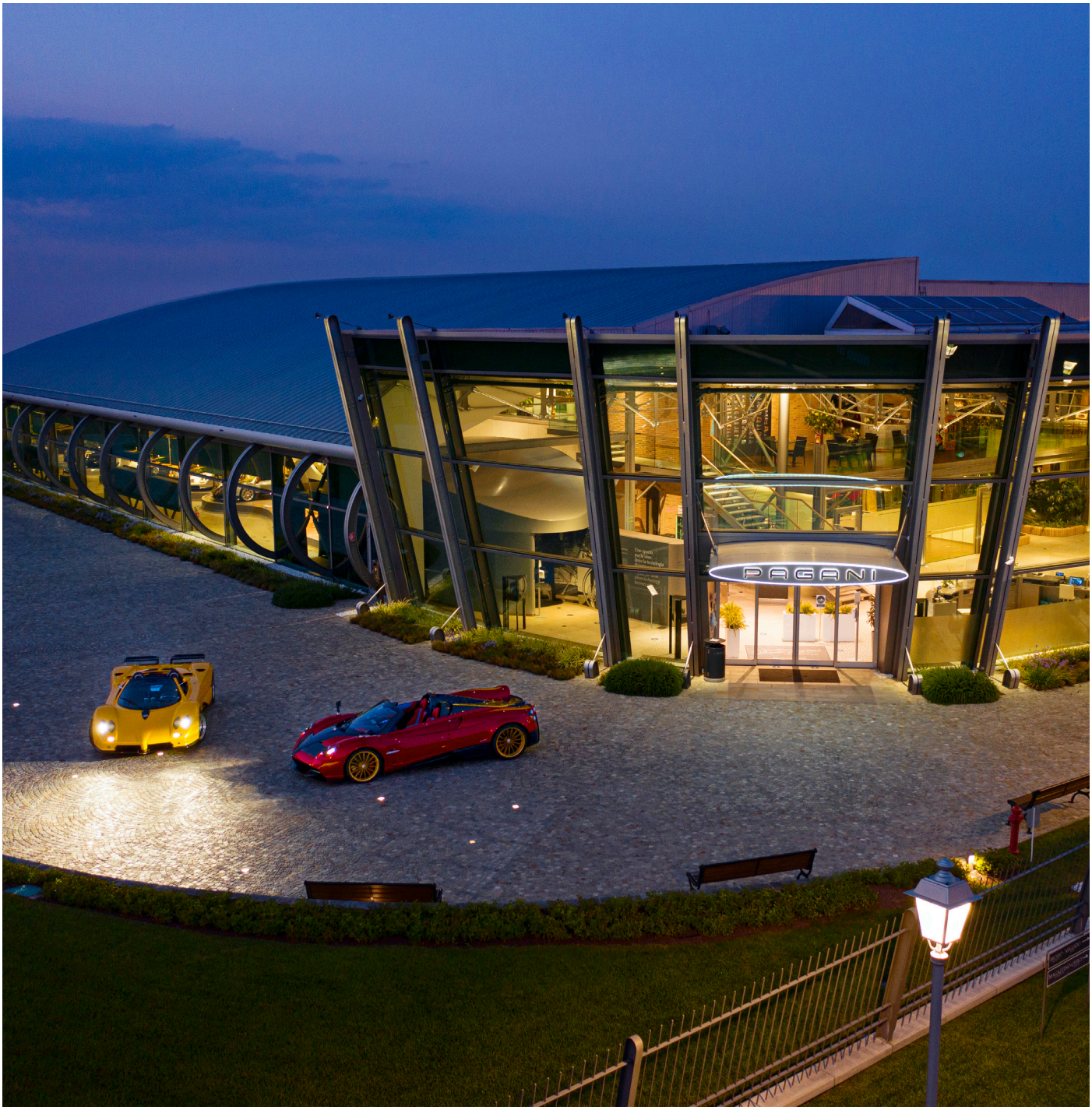
PROCEDURE FOR THE WISTLEBLOWING MANAGEMENT


PAGANI

PROCEDURE FOR THE WISTLEBLOWING MANAGEMENT

PARTE GENERALE
INDICE SOMMARIO

I.
INTRODUCTION

The introduction into Italian national law of a report management system which also provides for adequate protection for employees who report work-related misconduct is envisaged in various international conventions (UN, OECD, Council of Europe) that have been ratified by Italy, as well as in recommendations by the Parliamentary Assembly of the Council of Europe.

More specifically, with art. 1.51, Italian law n. 190 dated 6 November 2012 introduced art. 54-bis of Italian legislative decree n. 165/2001, the provisions of which were intended to encourage workers to report concerns about wrongdoings in their workplace, implementing a mechanism also known as "whistleblowing".

Through a specific regulation governing the management of these reports and the exercise of the power to apply penalties in order to protect parties who report their concerns about wrongdoings or misconduct which have come to their attention through any of the employment relationships provided for in art. 54-bis of Italian legislative decree n. 165/2001, ANAC (the Italian national anticorruption authority) has established further operational provisions on the matter.

The obligation, originally envisaged for public administration authorities, to establish corruption prevention systems including a whistleblowing mechanism, was then extended, in part, to the private sector, with Italian law n. 179 dated 30 November 2017.

The European Union subsequently approved European Directive 2019/1937 on the protection of people who report breaches of Union law, in order to create a minimum standard for the protection of reporting persons' rights in all member states.

Italy implemented the European Directive with Italian legislative decree n. 24 dated 10 March 2023.

The aim of Italian legislative decree n. 24/2023 is to provide for the protection of people who report breaches (of national and European Union legislative provisions that are detrimental to the public interest, or the integrity of a public administration authority or entity) which come to their attention within a work-related context in either the public or private sphere.

One of the main cornerstones of whistleblowing legislation is the protection guaranteed to a reporting person when they raise concerns in compliance with these provisions. This protection includes prohibiting employers from any of form of retaliation against reporting persons and, following on from this, the invalidity of any action taken against the reporting person in retaliation.

Italian legislative decree n. 24/2023 stipulates that protection against retaliation applies not only to those who report their concerns but also to other parties who, while not having made the report directly, are nevertheless deemed in need of protection.

However, there are some conditions, which are described below, that must be met in order for reporting persons to benefit from the protection envisaged.

Italian legislative decree n. 24/2023 also makes certain provisions intended to guarantee the protection of confidentiality and of personal data, which also govern the way in which documentation relating to the report is kept.

The provisions provided for by Italian legislative decree n. 24/2023 take effect for Pagani S.p.A. (hereinafter, also "Pagani") on 17 December 2023.

II.
PURPOSE AND SCOPE

The aim of this procedure (hereinafter also referred to as the "Procedure") is to provide clear operating instructions concerning the type of matter that can be reported, as well as the contents of the report, the target recipients, the reporting methods, the qualifying breaches, as well as the protection measures provided for by applicable legislation.

The term "breaches" means any conduct, acts, or omissions that are detrimental to the public interest or the company's integrity, which have come to the reporting person's attention as result of their working activities (see subsection 8.3).

Pagani is strongly committed to preventing offences occurring within its business activities and adopts the necessary organisational and disciplinary measures to counter any possible offences.

For this reason, the company believes it is essential for employees and third parties to report concerns about any wrongdoings or misconduct, whether unlawful or unethical, which may come to their attention as a result of their employment relationship with and their role within Pagani; this is to guarantee, among other things, compliance with the provisions of the company's Organisation and Management Model pursuant to Italian legislative decree n. 231/01 and its Code of Ethics.

The aim of this procedure is therefore to eliminate any factors that could hinder or discourage use of the whistleblowing mechanism, such as doubts and uncertainties regarding the procedure to follow and fears of retaliation or discrimination, as well as concerns that the matter reported will not be addressed with the due confidentiality.

The objectives of this procedure are to:

- Specify who can report concerns;
- Describe the qualifying disclosures, i.e. the types of breaches that can be reported;
- Describe the ways to report concerns;
- Outline the various stages of the report management process, including specifying the roles, responsibilities, and operating methods;
- Illustrate the protection measures envisaged for reporting persons;
- Inform the target recipients of the pecuniary penalties imposed by ANAC (the Italian national anticorruption authority) on the company and on the parties involved in the event of breach of the provisions of applicable legislation;
- Inform the target recipients of the applicable disciplinary measures.

This procedure comes into force on the date of approval by the board of directors of Pagani and applies to the aforesaid company.

III.
SOURCES OF PROVISIONS

This procedure is governed by the following legislation:

- **Directive (EU) 2019/1937:** the European Union directive concerning the protection of people who report breaches of Union law which come to their attention in a work-related context within either the public or private sector (also known as the Whistleblowing Directive).
- **Italian legislative decree n. 24 dated 10 March 2023:** the Italian legislative decree that transposes Directive (EU) 2019/1937 of the European Parliament and the Council, dated 23 October 2019, concerning the protection of people who report concerns about breaches of Union law, and also provides for the protection of people who report concerns about breaches of national legislative provisions.
- **Italian legislative decree n. 231 dated 8 June 2001:** the Italian legislative decree containing "Provisions for administrative law liability of legal persons, companies, and associations, including those without legal personality, pursuant to art. 11 of Italian law n. 300 dated 29 September 2000," as subsequently amended and supplemented.
- **Organisation Model:** the organisation, management, and control model adopted by Pagani pursuant to Italian legislative decree n. 231/2001.
- **Pagani Code of Ethics:** the document setting out the values, principles, and lines of conduct that must underlie the company's activities and expressing the commitments and ethical responsibilities which must be upheld by all workers (internal and external) when going about their work.

IV.
DEFINITIONS

ANAC: the Italian national anticorruption authority, whose mission is to prevent corruption in all areas of administration.

Reporting channel: online channel for reporting concerns accessible via the website homepage at https://www.pagani.com/it/ or by pasting the following address into a browser: https://segnalazioni.pagani.com.

Work-related context: work or professional activities carried out in the past or present within the relationships stated in art. 3.3 or art. 3. 4 of Italian legislative decree n. 24/2023, through which (regardless of the nature of such activities) a person acquires information on breaches and within which they could suffer retaliation in the event of reports, public disclosure, or complaints to the judiciary or audit authority.

Italian legislative decree n. 196/03: the Italian legislative decree (n. 196 dated 30 June 2003) titled "Code for the protection of personal data".

Italian legislative decree n. 231/01 or Decree: the Italian legislative decree (n. 231 dated 8 June 2001) titled "Provisions for administrative law liability of legal persons, companies, and associations, including those without legal personality" as subsequently amended and supplemented.

Public disclosure or publicly disclose: to publish information on breaches either through the press or online or, in any case, using means of disse-

mination with the potential to reach a wide audience.

Facilitator: an individual who assists a reporting person during the whistleblowing process, who works within the same work-related context and whose assistance must be kept confidential.

GDPR: Regulation (EU) n. 2016/679 dated 27 April 2016, concerning the protection of natural persons with regards to personal data processing, in addition to the free circulation of such data which repeals EC Directive 95/46 (General Data Protection Regulation)

Personnel tasked with managing the reporting channel: specifically trained staff within autonomous internal departments who are tasked with managing the reporting channels set up by Pagani pursuant to Italian legislative decree n. 24/2023; for the purposes of this procedure, the following personnel are tasked with managing the reporting channel and investigating whether the circumstances represented in the report are founded: a) the head of the legal affairs department; b) the HR manager.

Information on breaches: information, including well-founded suspicions, regarding breaches committed or which, on the basis of factual information, could be committed within the organisation with which the reporting person or the person making a complaint to the judiciary or audit authority has a legal relationship pursuant to art. 3.11 or art. 3.2 of Italian legislative decree n. 24/2023, as well as details of conduct to conceal such breaches.

Italian law n. 146/2006: Italian law n. 146 dated 16 March 2006 (ratification and implementation of the United Nations Convention and Protocols against transnational organised crime, adopted by the General Assembly on 15 November 2000 and 31 May 2001).

Model/OMM: organisation and management model pursuant to arts. 6 and 7 of Italian legislative decree n. 231/01.

Supervisory Body (SB): the entity provided for by art. 6 of Italian legislative decree n. 231/01, which is responsible for supervising the functioning of and compliance with the Model and the updating thereof.

Person concerned: a natural or legal person stated in the report (made either internally or externally), or in the public disclosure, as a person to whom the breach is attributed or who is otherwise implicated in the breach (whether reported or disclosed publicly).

Reporting person: a natural person who reports or publicly discloses information on breaches, acquired in a work-related context.

Platform: computerised tool for managing reports.

Retaliation: any conduct, or act or omission (even if only attempted or threatened) put in practice as a result of the report, the complaint to the judiciary or audit authority, or the public disclosure, which constitutes - or may constitute - either directly or indirectly, a tort against the reporting person or the person who made the complaint or public disclosure.

Report or to report: a concern raised, or to raise a concern, in writing, providing information on breaches.

Anonymous report: when the reporting person's personal details are not expressly provided and their identity cannot be established.

Open report: when the reporting person raises a concern openly, without any restriction linked to confidentiality.

External report: the written or oral provision of information on breaches submitted through the external reporting channel stated in art. 7 of Italian legislative decree n. 24/2023. External reports are not governed by this procedure.

Internal report: the written provision of information on breaches through the internal reporting channel stated in art. 4 of Italian legislative decree n. 24/2023, as per this procedure.

Confidential report: when the reporting person's identity is not stated expressly, but it is nevertheless possible to infer it in certain specific cases, as explained later.

Unlawful report: a report which, according to the findings of the preliminary investigations, is not founded on factual details and the actual circumstances ascertained during the investigations lead to the belief that the report was made in bad faith or with gross negligence.

Detailed/verifiable report: a report in which the reporting person's narration of events or circumstances that constitute the elements of the alleged offence (for example, type of offence committed, period in which it was committed, the amount involved, the causes and purposes of the offence, the companies/areas/people/units/departments involved or concerned, irregularities in the internal control system, etc.) is sufficiently detailed to enable the competent corporate bodies, using the investigative tools available, to verify whether the events or circumstances reported are founded.

Follow-up: the action undertaken by the personnel tasked with managing the reporting channel to assess the events reported, the findings of the investigations, and any measures adopted.

Company: Pagani S.p.A.

Private-sector entities: entities, other than those falling within the definition of public-sector entities, which: 1) have hired, in the last year, an average of at least fifty employees under permanent or fixed-term employment agreements; 2) fall within the scope of the Union acts stated in parts I.B and II of the annex, even if, over the last year, they have not reached the average number of employees stated in section 1); 3) do not meet the criteria stated in section 2), fall within the scope of Italian legislative decree n. 231 dated 8 June 2001, and adopt the organisation and management models envisaged therein, even if, over the last year, they have not reached the average number of employees stated in section 1).

Public-sector entities: the public administration authorities stated in art. 1.2 of Italian legislative decree n. 165 dated 30 March 2001, independent administrative authorities for protection, supervision, or regulation, public utility companies, entities established under public law stated in art. 3.1.d of Italian legislative decree n. 50 dated 18 April 2016, private-sector service providers in public-private partnerships, state-controlled companies, and in-house companies, as defined, respectively, by art. 2.1.m and art. 2.1.o of Italian legislative decree n. 175 dated 19 August 2016, including listed companies.

Reported parties: the party which or whom the reporting person states has committed the misconduct or wrongdoing reported.
Third parties: natural and legal persons which or who are party to agreements with Pagani, i.e. with whom the company enters into any form of contractually governed relationship and intend to work with the company [for example, but not only: independent contractors, suppliers; consultants (such as advisory and law firms); other third parties who or which have contractual relationships with Pagani (e.g. outsourcing companies, temporary staffing companies and temporary workers)].
Stakeholder: all parties with a legitimate interest relating to the business conducted by the company.
Feedback: information provided to the reporting person about the follow-up that has been given or will be given to the report.
Breaches: conduct, acts, or omissions that are detrimental to the public interest or the integrity of a public administration authority or private-sector entity consisting of: 1) accounting, or administrative, civil, or criminal law offences which do not fall under the provisions of sections 3), 4), 5), and 6); 2) material misconduct pursuant to Italian legislative decree n. 231 dated 8 June 2001, or breaches of the organisation and management models provided therein which do not fall under the provisions of sections 3), 4), 5), and 6); 3) offences that fall within the scope of application of the Union or national acts in the annex to Italian legislative decree n. 24/2023 or the national acts that constitute the implementation of the European Union legislation stated in the annex to Directive (EU) 2019/1937 but not stated in the annex to Italian legislative decree n. 24/2023 concerning the following fields: public procurement; financial services, products, and markets and prevention of money laundering and the financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and of personal data and security of networks and information systems; 4) acts or omissions which are detrimental to the financial interests of the European Union stated in art. 325 of the Treaty on the Functioning of the European Union and specified in the relevant secondary legislation of the European Union; 5) acts or omissions relating to the internal market, as stated in art. 26.2 of the Treaty on the Functioning of the European Union, including breaches of the European Union rules on competition and State aid, as well as those concerning the internal market and relating to acts breaching corporate tax rules or mechanisms with the intention of gaining tax benefits which defeat the object or purpose of the applicable corporate tax law; 6) acts or conduct which defeat the object or purpose of the provisions of the sectorial Union acts stated in sections 3), 4), and 5).

V.
RESPONSIBILITY

Responsibility for checking, approving, and updating this document lies with Pagani's governing body.
Responsibility for implementing this document lies with all the parties who or which carry out the activities specified in this procedure.

VI.
GUIDING PRINCIPLES

6.1 Knowledge and awareness

This whistleblowing procedure is fundamental to guarantee full awareness and consequently effective surveillance of risks and their interrelationships and to guide changes in strategy and the organisational context.

6.2 Guarantee of personal data confidentiality

Reports cannot be used in any way other than to follow up the concerns raised in them.
All the parties that receive, examine, and assess the reports and likewise any other party involved in the report management process are required to guarantee the utmost confidentiality surrounding the matter reported and the identity of the reported party, the reporting person, and the facilitator, who are appropriately protected from retaliation, discrimination, or any other unfair treatment.

6.3 Personal data processing

As data controller, Pagani is responsible for upholding the fundamental principles enshrined in EU Regulation 2016/679 (hereinafter also referred to as the "GDPR") and Italian legislative decree n. 196/2003, as amended by Italian legislative decree n. 101/2018, in order to ensure all personal data processing activities (collection, recording, organisation, storage, reference, etc.) carried out as part of its activity, are performed in compliance with applicable legislation. This requirement also extends to activities to protect people who report breaches of national or European Union legislation which are detrimental to the public interest or the integrity of a private-sector entity.

In order to be able to ensure full compliance with the provisions of personal data processing legislation, activities carried out to receive and manage reports must be based on the principle of limiting personal data use to the strictly necessary to follow up the matter reported.

Furthermore, personal data which is not manifestly useful in order to follow up a specific report must not be collected or, where collected, must be promptly deleted.

As data controller, Pagani is required to designate, in writing, the natural persons authorised to access the information of a personal nature contained in a specific report, including therein for follow-up purposes.

The designation of authorised personnel by the data controller must comply with the data minimisation principle, i.e. it must be restricted to a limited number of parties assigned specifically to these duties.

These parties must be formally appointed with a specific letter of instructions, which must be sent to each party concerned.

In order to carry out certain personal data processing activities, the data controller may also assign specific tasks to specific external parties. In this case, the data controller must:

- Only use the services of parties that can guarantee adequate technical and organisational measures to ensure the data processing meets legislative requirements and guarantees the protection of the data subject's rights;
- Govern this relationship with a specific legal document which establishes this party as the "External Data Processor". It is therefore necessary for the data controller to appoint the supplier/third party as an external data processor.

In application of the principle of transparency, information and notices concerning personal data processing must be easily accessible and understandable, written using plain language. To this end, data controllers must provide the reporting persons and the persons concerned with appropriate information, pursuant to arts. 13-14 of the GDPR, likewise ensuring exercise of the rights stated in arts. 15-22 of the GDPR within the limits set out in art. 2-*undecies*.f of Italian legislative decree n. 196/2003.

Data will be processed in a manner that guarantees the security of personal data, including protection, through appropriate technical and organisational measures, from unauthorised or unlawful processing and from accidental loss, destruction, and damage.

No tracking activities are permitted on reporting channels.

Conversely, there is an obligation to guarantee, where possible, that the activities of the personnel authorised to process the data are tracked, in order to comply with guarantees protecting the reporting person.

6.4 Independent and impartial judgment

All the parties authorised to receive, examine, and assess the reports must meet the respective moral and professional requirements and fulfil the necessary conditions when carrying out their activities, namely independence, objectivity, competence, and diligence.

6.5 Protection for reporting persons

Reporting persons are granted various protection measures for reports made in compliance with applicable legislative provisions, on condition that:

- The reporting person comes under the list of parties authorised to report concerns;
- At the time of reporting the concern or making the complaint to the judiciary or audit authority or the public disclosure, the reporting person had "well-founded reason" to believe the information was truthful and fell within the scope of the provisions;
- The report or public disclosure was made in compliance with the provisions of Italian legislative decree n. 24/2023;
- There is a consequential relationship between the report, disclosure, or complaint made and the retaliation suffered.

This protection regime also applies in cases of anonymous reports, complaints to the judiciary or audit authority, or public disclosures if the reporting person was subsequently identified and suffered retaliation, as well as in cases of external reports.

The personal and specific reasons that led the person to make a report, complaint, or public disclosure are immaterial in terms of how the report is treated and the protection from retaliation is handled.

Protection measures also apply to:

- The facilitator (individual who assists a reporting person during the reporting process, who works within the same work-related context and whose assistance must be kept confidential);
- People from the same work-related context as the reporting person, the party who made a complaint or public disclosure, and any people linked to these people by a long-term emotional bond or a kinship relationship within the fourth degree;
- Co-workers of the reporting person, or the party who has made a complaint or public disclosure, or people from the same work-related context as them and who have a current, habitual relationship with that person;
- Entities owned - either exclusively or through a majority share - by third parties - by the reporting person or the person who has made a complaint or public disclosure;
- Entities where the reporting person or the person who has made a complaint or a public disclosure works;
- Entities operating in the same work-related context as the reporting person or the person who has made a complaint or a public disclosure.

6.5.1 **Prohibition of discrimination against reporting persons**

The company does not tolerate or permit any form of retaliation, including attempted or threatened retaliation, linked directly or indirectly to a report made pursuant to this procedure against any reporting person which constitutes or may constitute, directly or indirectly, a tort against the person/entity ([1]).
Responsibility for managing retaliation complaints within the public and private sectors lies with ANAC; where a retaliation complaint mistakenly reaches public- or private-sector entities, instead of ANAC, these entities are required to guarantee the confidentiality of the identity of the person who sent it and to send the complaint on to ANAC, giving simultaneous notice thereof to the person who filed the complaint.
The complainant must provide ANAC with objective information supporting the consequential relationship between the report, complaint, or public disclosure made and the complained retaliation.
Responsibility for any declaration of invalidity of actions constituting retaliation lies with the judiciary, which issues all measures, including interim measures, necessary to ensure protection of the legal rights of the complainant, including compensation for damage, reinstatement in the workplace, and issuance of an order to cease and desist from retaliation.

In the context of judicial or administrative proceedings to investigate any retaliation against the reporting persons, it is presumed that the retaliation has been put in place as a result of the report; the burden of proving that such conduct or acts were carried out for reasons unrelated to the report, public disclosure, or complaint lies with the party that has committed the said conduct or acts.
This benefit does not apply to: facilitators, people from the same work-related context with a long-term emotional bond or a kinship relationship within the fourth degree with reporting parties or those who make a public disclosure or complaint, work colleagues who work in the same work-related context and have a current, habitual relationship with the reporting person, and also legal entities if they are owned by the reporting person or the person making the complaint or public disclosure, or entities in which the said person works or entities that operate in the same work-related context. Therefore, if any of these parties files a retaliation complaint, the burden of proof lies with them.
In the event that an application for compensation is filed with the judiciary by the reporting persons and these persons demonstrate, pursuant to Italian legislative decree n. 24/2023, that they have made a report, a public disclosure, or a complaint to the judiciary or audit authorities and have suffered damage, it is presumed, unless proven otherwise, that the damage is a consequence of such report, public disclosure, or complaint to the judiciary or audit authority.

Any person who has suffered dismissal as the result of a report, public disclosure, or complaint to the judiciary or audit authority has the right to be reinstated in their job.

Any reporting person who believes they have suffered discrimination or retaliation can also provide detailed information on the discrimination that has occurred: a) to their superior; b) to the personnel tasked with managing the reporting channel; c) to the public prosecution department in the event of a criminal offence.
The reporting person remains within their rights to report the incident to the trade union or to the competent judicial authority.

---

1. The actions listed in art. 17. 4 of Italian legislative decree n. 24/2023 constitute retaliation, in particular: a. dismissal, suspension or equivalent measures; b. demotion or failure to promote; c. change of duties, change of place of work, reduction in pay, change of working hours; d. suspension of training or restriction of access to training; e. negative comments or references; f. imposition of disciplinary measures or other penalties, including pecuniary penalties; g. coercion, intimidation, harassment, or ostracism; h. discrimination or otherwise unfavourable treatment; i. failure to convert a temporary employment agreement into a permanent employment agreement where the worker had a legitimate expectation of such conversion; l. failure to renew or early termination of a temporary employment agreement; m. injury, including injury to reputation, in particular on social media, or financial damage, including loss of income and loss of earning potential; n. early termination or cancellation of an agreement for the supply of goods or services; o. cancellation of a licence or permit; p. being requested to undergo psychiatric or medical tests.

6.5.2 **Confidentiality duties regarding the identities of the reporting person and the facilitator, and exclusion of the report from access rights**

With the exception of the cases of liability for slander, libel, and defamation envisaged in the provisions of the Italian Criminal Code or art. 2043 of the Italian Civil Code and cases in which anonymity is not enforceable by Italian law (e.g. criminal, tax, or administrative law investigations, inspections by supervisory bodies), the reporting person's identity is protected in all contexts following the report.
Therefore, without prejudice to the aforesaid cases, the identity of the reporting person and any other information from which this may be inferred, directly or indirectly, cannot be disclosed, without the express consent of the reporting person, to any persons other than those authorised to receive or follow up the reports, who have been expressly authorised to process such data.
Confidentiality is also guaranteed in the case of reports - whether internal or external - made orally via telephone lines or, alternatively, voice messaging systems or, at the request of the reporting person, through a direct meeting with the person tasked with managing the report.
The confidentiality of the reporting person is protected even when the report reaches personnel other than those tasked with managing the reports, to whom, in any case, they must be sent without delay.
The aforesaid confidentiality duties are likewise guaranteed in relation to the facilitator assisting the reporting person, with regards to both their identity and the assistance activity provided.

All the parties tasked with receiving reports or involved in their management are required to protect the confidentiality of this information.
Any breach of the confidentiality duty will result in liability for disciplinary action, without prejudice to other forms of liability provided for by Italian law.

In criminal proceedings, the identity of the reporting person is covered by duties of confidentiality in the ways and within the limits established by art. 329 of the Italian Code of Criminal Procedure.
In proceedings before the Court of Auditors, the identity of the reporting person cannot be disclosed until the preliminary investigations are complete.

In disciplinary proceedings, the identity of the reporting person cannot be revealed if the disciplinary action is based on investigations which are separate from and further to the report, even if they are a consequence of the report. If the action is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the person subjected to disciplinary proceedings, the report will be usable for the purposes of the disciplinary proceedings only if the reporting person has consented to the disclosure of their identity.
Written notice of the reasons for the disclosure of the confidential data is given to the reporting person if the disclosure of their identity and related information is also essential for the purposes of the defence of the person concerned.
If the reporting person refuses to give consent, the report cannot be used in the disciplinary proceedings which, therefore, cannot be initiated or continued without further information on which to base the action.
In any case, if the respective conditions are met, the party is entitled to proceed by filing a complaint with the judiciary.
In any proceedings initiated following internal or external reports, the identity of the reporting person may only be disclosed where such disclosure is indispensable for the purposes of the defence of the person concerned and if the reporting person consents to the said disclosure.
Written notice of the reasons for the disclosure of the confidential data is given to the reporting person if the disclosure of their identity and related information is also essential for the purposes of the defence of the person concerned.

The report is also excluded from rights available to citizens to access documents made available by public administration authorities and likewise the extension of the same rights to access further documents in addition to those already made available by public administration authorities.

With particular reference to the protection of personal data, it is hereby stated that such data will be processed solely for the purpose of managing the report and verifying the information contained therein.
The said data will be processed with paper and/or electronic/computerised/online tools/media, in full compliance with Italian law, in accordance with the principles of lawfulness and fairness, and in such a way as to protect the confidentiality of the reporting person.

Any disclosure of the identity of the reporting person to persons other than those tasked with receiving or following up the reports is always subject to express consent of the reporting person.

6.6 Protection for the reported party

6.6.1 **Confidentiality duties concerning the identity of the reported party and all the people mentioned in the report**

In compliance with applicable legislation, Pagani has adopted the same forms of protection to guarantee the privacy of the reporting person also for

the person allegedly responsible for the breach, as well as for all the people mentioned in the report; this in no way prejudices any further form of liability provided for by Italian law that results in the obligation to disclose the name of the reported party (e.g. applications to the judiciary).
Except in cases of applications to the judiciary, pending investigations into the liability of the reported party for disciplinary action and until the proceedings initiated due to the report have ended, the personnel tasked with managing the reporting channel must treat the identity of the reported party and all the people mentioned in the report with discretion and confidentiality; more specifically, they must not reveal the name of the reported party without their consent and must not allow third parties to access the report and/or their identity details.
Confidentiality is also guaranteed: a) in the case of reports - whether internal or external - made orally via telephone lines or, alternatively, voice messaging systems or, at the request of the reporting person, through a direct meeting with the person tasked with managing the report; b) when the report is made using other methods than those established by the public administration authorities or other authorities and by ANAC in compliance with the decree; c) when the report reaches personnel other than those tasked with managing the reports, to whom, in any case, they must be sent without delay.
The company does not impose disciplinary penalties on the reported party on the basis of the representations of the reporting person without objective confirmation and due investigation of the events reported and until the end of the proceedings initiated due to the report, which are conducted in compliance with the said guarantees envisaged for the reporting person.

6.6.2 **The reported party's right to be heard**

The reported party may also be heard, at their request, through paper-based proceedings involving the acquisition of written comments and documents.
The reported party does not always have the right to be informed of any report concerning them. This right only exists in the case of proceedings initiated against them following completion of the report management activities and in the event that such proceedings are based in whole or in part on the report.

6.6.3 **Protection of the reported party from reports made in bad faith**

All parties are required to respect each other's dignity, honour, and reputation. To this end, the reporting person is required to declare whether they have any personal interest connected to the report.
More generally, the company guarantees adequate protection against reports made in bad faith, condoning conduct of this kind and stating that reports made with the intention of causing harm or prejudice in any way, as well as any other form of misuse of this mechanism, will result in liability in disciplinary proceedings and proceedings before any other competent authorities.

VII.
TRAINING AND INFORMATION

In order to encourage the use of internal whistleblowing systems and to encourage the diffusion of a culture of legality, Pagani provides its employees and associate workers with clear, accurate, and comprehensive explanations of the internal reporting procedure adopted.
Pagani also ensures timely information for all employees and individuals who collaborate with the company, not only in relation to the reporting methods adopted, but also with reference to the awareness, understanding, and dissemination of the underlying objectives and spirit of implementation.
Information about the reporting channel, methods, and conditions is provided, in a clearly visible manner:

- In the workplace, as well as in places which are accessible to people who, although not frequenting the workplace, have a legal relationship with the company within the scope of this procedure;
- On the Pagani website, at https://www.pagani.com/it/.

The same dissemination methods set out above are adopted for subsequent revisions and additions to the procedure.

The same methods are used to provide information about the conditions for external reporting and public disclosure, as well as regarding retaliation complaints to be filed to ANAC.

VIII.
FOR REPORTING PERSONS: HOW AND WHEN TO MAKE A REPORT USING THE INTERNAL REPORTING CHANNEL

8.1 Who can make a report?

The reporting system may be used by the following parties:

- Employees of the company;
- Independent contractors who provide their services at the company;
- Independent contractors and workers who provide their services or work for entities that supply goods or services to or carry out work for the company;
- Freelance professionals and consultants who provide their services at the company;
- Volunteers and paid and unpaid trainees;
- Shareholders and persons performing administrative, management, control, supervisory, or representation roles, even if these roles are performed within the company on a purely de facto basis;

In all their dealings with the company and as established in the Model and in the Code of Ethics, reporting persons must only report the qualifying disclosures provided for in the section titled "What can be reported?".

8.2 When can a report be filed?

- During an existing legal relationship;
- During a trial period;
- Prior to a legal relationship if the information on the breaches was acquired during a selection process or other pre-contractual activities;
- After termination of a legal relationship if the information on the breaches was acquired prior to the termination of the said relationship.

8.3 Qualifying disclosures: what can be reported?

For the purposes of reports, public disclosures, or complaints, the following matters are deemed qualifying disclosures: information on breaches (including well-founded suspicions) of national and European Union regulations which are detrimental to the public interest or the integrity of a public administration authority or private entity and are committed within the organisation of the entity with which the reporting person has a qualifying legal relationship pursuant to law, namely:

- Accounting, or administrative, civil, or criminal law offences;
- Material misconduct pursuant to Italian legislative decree n. 231/2001, or breaches of the Organisation Models;
- Offences falling within the scope of EU acts relating to the following (sensitive) sectors: public procurement; financial services, products, and markets and prevention of money laundering and the financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and of personal data and security of networks and information systems;
- Acts or omissions which are detrimental to the financial interests of the Union, as identified in EU regulations, directives, decisions, recommendations, and opinions;
- Acts or omissions relating to the internal market, including breaches of EU legislation on competition and state aid, as well as breaches concerning the internal market connected to breaches of corporate tax legislation or mechanisms committed to obtain a tax advantage that defeat the object or purpose of corporate tax legislation applicable to the company;
- Acts or conduct that defeats the object or purpose of the sectorial Union provisions stated in the subsections above.

The report may also include:

- Information relating to conduct aimed at concealing the aforesaid breaches;
- Misconduct which has not yet taken place but which the reporting person reasonably believes could occur in the event of certain actual conditions;
- Well-founded suspicions, as defined by the ANAC Guidelines.

The following are not qualifying disclosures: information that is clearly unfounded, information that is already entirely public knowledge, as well as information based on unsubstantiated rumours and hearsay.

The legislative provisions in question do not apply to:

- Disputes, claims, or applications in which the reporting person or the person who has filed a complaint with the judiciary or audit authority has a personal interest relating exclusively to their individual employment relationships or to their relationships with superiors in their place of employment;
- Reports of breaches which are already provided for as compulsory based on European Union or national acts concerning: financial services, products and markets, prevention of money laundering and terrorist financing, transport safety, and environmental protection;
- Reports of breaches of national security, as well as procurement relating to defence or national security aspects, unless such aspects fall under relevant secondary law of the European Union.

This shall not affect the application of provisions regarding workers' exercise of their right to contact representatives or trade unions and to protection against misconduct or acts prompted by such contact, or the autonomy of the social partners and their right to enter into collective bargaining agreements, as well as the right to repress anti-union conduct stated in art. 28 of Italian law n. 300 dated 20 May 1970.

8.4 Reported parties

The reports may concern any of the following parties: members of the corporate bodies, management, employees, shareholders, independent contractors, or workers not employed by the company, as well as sales partners, suppliers, and any other parties who or which have relationships with the company to whom or which any misconduct that has come to the attention of the reporting person is attributable.

8.5 Contents of the report

The reporting person is required to provide any information which may be useful for the departments responsible for carrying out the necessary and appropriate checks to verify the matter reported. To this end, the report should contain the following information:

- Details of the reporting person including their position or role within the company;
- A clear, complete description of the events reported;
- If known, the time and place of the events reported;
- If known, the duration of the misconduct;
- If known, the personal details or other information that allow identification of the parties concerned (such as the position and the department in which they work), providing all the details that could be useful for verification and investigation purposes;
- Specification of whether or not the party benefited from the matter reported;
- Specification of whether, in the reporting person's opinion, the party may be contacted for further information without jeopardising confidentiality during verification of the report;
- A precise description of the events reported;
- Specification of any other information which could be useful to verify the contents of the report;
- Specification of the ways in which the matter came to the reporting person's attention;
- The details of any other parties who could provide information on the matter reported;
- Any other documents that could be useful to confirm the events reported.

The reporting person should also specify whether: a) the events that have occurred have already been reported to another authority or institution and if so to which authority or institution; b) they have spoken to someone about the matter reported, providing their contact details if this is the case; c) there are other people operating in the same work-related context as the reporting person who have provided assistance in the reporting process, providing their details in the event.

Reports which do not include any information from which the identity of the reporting person can be inferred are considered anonymous.
It should be noted that anonymous reports, i.e. reports without information revealing the identity of the reporting person, even if made using the methods stated below, will only be followed up if they:

- Are adequately detailed and disclose specific events and situations;
- Do not appear, at first sight, to be immaterial, unfounded, or unsubstantiated;

- Concern particularly serious circumstances and describe the matter in an adequately detailed, substantiated, and context-specific manner (e.g. clearly stating names, roles, and positions, mentioning specific departments, procedures, or referring to particular events).

Anonymous reports will therefore be managed according to the criteria established for ordinary reports.
This does not affect the requirement of good faith and truthfulness in the representation of the events, which is intended to protect the reported person.
The report must not concern personal grievances held by the reporting person or claims/requests that fall within the scope of the provisions governing employment relationships or relationships with superiors or co-workers; it must not be abusive in tone or contain personal insults or moral judgments intended to libel or slander or to undermine the reputation and/or personal and/or professional dignity of the person or persons concerned by the matter reported.

8.6 Reporting methods

Concerns must be reported using the dedicated ISWEB reporting channel accessible via the Pagani website, which can also be accessed by pasting the following address into a browser: https://segnalazioni.pagani.com.
The reporting person can choose whether to report completely anonymously or to provide their name and contact details (confidential report).
The reporting person can also state an alternative method for contact them (whistleblowing platform, email, mobile phone, or any other means).

This channel allows users to report concerns in writing using a fillable form.

The software guarantees: a) the utmost confidentiality for the reporting person through specific security requirements; b) maximum protection in terms of security, confidentiality, and compliance with legislation in relation to the activities carried out by personnel tasked with managing the report; c) very high levels of data protection through infrastructure specifically designed to ensure such protection.
The software is continuously updated to ensure constant compliance with applicable legislative and technical requirements.
All operations carried out on the platform are tracked.

The software also allows the reporting person to make anonymous reports directly, and then, if they wish, add their personal data at a later date.

The solution is provided via a cloud service provider accredited by the Italian national cybersecurity agency. All reports received are encrypted.

Use of the reporting channel is protected by secure sockets layer technology.

The reporting person must provide a detailed report, containing all the information which may be useful to personnel tasked with the necessary and appropriate checks and investigations to establish whether the matter reported is founded.

Upon completion of the report submission process, the software assigns the report an identification number. Upon accessing the section headed "Have you already made a report? Enter your receipt.", the user can enter the receipt number generated upon submission of the report; they can then monitor the report management progress or communicate directly with the personnel tasked with managing the report if further information is required or a meeting is sought.

This does not affect the possibility of making a complaint to the judiciary or audit authority for matters within their remit.

IX.
FOR THE PARTIES THAT RECEIVE THE REPORT: WHAT HAPPENS AFTER THE REPORT?

The management of the reporting channel and verification of the validity of the circumstances represented in the report are entrusted to the Pagani legal department manager or the HR manager, based on the division of work and the duties assigned to the respective department.
These departments ensure that all appropriate checks are carried out with respect to the verifiable circumstances reported. These checks may consist of one or more of the following activities and the departments involved must guarantee that they are carried out as quickly as possible and applying certain principles, namely objectivity, competence, and professional diligence. Suitable methods will also be ensured to guarantee transparency, traceability, and fairness during report management activities.
The documentation concerning all the stages of the investigations must be filed correctly according to the type of reporting channel used, in order to demonstrate that due diligence was applied when following up on the report.

Pursuant to the provisions of the Decree, it is also necessary that confidentiality is maintained, during the report investigation stages, concerning the identity of the reporting person, the reported party, and all the persons concerned by and/or mentioned in the report.

For the purposes of this procedure, the personnel tasked with managing the reporting channel are required to:

- Issue notice of receipt of the report to the reporting person within seven days of the date the report was received;
- Maintain dialogue with the reporting person and, if necessary, seek further information;
- Follow up received reports with due diligence;
- Provide feedback on the report within three months of the date of advice of receipt or, in the event that such advice is not provided, within three months of the expiry of the seven-day period starting upon submission of the report.

The activities constituting the reporting management process are described in the following sections.

9.1 Receipt

Once the report has been received, the personnel tasked with managing the reporting channel must issue the reporting person with advice of receipt of the report within seven days of the date of receipt, to inform them that the report has been taken into consideration.
If the internal report concerns breaches of the Model or the Code of Ethics, the personnel tasked with managing the reporting channel will arrange for it to be sent to the Supervisory Body within seven days of receipt.
The Supervisory Body may carry out a parallel investigation for the purposes of the Model and the Code of Ethics.
If the report is sent to any party other than the personnel tasked with managing the report and/or is sent using other methods than those envisaged, the recipient is under obligation to send it to the personnel tasked with management of the reporting channel within seven days of receiving it, sending the original with any attachments and informing the reporting person that it has been sent; this action must be taken ensuring the utmost confidentiality and using methods suitable to protect the reporting person and the identity and integrity of the reported party, without prejudice to the effectiveness of the subsequent investigation activities.
In the event that the reporting person, the reported party, or in any case any person concerned by the report is a member of the personnel tasked with managing the reporting channel, the report may be addressed to the senior management team, who are responsible for ensuring the report is managed effectively, independently, and always in compliance with the duty of confidentiality established by applicable provisions.

9.2 Preliminary check

The aim of the preliminary check is to classify the disclosures received in order to establish which reports need to be processed in accordance with this regulatory instrument, as well as to assess whether the conditions have been met to start the subsequent investigation stage.
The personnel tasked with managing the reporting channel carry out an initial admissibility screening of the report, taking into consideration the following aspects:

- Whether the reporting person falls within the qualifying parties stated in art. 3 of Italian legislative decree n. 24/2023;
- Whether the report falls within the qualifying disclosures envisaged by art. 2 of Italian legislative decree n. 24/2023;
- Whether the report is intended to make the company aware of conduct that puts its business and/or third parties at risk;
- How serious and urgent the risk is for the company and/or third parties;
- Whether the matter reported has already been assessed in the past;
- Whether the report contains sufficient information to be verified or, on the contrary, it is too general in nature or lacks the specific information required to proceed with subsequent investigations.

Once the appropriate investigations and examinations have been completed, the personnel tasked with managing the reporting channel may either:

- Recommend that the reports be filed (informing the reporting person - if known - thereof) if they: i) are inadmissible, as the reporting person does not qualify to make the report and the matter reported is not a qualifying disclosure; ii) are inadmissible due to a) lack of details constituting essential information; b) manifestly unfounded nature of the alleged circumstances reported as qualifying breaches; c) representation of facts so general in nature that the designated offices or person cannot understand them; d) submission of documentation only, without actually reporting any breach; iii) are clearly unfounded and unlawful; iv) disclose events which have already been specifically investigated in the past and have already been filed and no new information has emerged from the preliminary checks carried out which warrants further consideration; v) are detailed, verifiable circumstances for which, given the findings of the preliminary checks conducted, the said personnel do not consider it necessary to proceed with subsequent investigations.

Filed reports may be reopened if new information, documents, or facts are received, or if new information emerges from reports made by other reporting persons which establishes the validity of the report;

- Contact the reporting person if they consider the report to be too general in nature, to seek more information which could be useful for the investigation, and then file the report if no further information is provided or the information provided is deemed insufficient;
- Send non-qualifying disclosures received to the company departments responsible for the matter in question, which will process the reports on the basis of applicable legislation, informing the sender of the disclosure, where possible, that the issue reported does not qualify as a matter for this regulatory instrument and that it will be taken into account by company departments responsible for such matters.

9.3 Investigations

The objective of the verification activities on the reports is to carry out specific checks, analyses, and assessments regarding the validity or otherwise of the events reported, as well as to make any recommendations concerning corrective actions to adopt in the areas or company processes concerned by the report.
After a report has been submitted, if the reporting person is not anonymous, they may be contacted by the competent body to acquire further information of use for the investigations.
The reporting person also has the right to provide any further information which may come to their attention in order to supplement the information already disclosed in the report and may request report status updates; this allows a direct line of communication to be established with the reporting person.

The management of the report and assessment of the validity of the circumstances represented in it are entrusted to the competent bodies, which carry out this activity in compliance with the principles of impartiality and confidentiality and in any way deemed appropriate, including hearing the reporting person personally in addition to any other parties that may also have information on the matter reported.
The personnel tasked with managing the reporting channel carry out, directly, all the activities to investigate the circumstances reported.
They may also seek assistance from and work with the company's various organisations and departments (including the Supervisory Body) when their involvement is necessary due to the nature and complexity of the checks, and likewise with external consultants, in which case the costs are borne by the company.
The personnel tasked with managing the reporting channel will establish the methods for carrying out the investigations and, if deemed appropriate, may communicate directly with the reporting person - if known - or the parties mentioned in the report, or anyone they believe can provide information which is important for proper report management.
During report investigations, the right to confidentiality and respect for the anonymity of the reporting person is maintained unless certain characteristics of the investigations to be carried out make this impossible. In the event, any parties called upon to assist the investigating bodies are subject to the same duties of conduct with regards to maintaining the confidentiality of the reporting person.

If, upon completion of the investigations, it is found that the report is: (i) not founded on objective information, and (ii) made in bad faith or with gross negligence, the personnel tasked with managing the reporting channel:

- May decide (providing their reasons) to file the report, deleting the names and any information that could allow reported parties to be identified,
- Will send the report to the departments concerned, which will decide whether to take any disciplinary measures or other action against the reporting person,
- Will monitor the implementation of such action and ensure the reported party is promptly informed through the reporting channel.

Filed reports may be reopened if new information, documents, or facts are received, or if new information emerges from reports made by other reporting persons which establishes the validity of the report.
If, upon completion of verification activities, the report is deemed founded, the personnel tasked with managing the reporting channel will, depending on the breach:

- promptly inform the following parties of the findings of the investigations and their recommendations: i) the board of directors, represented by the chair of the board and, at the first possible meeting, the entire board of auditors;
- for the purposes of the Model and the Code of Ethics, provide the Supervisory Body with an information notice summarising the reporting management activity, with specification of the findings of the investigations and the progress of the corrective actions identified;
- report the findings of the investigations concerning an ascertained breach to the head of the department to which the perpetrator of the breach belongs, so that the said supervisor can arrange, if necessary, further investigations (possibly involving lawyers), in addition to applying the management and improvement measures within their remit (including disciplinary action if the relative conditions are met);
- take any further measures and/or action as may, in the specific case, be necessary to protect the company, including filing a complaint with the judiciary;
- inform the reporting person promptly through the reporting channel.

9.4 Feedback to the reporting person

Once the investigations are complete and the appropriate decisions regarding the report have been made, the personnel tasked with managing the reporting channel are required to:

- Provide feedback to the reporting person through the reporting channel within three months of the date of the advice of receipt or, in the absence of such notification, within three months of the expiry of the seven-day deadline from the submission of the report, in order to inform them that the report is being managed and assessed and of the activities carried out;
- Prepare, working with any external consultants appointed, a final report setting out the findings of the investigations conducted.

X.
DOCUMENTATION CHECKS, FILING, STORAGE, AND TRACEABILITY

All reports received via the computerised tool are automatically coded and recorded.

All documentation is kept for as long as is necessary to process the report and in any case no longer than five years after the date of notification of the final outcome of the reporting procedure, in compliance with the confidentiality duties envisaged by applicable legislation.

In the event of reports made by telephone:

- If a recorded telephone line or another recorded voice messaging system is used to report a matter, the report is documented (with the consent of the reporting person) by the personnel tasked with this duty by recording the message on a media storage and playing device or by transcribing the message in full. In the event of transcription, the reporting person can check, correct, and then confirm the contents of the transcription by signing it;
- If an unrecorded telephone line or another (unrecorded) voice messaging system is used to report a matter, the report is documented in writing by the personnel tasked with this duty in a detailed account of the conversation. The reporting person can check, correct, and then confirm the contents of the transcription by signing it.

When, at the request of the reporting person, the matter is reported orally during a meeting with the relevant staff, the report is documented (with the consent of the reporting person) by the personnel tasked with managing the reporting channel by recording it on a media storage and playing device or by recording the conversation in the minutes.

In the case of minutes, the reporting person can check, correct, and then confirm the minutes of the meeting by signing them.

In order to guarantee report management and traceability and relating investigation activities, the personnel tasked with managing the reporting channel prepare and update the system dedicated to the management, monitoring, and reporting of reports, ensuring all the relative supporting documents are filed.

For this purpose, the personnel tasked with managing the reporting channel guarantee the storage of the original report documentation and the working papers relating to the investigations and audits relating to the reports, in specific paper/computerised filing systems with the highest security/confidentiality standards in accordance with applicable legislative provisions and according to specific internal rules.

When processed, the personal data of the persons concerned by and/or mentioned in the reports is protected pursuant to applicable law and company procedures on data protection.

XI.
PENALTY SYSTEM

11.1 Loss of protection

The reporting person remains liable before the courts and liable to disciplinary action if:

- the reporting person is found liable according to criminal law for libel, slander, or defamation (even in a non-final first instance ruling) or in the event that such offences are committed in the complaint made to the judiciary or audit authority;
- the reporting person is found liable according to civil law for the same offences due to wilful misconduct or gross negligence;

Furthermore, the reporting party may be found liable in the event of misuse of this procedure, such as reports which are unfounded, manifestly self-serving, and/or are made solely with the intention of harming the reported party or other parties, and any other event of misuse or intentional exploitation of this procedure.

Likewise, penalties are envisaged for all confirmed breaches of the measures put in place to protect the reporting person and the reported party.

Appropriate disciplinary/penalty measures will be applied to the person responsible for the reported misconduct.

The disciplinary measures - as envisaged or stated by the Model, by the respective sectoral collective bargaining agreement, and - where in force - by the disciplinary code of the company concerned, will be proportionate to the extent and seriousness of the misconduct ascertained and may lead to the termination of the employment relationship, in compliance with legal provisions and the provisions of applicable collective bargaining agreements. More specifically, when assessing the disciplinary penalty to be adopted against those responsible for retaliation or discrimination against the reporting person, the seriousness of such retaliation or discrimination and the possible damage to health suffered by the reporting person as a consequence of such measures will be taken into account, as well as the whether the retaliation or discrimination occurred repeatedly or involved two or more people. In the event of reports which have clearly been made in bad faith, the personnel tasked with managing the reporting channel reserve the right to file them, deleting the names and information that could allow the identification of the reported party(ies).

11.2 Limitations of liability

Anyone who discloses or disseminates information on breaches which is covered by duties of confidentiality or by requirements relating to the protection of copyright or the protection of personal data, and likewise anyone who discloses or disseminates information on breaches that is detrimental to the reputation of the person concerned or reported, is not liable.
There is no criminal liability when "at the time of disclosure or dissemination, there were reasonable reasons to believe that the disclosure or dissemination of the information in question was necessary in order to reveal the breach and the report, public disclosure, or complaint to the judiciary or audit authority was made in the required manner".
In the case just stated, there is also no further liability of a civil or administrative law nature.
Unless the events constitute an offence, there is no liability (including civil or administrative law liability) for the acquisition of information on breaches or for lawful access to such information. There is likewise no criminal liability or any other liability (including civil or administrative law liability) for conduct, acts, or omissions connected to the report, public disclosure, or complaint which are strictly necessary to reveal the breach.
There may be, however, criminal liability or any other liability (including civil or administrative law liability) in the event of conduct, acts, or omissions not connected to the report, public disclosure, or complaint to the judiciary or audit authority or which are not strictly necessary to reveal the breach.

11.3 Further provisions

Retaliation, hindrance or attempted hindrance of reporting, breach of the duty of confidentiality, failure to investigate and examine reports received, and manifestly self-serving reports made for the sole purpose of libel, slander or defamation of the reported party or other parties may be punished by the application of disciplinary measures or penalties.
Waivers and agreements concerning, in whole or in part, the rights and protections provided for by this procedure and, in general, by Italian legislative decree n. 24/2023 are not valid, unless they are made in the ways and manners stated in art. 2113.4 of the Italian Civil Code.
In compliance with the provisions of art. 18 of Italian legislative decree n. 24/2023, ANAC has drawn up a list of tertiary sector entities that provide support to reporting persons.
For any matters not expressly provided for herein, reference must be made to Italian legislative decree n. 24/2023.

XII.
PECUNIARY PENALTIES APPLIED BY ANAC PURSUANT TO ADMINISTRATIVE LAW

As envisaged by art. 21 of Italian legislative decree n. 24/2023 and without prejudice to other kinds of liability (pursuant to civil law, criminal law, administrative law, and disciplinary provisions), ANAC may apply the following pecuniary penalties to any person (company, i.e. legal person, or natural person) found liable:

- from €10,000 to €50,000 if it finds that the natural person identified as liable has committed acts of retaliation;
- from €10,000 to €50,000 if it finds that the natural person identified as liable has hindered or attempted to hinder the reporting person when making the report;
- from €10,000 to €50,000 if it finds that the natural person identified as liable has breached the duty of confidentiality stated in art. 12 of Italian legislative decree n. 24/2023. This does not affect the penalties applicable by the Italian data protection authority (known in Italian as the *Garante*) to the parties tasked with data processing activities pursuant to applicable data protection provisions (Measure 146);
- from €10,000 to €50,000 if it finds that no reporting channels have been set up; in this case, liability lies with the steering body, in both public- and private-sector entities;
- from €10,000 to €50,000 if it finds that no procedures have not adopted for making and managing reports or that the procedures adopted do not comply with the provisions of the decree; in this case, liability lies with the steering body, in both public- and private-sector entities;
- from €10,000 to €50,000 if it finds that the reports received have not been examined and investigated; in this case, the party responsible for managing the report is deemed liable;
- from €500 to €2,500, if it finds the reporting person liable, pursuant to civil law, for libel, slander, or defamation in cases of wilful misconduct or gross negligence (even if established with a first-instance ruling) unless the said person has already been convicted (including therein with a first-instance ruling) of libel, slander, or defamation or in any case of the said person committing the same offences in a complaint to the judiciary.

XIII.
ANNEXES

ANNEX 1
INFORMATION ON THE PROCESSING OF PERSONAL DATA IN RELATION TO CONFIDENTIAL REPORTS OF BREACHES (WHISTLEBLOWING NOTICE)

This notice is provided by the data controller in relation to personal data processed as part of activities for managing reports of breaches (also known as 'whistleblowing') made pursuant to Italian legislative decree n.24/2023 and Directive (EU) 2019/1937. If the report comes from a person linked by an employment or working relationship with the data controller, this policy must be understood as a supplement to rather than a substitute for the policy provided by the data controller within the context of management of the employment relationship.

Data controller – contact details

Pagani S.p.A.
registered premises: VIA DELL'ARTIGIANATO N. 5, SAN CESARIO SUL PANARO (MO), POSTCODE: 41018
Tel. 059 4739201
Email: info@pagani.com

Data Subjects

The person who reports the concern (the "Reporting Person"); the reported party or persons mentioned in the report; any other persons concerned by the report as defined by Italian legislative decree n. 24/2023, such as the facilitators or other related persons, all of whom are hereinafter referred to as the "Data subjects".

Processing purposes

The data will be processed for the following purposes and on the lawful basis stated:

- **Purpose:** management of reports made as a result of the application of Italian legislative decree n. 231/01, EU Directive 2019/1937, and Italian legislative decree n. 24/2023
- **Lawful basis:** the processing is necessary to meet a legal requirement applicable to the data controller (GDPR, Art. 6. 1.c)

In no way will your personal data be subjected to automated decision-making processes (profiling).

Categories of personal data processed

For the aforesaid purposes, the following kinds of data must be processed:

- Common identification and contact data of the Reporting Person (except in the case of anonymous reporting) and of the other Data Subjects; other common personal data of the Data Subjects contained in the report;
- Special personal data, as defined by art. 9 of the GDPR, in the following categories (if information of this type is included in the report and relates to the Data Subjects): health and healthcare data, trade union membership, political opinions, religious or philosophical beliefs, and racial or ethnicity data.

Processing methods

The data collected is processed solely by expressly trained personnel authorised by the Data Controller to do so using electronic tools on digital filing systems and manual procedures on paper filing systems; all processing is performed in compliance with the principles of relevance, minimisation, and lawfulness and with personal data legislation; processing is also carried out with the application of guaranteed security measures to prevent unauthorised access to data and the alteration, elimination, or unauthorised disclosure or dissemination of data.

Disclosure of personal data

Personal data may be disclosed to: boards, committees, and bodies, public authorities such as the judiciary or police force, when processing the data as independent data controllers. It may be disclosed to third parties, designated as our data processors, for example to any external consultants or law firms who or which may be involved in the process of managing the report.
Personal data will not be disseminated in any way and will not be sent to third countries. All processing thereof will take place exclusively within the European Union.

Dissemination of personal data

Personal data will not be disseminated in any way.

Transfer of data to third countries

The personal data collected is processed exclusively within the European Union.

Data retention period

In accordance with the terms established by art. 14 of Italian legislative decree n. 24/2023, personal data is retained for as long as is necessary to process the report or for no more than 5 years after the date of notification of the final outcome of the report; furthermore, the data may be kept for as long as is necessary to carry out any proceedings (disciplinary, accounting, or administrative or criminal law) initiated following the report.
This does not affect other provisions for the retention of personal data (including special data) for any longer period (in accordance with the statute of limitations provided for the exercise of rights) for needs linked to the exercise of the right of defence in the event of disputes.
Personal data that is clearly not useful for processing a specific report is not processed and, if collected accidentally, is promptly deleted.

Rights of the Data Subject pursuant to Regulation (EU) 2016/679 - Articles 15 to 22

The Data Subject has the right to contact the Data Controller (at the addresses stated in the contact details) to obtain confirmation of the existence or otherwise of personal data concerning them, including data which has not yet been registered, and the disclosure thereof in an intelligible form. The Data Subject has the right to know: the source of the personal data; the processing purposes and methods; the logic applied in the event of automated processing, i.e. performed with the aid of electronic means; the identification details of the Data Controller, data processors, and the representative of the Data Controller or data processor if they are established outside the European Union; the parties or categories of parties to whom the personal data may be disclosed or who may become aware of it in their capacity as designated representative within the country, as data processors, or persons tasked with data processing duties. The Data Subject is entitled to have: their data updated, rectified, and - when interested therein - completed; the erasure or anonymisation of, or a hold on data processed in breach of the law, including data whose retention is unnecessary for the purposes for which the data was collected or subsequently processed; notification from those to whom the data has been disclosed or disseminated that the deletion and/or anonymisation activities have been carried out (with specification of the content of the data concerned), unless this proves impossible or involves a manifestly disproportionate effort in relation to the rights protected; the portability of data in a structured, transmissible electronic format. The Data Subject has the right to object, in full or in part and for legitimate reasons, to the processing of personal data concerning them.

The Data Subject also has the right to file a complaint with the data protection authority, in the manner and terms envisaged. Please visit the website www.gpdp.it for further details. For further information on the protection of personal data, please visit the website of the Garante, i.e. the Italian data protection authority, at: www.gpdp.it/regolamentoue

Pursuant to article 2-*undecies* of the Italian data processing code or Privacy Code (implementing article 23 of the GDPR), Data Subjects are hereby advised that their rights cannot be exercised (either through a request to the Data Controller or a complaint pursuant to article 77 of the GDPR) if the exercise of these rights would effectively be detrimental to the confidentiality concerning the identity of the reporting person. More specifically, these rights may be exercised: subject to compliance with the sector legal or regulatory provisions; subject to delays, limits, or exclusions - in which case reasoned notice thereof will be given without delay to the Data Subject (unless the provision of such notice could defeat the object of the limitation) - for as long (within limits) this constitutes a necessary and proportionate measure, taking into account the Data Subject's fundamental rights and legitimate interests, in order to maintain confidentiality concerning the identity of the reporting person. In these cases, the Data Subject's rights can also be exercised through the data protection authority (the *Garante*, in Italy) in the manner stated in art. 160 of the Italian data protection code, in which case the said authority will inform the Data Subject when it has carried out all the necessary checks or completed a review, likewise advising the data subject of their right to bring legal proceedings.

ANNEX 2
HOW AND WHEN TO MAKE A REPORT USING THE EXTERNAL REPORTING CHANNEL

ANAC is the competent authority for external reporting, including reports from the private sector.
To make a report directly to ANAC, at least one of the following conditions must be met:

- It is not mandatory for an internal reporting channel to be set up within the work-related context in question or, even if it is mandatory, it is not active or, even if it is activated, it does not comply with the provisions set out herein;
- If the reporting person has already made an internal report but it has not been followed up;
- If the reporting person has reasonable grounds to believe that, if they were to make an internal report, it would not be followed up effectively or the report could prompt retaliation;
- If the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious risk to the public interest.

Like the internal reporting channels, the reporting channel set up by ANAC must ensure (through encryption tools, for example) confidentiality concerning the identity of the reporting person and any persons concerned by the report, as well as the contents of the report and the relevant documentation.

Also in this case, reports may be made either via computerised platform or orally (by telephone or voice messaging systems) and, if requested by the reporting person, through a direct meeting to be arranged within a reasonable timeframe.

If the external report has been submitted to any party who or which is not responsible for such duties, it must be sent, within seven days of receipt, to ANAC, informing the reporting person that it has been sent on.

ANAC is required to:

- Provide any Data Subject with information on the use of the external reporting channel and the internal reporting channel, as well as on the protection measures stated in Italian legislative decree n. 24/23
- Send a notice of receipt of the report to the Data Subject within seven days of the date of receiving it, unless the reporting person expressly requests otherwise or unless ANAC deems that the notice would undermine the confidentiality of the identity of the reporting person;
- Maintain dialogue with the reporting person and, if necessary, seek further information from them;
- Follow up received reports with due diligence;
- Conduct the investigations needed to follow up the report, including hearing accounts and acquiring documents;
- Provide feedback on the report within three months or, if there are clearly explained reasons, within six months of the date of advice of receipt of the external report or, in the event that such notice is not sent, of the terms of seven days after receiving the report;
- Advise the reporting person of the final outcome.

ANAC can decide not to follow up reports disclosing minor breaches and therefore file them.

Confidentiality duties must be upheld even if the report is received through channels other than those established officially or through personnel other than the designated persons; in any case, all reports must be sent on to the latter without delay.

ANAC must employ report management personnel who are appropriately trained to provide Data Subjects with information on the use of internal and external reporting systems and the protection measures to which they are entitled.

ANNEX 3
HOW AND WHEN TO MAKE A REPORT USING PUBLIC DISCLOSURE

A reporting person who makes a public disclosure may also benefit from protection.

A reporting person making a public disclosure will be guaranteed protection provided that at least one of the following conditions is met:

- The reporting person has already made an internal and external report or has made an external report directly and has received no response, within the envisaged deadlines, concerning the measures provided for or adopted to follow up the reports;
- The reporting person has reasonable grounds to believe, on the basis of actual circumstances and therefore not simply on inferences, that the breach may constitute an imminent or obvious risk to the public interest;
- The reporting person has reasonable grounds to believe that the external report may prompt retaliation or may not be effectively followed up due to the specific circumstances of the actual case, such as the risk of evidence being hidden or destroyed or if there is well-founded fear that the person receiving the report may be colluding with the perpetrator of the breach or involved in the breach itself.

Confidentiality protection does not apply if the reporting person has intentionally revealed their identity, for example via web platforms or social media. The same applies in the event that the reporting person contacts a journalist directly. In this case, though, the rules on professional confidentiality for journalists concerning the source of the information apply.

However, in the event that the person making the disclosure does not reveal their identity (e.g. by using a pseudonym or a nickname in the case of social networks), such disclosures are deemed equivalent to anonymous reports.