of the potential report, the procedure for transmitting and managing the communication, as well as the protections and responsibilities of the reporter. Dissemination must take place through the internal information channel (*e-mail* communication, shared folder on the corporate portal) or through external information channel, making such information easily accessible also, as far as possible, to people who, although not frequenting the workplace, are legitimately entitled to submit *whistleblowing* reports. They should be materially displayed, for example, in the workplaces in a visible and accessible place, as well as the reference to the implemented protocol should be contained in the 231 clauses provided in the standard contracts with business *partners* and external professionals/consultants.

The Company is committed to ensuring the utmost expository clarity in the merits also of the protections and responsibilities to which the whistleblower is exposed, providing a detailed examination of the concept of retaliation, an exemplification of the forms it may take and the protective response tools available to the whistleblower who is a victim of it.

This aspect of training should be contemplated as "permanent" to the protocol: that is to say, in the directions provided to access the various reporting channels, the whistleblower's set of protections and responsibilities should also always be prescribed, in order to provide the most comprehensive picture possible of his or her legal position following the possible reporting.

Pursuant to the combined provisions of Regulation 2016/679/EU (so called G.D.P.R.) and Legislative Decree No. 196 of June 30, 2003 (as amended by Legislative Decree No. 101/2018), in addition, the Company, as the data controller, is required to provide information regarding the use of personal data received. The protection of personal data is to be ensured not only to the reporting person but also to the other persons to whom confidentiality protection applies, such as the Facilitator, the Person

Involved, and the persons mentioned in the report as *affected by* the data processing.

As is well known, the regulations on the protection of personal data stipulate that data controllers and co-processors, provide, under their own responsibility and within their own organizational structure, that specific tasks and functions related to the processing of personal data are assigned to individuals, expressly designated, operating under their authority: such individuals must receive adequate and specific professional training aimed at increasing their specialized skills - which, in any case, they must already have - including on the subject of personal data protection legislation, data and information security, as well as on the subject of training with regard to the procedures prepared.

Ultimately, according to the provisions of the personal data legislation and Legislative Decree No. 24/2023, data controllers, data processors and persons authorized to process personal data are required to comply, in particular, with the following basic principles:

⇒ Process data in a lawful, fair and transparent manner towards the data subjects ("lawfulness, fairness and transparency");

⇒ Collect data only for the purpose of handling and following up on reports made by those protected by Legislative Decree 24/2023 ("purpose limitation");

⇒ ensure that data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"): in this regard, the decree specifies, in fact, that personal data that are manifestly not useful for the processing of a specific report are not collected or, if accidentally collected, are deleted without delay;

⇒ Ensure that data are accurate and, if necessary, updated: all reasonable steps must be taken to delete or rectify in a timely manner inaccurate data related to the specific report, public disclosure, or complaint being handled ("accuracy");

⇒ retain the data in a form that allows the identification of the data subjects for as long as 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 reporting procedure ("retention limitation");

⇒ To carry out processing in a manner that ensures adequate security of personal data, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and accidental loss, destruction or damage ("integrity and confidentiality");

⇒ Establish a reporting management model in accordance with the principles of personal data protection. In particular, such measures must ensure that personal data are not automatically made accessible without the intermediary of the data controller or authorized person to an indefinite number of individuals.

⇒ conduct, at the design stage of the reporting channel and thus before processing begins, a data protection impact assessment in cases where the processing of reports may pose a high risk to the rights and freedoms of data subjects in order to identify and apply the necessary technical measures to avoid such risk;

⇒ Make *ex ante* disclosures to possible data subjects about the processing of personal data;

⇒ Ensure that the register of processing activities is updated, supplementing it with information related to the acquisition and management of reports.

In case of violation of the regulations on personal data protection by authorized persons or data processors, the responsibility falls on the Data Controller or the Data Processor under whose direction said persons have acted. In such cases, the Data Protection Authority may take corrective measures and, in cases provided for by law, apply administrative fines. These administrative sanctions do not apply in relation to processing carried out in the judicial sphere. The same violations may also be of criminal relevance and give rise to civil liability.

The Company's organizational structure is coordinated in the area of *whistleblowing* management as follows:

⇒ the relevant *Privacy* function provides the Recipient with processing guidelines and information on personal data protection measures (e.g., sharing authorization forms, IT security measures, guidelines on the selection of sensitive data and record keeping);

⇒ the Data Protection Officer is responsible for periodically monitoring that the protocols for handling the report are *privacy compliant*, i.e., that they provide adequate safeguards on the confidentiality of the information received and the protection of the identity of the whistleblowers and all data subjects;

⇒ the Data Processor ensures the proper application of the principle of minimization of data processing, in accordance with the requirements specified in the regulations and compliance with

the principles of *data retention*, in particular, monitors that personal data not useful for the processing of a specific report are not collected or, if accidentally collected, are deleted without delay, while ensuring the proper management and storage of data necessary in the preliminary activity of the reporting procedure;

⇒ the designated function prepares the Data Protection Impact Assessment in cases where the processing of reports may pose a high risk to the rights and freedoms of data subjects in order to identify and apply the necessary technical measures to avoid such risks.

DISCIPLINARY SANCTIONS

In order to ensure the maximum effectiveness of the measures and safeguards introduced in this protocol, in accordance with national legislation, the Company has identified the following cases relevant for disciplinary purposes, specifically conformed for violations of the requirements set forth on the subject of *whistleblowing* and reported in the related *policy*, for which the disciplinary sanctions will be applied as indicated in the content and methods in *Section 4. The Disciplinary System of* the General Part of the 231 Organization and Management Model adopted by S.G.I. S.p.A. in its latest update:

⇒ Violation of the duty of confidentiality in the handling of reports by the Recipient and the Data Processor;

⇒ Establishment of criminal liability of the reporting party (convicted by even non-final first-degree judgment) for the crimes of slander or libel with reference to the facts that are the subject of the report, or civil liability, for intentionally reporting false information with malice or negligence;

⇒ Adoption of retaliatory measures/acts or omissions having this purpose against the reporter or persons protected under the regulations;

⇒ Adoption of conduct obstructing the transmission of the report and the subsequent verification activity by the Recipient;

⇒ *Management's* failure to adopt appropriate reporting channels, i.e., procedures for forwarding and handling reports, or the activity of reviewing and analyzing reports received;

⇒ any form of abuse of this procedure, such as, but not limited to, reports that are manifestly opportunistic and/or made for the sole purpose of harming the whistleblower or others, and any other hypothesis of misuse or intentional instrumentalization of the institution.

ALTERNATIVE REPORTING CHANNEL

In cases where the *whistleblower* report involves a member of the Recipient Body, the alternative reporting channel must be activated.

The whistleblower may forward the communication - by filling out the forms attached to this protocol - by *e-mail* through his or her personal *account* or possibly by resorting to the address created *ad hoc* by the Company in order to maximize the protection of confidentiality and anonymity (segnalazioniodvsgi@gmail.com), to lawyer Marco Alessandro Bartolucci, external professional reference *compliance 231*, at the e-mail address *mab@marcoalessandrobartolucci.it.*

The whistleblower may also possibly resort to oral communication by contacting the following telephone number tel. 02 5518 2641/654 or request a face-to-face meeting, which will be scheduled in reasonable terms outside the company premises, at the indicated professional's office.

Again, the reporter can request that the report be either *open* or *confidential* by checking the corresponding box on *Form 1: Reporter's Data*.

If the whistleblower intends to communicate the report *anonymously*, using the generic e-mail *account* indicated *above,* similarly to what is prescribed for communication to the Supervisory Board, only *Form 2: Content of the report* must be completed. In the case of a sufficiently substantiated report, it must be handled in the ordinary manner in the same way as a report with an identified whistleblower, subject to the preclusion of the protections provided by the regulations in the event that a subsequent identification does not take place.

The Alternative Report Recipient, upon receipt of the report, reviews the contents of *Form 2* to verify the reliability of the report and relevance to the scope of the institution.

Within seven days of the act of receipt of the report, a Response must be sent to the reporter: this may take the form of a reply to the *e-mail* address from which the report came or a communication to the *e-mail* address provided by the reporter at the time of the oral report and the request for a face-to-face meeting.

After blacking out the signature based on the consent given by the reporter on the disclosure of his or her name and within the limits of compatibility with the tenor of the report, he or she informs the CEO for further verification.

Upon the outcome of these reviews, the CEO shall provide:

⇒ To the submission of the complaint to the judicial authority if the legal requirements are met;

⇒ to the convening of the meeting of the administrative body to initiate the procedure for the recomposition of the Supervisory Board.

In any case, an acknowledgement of the report must be provided within three months from the date of the acknowledgement of receipt or in any case within three months after the expiration of the seven-day period from the date of receipt.

***

The following attached documents are an integral part of this protocol:

- **Doc. 01: Annex C-1** ***Form 1: Data of the reporter;***
- **Doc. 02: Annex C-2** ***Form 2: content of the report.***

Società Gasdotti Italia

Società Gasdotti Italia S.P.A.

P.I. 04513630964 REA MI - 1753569

Contact

Tel

0775.88601

Email

segreteria@sgispa.com

Pec

sgispa@legalmail.it

Locations

Registered office

Via della Moscova, 3 - Milan

Other locations

FROSINONE - Via dei Salci, 25

ROME - Via Toscana, 10

CHIETI - Via Padre Ugo Frasca snc

LARINO - Contrada Monte Arcano snc

Società Gasdotti Italia

Appendix C-1

FORM 1. Data of the reporter for confidential or open communication

Pursuant to current regulations and referring to the *Whistleblowing* protocol attached to the Organization, Management and Control Model of S.G.I. S.p.A, which is intended herein to be referred to in its entirety, it is recalled that the subjects to whom the regulations on whistleblowing and related protection apply are: employees, self-employed workers who carry out their work activities at the entity, workers or collaborators, who carry out their work activities at entities, including those in the private sector that provide goods or services or carry out works in favor of third parties, freelancers and consultants who carry out their activities at the entity, volunteers and trainees, paid and unpaid, who carry out their activities at the entity (art. 3, para. 3).

The protections provided by the rule apply to the above-mentioned individuals even when the legal relationship has not yet begun, if the information on violations was acquired during the selection process or other pre-contractual stages; during the probationary period; and after the dissolution of the legal relationship if the information on violations was acquired during the course of the relationship.

According to Leg. 24/2023, moreover, the protection measures also apply to "facilitators," i.e., natural persons who assist a whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential; to persons in the same work context as the whistleblower, the person who made a complaint to the judicial or accounting authority or made a public disclosure and who are related to them by a stable emotional or kinship relationship within the fourth degree; to co-workers of the whistleblower or the person who made a complaint to the judicial or accounting authority or made a public disclosure, who work in the same work environment as the whistleblower or the person who made a complaint to the judicial or accounting authority or made a public disclosure and who have a habitual and current relationship with the said person; to entities owned by the whistleblower or the person who made a complaint to the judicial or accounting authority or made a public disclosure or for which the same persons work; and to entities that work in the same work environment as the said persons.

On the other hand, the protection in question does not apply in the case of disputes, claims or demands related to a personal interest of the reporter or the person who filed a complaint to the judicial or accounting authority, which relate exclusively to their individual labor or public employment relationships, or inherent in

their labor or public employment relationships with hierarchically superordinate figures (Art.1, paragraph 2, letter a) Legislative Decree 24/2023). The protection, shall not apply, moreover, when the criminal liability of the reporter for the crimes of defamation or slander or otherwise for the same crimes committed with the complaint to the judicial or accounting authority or his civil liability, for the same title, in cases of malice or gross negligence, is established, even by a judgment of first instance.	
Name	
Last name	
Tax Code	
Current qualification/position within the company/relationship to provide services, supply/professional assignment.	
Current organizational unit and place of employment	
Qualification/Position at the time of the reported event	
Current organizational unit and place of employment at the time of the reported event	
Phone number	
E-mail	

The reporter gives his or her consent to the disclosure during the investigation of his or her personal details (so-called *open-form* disclosure):

- Yes
- No, I prefer the communication to be in a so-called *confidential* form, i.e., the reporter discloses his or her name to the Recipient but does not give consent to its disclosure.

Date Signature

_____ _____

***

The reporter consents to the processing of the personal data indicated in this form in the manner set forth in the notice below:

INFORMATION ON THE PROCESSING OF PERSONAL DATA OF INDIVIDUALS WHO REPORT WRONGDOING IN ACCORDANCE WITH LEGISLATIVE DECREE 24/2023

(Art. 13, EU Regulation 2016/679 - GDPR)

DATA CONTROLLER AND DATA PROTECTION OFFICER

The Data Controller is: Società Gasdotti Italia S.p.A., in the person of the Chief Executive Officer; tel. 0775-88601; fax. 0775-201279; C.F. 04513630964.

PURPOSE AND LEGAL BASIS FOR PROCESSING

Personal data are processed by the Recipient of the report in the performance of his or her duties arising from legal obligations, with particular reference to the task of ascertaining any illegal conduct reported, in the interest of the Company's integrity, by the relevant employee or assimilated, who has become aware of it by reason of his or her employment relationship.

DATA BEING PROCESSED

The data being processed are the personal identifying data of the reporter or the reported person disclosed through the submission of reports of wrongdoing and, if necessary, transmitted subsequent to said report.

TYPE OF DATA AND COMPULSORINESS

The inclusion of the reporter's personal data is not mandatory, but failure to provide them will not allow the application of the protection measures regulated by Chapter III of Legislative Decree 24/2023. In case of their provision, it is informed that they are first name, last name, telephone number, e- mail and job position. These data will be processed by the Supervisory Board in the performance of its tasks of public interest or otherwise related to the exercise of its functions under the aforementioned Legislative Decree 24/2023.

The data provided by the reporter, also relating to the persons in various capacities involved in the report, will be processed for the purpose of carrying out the necessary investigative activities aimed at verifying the merits of the fact being reported and the adoption of any consequent measures. The management and preliminary verification of the substantiality of the circumstances represented in the report will be entrusted to the Supervisory Board, which will do so in accordance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the reporter and any other persons who may report on the reported facts.

CATEGORIES OF DATA RECIPIENTS

Recipients of the data collected as a result of the report are the Judicial Authority, the Court of Auditors and ANAC, where appropriate.

Alerts may not be used beyond what is necessary to adequately follow up on them.

In ways that still ensure the confidentiality of the reporter's identity, the Supervisory Board shall account for the number of reports received and their status in information flows to the Board of Directors.

DISCLOSURE OF THE IDENTITY OF THE REPORTER

In the absence of the express consent of the whistleblower, the identity of the whistleblower may not be disclosed to persons other than the Supervisory Board or those competent to follow up the reports, during all stages of the proceedings to which the report has given rise, including the possible transfer of reports to other Authorities.

In the event that consent has not been expressed in this Form (hypothesis of so-called confidential communication), the subsequent acquisition of consent may take place with a special reasoned request by the Supervisory Board to the reporter through the contact details provided by the latter in the report.

The report is, in any case, subtracted from the documental access provided for by Articles 22 et seq. of Law 241/1990, as well as simple or generalized civic access under Article 5 of Legislative Decree 33/2013.

RETENTION PERIOD

The data referred to in the reports, and related documentation, will be retained for as long as necessary for the processing of the report, but no longer than five years from the date of notification of the final outcome of the reporting procedure.

RIGHTS OF THE DATA SUBJECT AND HOW TO EXERCISE AND COMPLAIN

The rights referred to in Articles 15 to 22 GDPR may not be exercised by request to the data controller or by complaint under Article 77 GDPR if the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the person reporting violations of which he or she has become aware by reason of his or her employment relationship or duties performed, pursuant to Legislative Decree 24/2023. In that case, the rights shall be exercised in accordance with the provisions of the law or regulations governing the field, which must at least bear measures aimed at regulating the areas referred to in Article 23(2) GDPR. The exercise of the same rights may, in any case, be delayed, restricted or excluded by reasoned notice given without delay to the data subject, unless such notice would jeopardize the purpose of the restriction, for such time and to the extent that this constitutes a necessary and proportionate measure, having regard to the fundamental rights and legitimate interests of the data subject, in order to safeguard the interests involved. In such cases, the rights of the data subject may also be exercised through the Guarantor in the manner set forth in Article 160 of Legislative Decree No. 196/2003.

Date

Signature

_____ _____

Società Gasdotti Italia

Annex C-2

FORM 2. Content of the report

Pursuant to the regulations in force and referring to the *Whistleblowing* protocol attached to the Organization, Management and Control Model of S.G.I. S.p.A., which is intended herein to be referred to in its entirety, it is recalled that the reports, in order to fall within the scope of application of Legislative Decree 24/2023, must relate to "*violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity*," the knowledge of which of what was reported occurred in the "*work context*." In particular, the following are the object of internal reporting: illegal conduct relevant under Legislative Decree No. 231 of June 8, 2001, thus the facts listed in the so-called predicate offenses indicated in the General Part of the Organization and Management Model adopted by the Company; any pathological malfunction of the activity within the Company that denotes a violation of the control principals laid down in the Organization and Management Model adopted by the Company or is potentially capable of causing harm to the Company and its personnel; any violation of the Code of Ethics adopted by the Company.

The information may concern both violations that have been committed and those not yet committed that the whistleblower reasonably believes could be committed based on concrete evidence. Those elements that concern conduct designed to conceal violations (think, for example, of the concealment or destruction of evidence about the commission of the violation) may also be subject to reporting.

They cannot be the subject of the report:

-Clearly unsubstantiated information or information that is already totally in the public domain;

-information acquired only on the basis of poorly reliable indiscretion or rumor (so-called rumors);

-challenges, claims or demands related to an interest of a personal nature of the reporting person or the person making a complaint to the judicial or accounting authority that pertain exclusively to his or her individual labor relations, i.e., inherent in his or her labor relations with hierarchically subordinate figures (i.e., therefore, are excluded, for example, reports concerning labor disputes, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker)

-violations where they are already mandatorily regulated by the European Union or national acts specified in Part II of the Annex to the Decree or national acts that constitute implementation of the

European Union acts specified in Part II of the Annex to Directive (EU) 2019/1937, albeit not specified in Part II of the Annex to the Decree.

-violations of national legislation already covered in European Union directives and regulations and in the implementing provisions of the Italian legal system that already guarantee appropriate reporting procedures.

The whistleblower must provide all the elements relevant to the reconstruction of the fact aimed at ascertaining the merits of what was reported. In particular, it is necessary to be clear:

-the generalities, job title or position, place of employment and contact information of the reporter;

-The circumstances of time and place in which the reported event occurred;

-The description of the fact;

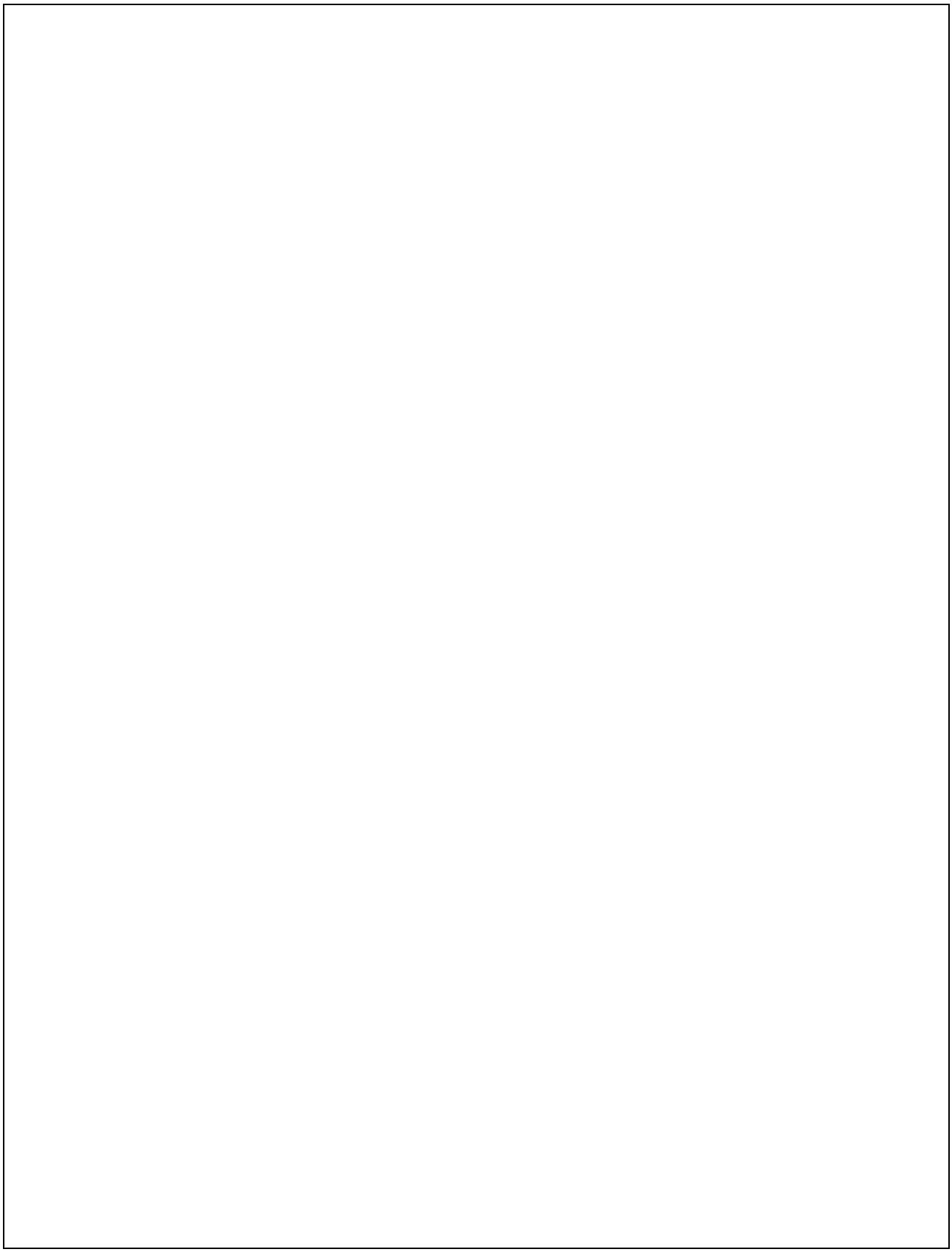
-general information or other elements that would allow the person involved to be identified;

-the particulars of any other individuals who may report on the facts being reported;

-any other information or documentation that may provide grounds for the facts being reported.

Date and/or period when the event occurred:	
Physical location where the event occurred:	
I consider the actions or omissions committed or attempted to be (*): (*) The report does not concern grievances of a personal nature of the reporter or requests that pertain to the discipline of the employment relationship or relations with the hierarchical superior or colleagues, for which reference should be made to the H&R function.	

DESCRIPTION OF THE FACT (CONDUCT AND EVENT)



PERPETRATOR(S) (Give biographical data if known and, if not, any other suitable identifying information)
OTHER PARTIES, IF ANY, WITH KNOWLEDGE OF THE FACT AND/OR ABLE TO REPORT ON THE SAME (Give biographical data if known and, if not, any other suitable identifying information)

ANY ATTACHMENTS TO SUPPORT THE REPORT (Indicate whether you have attached to the *e-mail* communication)