Whistleblowing
Informativa sulla protezione dei dati personali
(artt. 13 e 14 Reg. Ue 2016/679 GDPR)

La presente informativa viene resa ai sensi degli artt. 13-14 del Regolamento Europeo 2016/679 (di seguito "GDPR") a tutti coloro i quali fanno uso del canale interno di segnalazione predisposto in base a quanto previsto dal d.lgs. 24/2023 di recepimento della Direttiva UE 2019/1937 (c.d. Direttiva "Whistleblowing").

TITOLARE DEL TRATTAMENTO
Il titolare del trattamento dei dati è **GUERRINI INDUSTRY SPA,** con Sede in Via delle Fisarmoniche 41/43, 60022 Castelfidardo (AN), Italy, Tel: (+39) 071 7808177, e-mail: info@guerrinispa.com, PEC: guerrini.industry@legalmail.it

CATEGORIE DATI TRATTATI
Dati personali comuni del Segnalante (nel caso di Segnalazioni non anonime) nonché di eventuali Persone coinvolte ("Segnalati") o menzionate nella Segnalazione ("Terzi") e Facilitatori quali: dati identificativi (ad es. nome, cognome), dati di contatto (es. numero telefonico fisso e/o mobile, indirizzo postale/e-mail).
Dati particolari di cui all'art. 9) o Dati giudiziari di cui all'art. 10) del GDPR, qualora inseriti nella segnalazione.

FINALITA' DEL TRATTAMENTO DEI DATI
Il Titolare tratterà i dati per scopi strettamente necessari all'applicazione ed alla gestione della procedura di Segnalazione.
I suddetti dati personali sono trattati per l'adempimento di obblighi previsti dalla legge o dalla normativa comunitaria (d.lgs. 24/2023, di attuazione della Dir. UE 1937/2019).

BASE GIURIDICA DEL TRATTAMENTO
La base giuridica del trattamento è costituita dall'adempimento di un obbligo legale a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR
In caso di trattamento di dati c.d. "particolari", la base giuridica è l'art. 9, par. 2, lett. b) GDPR in riferimento agli obblighi del datore di lavoro

FONTE DEI DATI
La fonte da cui hanno origine i dati personali è la segnalazione effettuata dal soggetto Segnalante. Il conferimento dei dati personali da parte del Segnalante è volontario, potendo sempre scegliere di rimanere anonimo.

LUOGO DI TRATTAMENTO DEI DATI
I dati non saranno trasferiti in Paesi terzi non appartenenti all'Unione Europea e con normative di protezione dei dati personali non allineate al GDPR. I dati non saranno oggetto di alcuna diffusione a terzi non autorizzati per finalità diverse da quelle riportate nella presente informativa.

TEMPI DI CONSERVAZIONE
Il Titolare del trattamento conserverà i dati personali secondo i termini previsti dall'art. 14 del d.lgs. n. 24/2023, cioè per il tempo necessario al trattamento della segnalazione e comunque per non oltre 5 anni.

CON CHI CONDIVIDIAMO I DATI RACCOLTI
Gestore delle Segnalazioni è la Società SOLUZIONI Srl-Societa' Benefit, con sede legale in Ancona (AN), via I Maggio 50, 60131,tel: 071.2900473, Partita iva 02639800420, email: info@soluzioni-azienda.it, Pec: soluzioni-azienda@pec.it, nominata Responsabile del Trattamento ex art. 28 GDPR, nelle persone nominate Autorizzate al Trattamento ex art. 29

GDPR e 2-quaterdecies Codice della Privacy, che potranno avere accesso ai dati personali relativi alla segnalazione, laddove forniti e raccolti, al fine della gestione della segnalazione secondo quanto previsto dalla Procedura Whistleblowing.
Resta inteso che la condivisione dei dati personali sarà limitata allo stretto necessario al fine di garantire la riservatezza.
Inoltre, per alcuni trattamenti connessi alla gestione amministrativa del Whistleblowing, possono essere autorizzati alcuni dipendenti del Titolare, al fine di riscontrare le istanze del Gestore della Segnalazione, restando salve le garanzie di riservatezza previste dalla normativa.

MODALITA' DEL TRATTAMENTO
I dati personali sono trattati sia con strumenti automatizzati sia con strumenti manuali. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

DIRITTI DEGLI INTERESSATI
L'interessato ha diritto di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione dei trattamenti che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati, ai sensi del GDPR e, pertanto, in qualsiasi momento può richiedere una copia digitale degli stessi o il trasferimento automatico ad altre aziende. Nei casi previsti, può anche opporsi o revocare il consenso prestato. L'eventuale richiesta di esercizio dei diritti sarà valutata nei limiti degli artt. 23 GDPR e 2-undecies d. lgs. 196/2003 (Codice della Privacy). Tali diritti non possono essere esercitati dagli interessati qualora dall'esercizio possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ovvero che segnala violazioni ai sensi degli artt. 52-bis, 52-ter d. lgs. 385/1993 o degli art. 4-undecies e 4-duodecies d.lgs. 58/199. Per esercitare tali diritti o per avere informazioni sul loro contenuto, è possibile inviare una richiesta via e-mail all'indirizzo del Titolare del Trattamento sopra indicato, utilizzando il "*Modulo per l'Esercizio dei Diritti dell'Interessato*" messo a disposizione presso gli uffici aziendali. Resta fermo il diritto per l'interessato di proporre reclamo innanzi all'Autorità Garante per la Protezione dei Dati Personali ex art. 77 GDPR (www.garanteprivacy.it)

WHISTLEBLOWING PROCEDURE

Legislative Decree 24/2023

1. PURPOSE OF THE PROCEDURE AND RELEVANT REGULATORY CONTEXT

This procedure applies to GUERRINI INDUSTRY SPA with headquarters in Via delle Fisarmoniche 41/43, 60022 Castelfidardo (AN), Italy, Tel: (+39) 071 7808177, e-mail: info@guerrinispa.com, pec: guerrini.industry@legalmail.it and has the purpose of implementing and regulating a system of reporting irregularities within the scope of the activities carried out by the Organization.

Specifically, the procedure implements the provisions of Legislative Decree No. 24 of 10 March 2023 (the "Whistleblowing Decree") *"implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions for the protection of persons reporting breaches of national legislation",* which regulates the protection of persons reporting breaches of national or European Union legislation that harm the public interest or the integrity of a public administration or private entity, of which they have become aware in a public or private work context.

The procedure also complies with personal data protection legislation and, in particular, with the provisions of Regulation (EU) 2016/679 (GDPR), relating to the protection of natural persons with regard to the processing of personal data.

2. SUBJECTIVE SCOPE OF APPLICATION

The subjects who can make a Report are divided into:

- Fixed-term or permanent employees
- Self-employed workers
- Freelancers or consultants
- Volunteers and interns (paid or unpaid)
- Hired on a probationary period
- Persons undergoing selection or who have terminated their employment relationship (if the violation is known during the selection process or during the employment relationship)
- Shareholders
- Persons with administrative, management, control, supervisory or representative functions

The subjects protected in the event of a Report are:

- Whistleblower (the person who reports an offence through Whistleblowing channels)
- Facilitator (natural person who assists the Reporter in the Reporting process, operating within the same work context and whose assistance must be kept confidential)

- People from the same work context as the whistleblower, whistleblower or person making a public disclosure and who are linked to them by a stable emotional or kinship bond within the fourth degree

- Work colleagues of the whistleblower, whistleblower or person making a public disclosure, who work in the same work context as the whistleblower and who have a habitual and ongoing relationship with the said person

- Entities owned - exclusively or with majority participation by third parties - by the Reporting Party, whistleblower or person making a public disclosure
- Entities where the whistleblower, whistleblower or person making a public disclosure works (art. 3, paragraph 5, letter d))
- Entities operating in the same work context as the whistleblower, whistleblower or whoever makes a public disclosure

  The Organization falls within the provisions of Articles 2, paragraph 1, letter q) no. 1 and 3, paragraph 2, letter a) of Legislative Decree 24/23 since it has *"employed, in the last year, an average of at least fifty subordinate workers with permanent or fixed-term employment contracts" (Article 2, paragraph 1, letter q) no. 1*

3. OBJECTIVE SCOPE OF APPLICATION

The violations that can be reported pursuant to the Whistleblowing Decree, since the Organization is among those identified by Legislative Decree 24/23, must concern behaviors, acts, or omissions that harm the public interest or the integrity of the private entity (i.e., the Company), of which the Reporting Party has become aware in the workplace, pursuant to art. 3, paragraph 2, letter a) of Legislative Decree 24/23 which states:

"For the persons referred to in Article 2, paragraph 1, letter q), numbers 1) and 2), to the persons referred to in paragraphs 3 or 4, who make internal or external reports, public disclosures, or reports to the judicial or accounting authorities, of the information on the violations referred to in Article 2, paragraph 1, letter a), numbers 3), 4), 5), and 6)"

In particular:
Violations of EU law
It's about:

•offenses committed in violation of the EU legislation listed in Parts 1B and 2 of the Annex to the Decree and all national provisions implementing it (even if the latter are not expressly listed in the aforementioned Annex). It should be noted that the regulatory provisions contained in the indicated parts of the Annex are intended as a dynamic reference as they must naturally be adapted as the legislation itself changes.

Specifically, these offenses relate to the following areas: public procurement; financial services, products, and markets; and the prevention of money laundering and terrorist financing; 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; privacy and data protection; and network and information system security.

For example, consider the so-called environmental crimes, such as the discharge, emission or other release of hazardous materials into the air, soil or water or the unlawful collection, transportation, recovery or disposal of hazardous waste;

•acts or omissions which harm the financial interests of the European Union (Article 325 of the TFEU fight against fraud and illegal activities which harm the financial interests of the EU) as identified in the

EU regulations, directives, decisions, recommendations, and opinions.
Consider, for example, fraud, corruption and any other illegal activity connected to Union expenditure;

•acts or omissions affecting the internal market, which undermine the free movement of goods, persons, services, and capital (Article 26(2) TFEU). This includes violations of EU rules on competition, state aid, corporate tax, and arrangements aimed at obtaining a tax advantage that defeats the object or purpose of the applicable corporate tax legislation;

• Acts or behaviors that undermine the object or purpose of European Union provisions in the areas listed above. This category includes, for example, abusive practices as defined by the case law of the Court of Justice of the European Union. Consider, for example, a company operating in a dominant position on a market. The law does not prevent such a company from achieving a dominant position on a market through its own merits and capabilities, nor from ensuring that less efficient competitors remain in the market. However, such a company could, through its behavior, undermine effective and fair competition in the internal market through the use of so-called abusive practices (predatory pricing, target discounts, bundling), thus violating the protection of free competition.

The reports that are EXCLUDED from the application of the regulation are:

- disputes, claims or requests related to a personal interest of the reporting person or of the person who filed a complaint with the judicial authority which relate exclusively to their individual employment or public employment relationships, or which are inherent to their employment or public employment relationships with hierarchically superior figures.

  Therefore, for example, reports regarding labor disputes and pre-litigation phases, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker or with hierarchical superiors, reports relating to data processing carried out in the context of the individual employment relationship in the absence of harm to the public interest or the integrity of the public administration or private entity are excluded;

- reports of violations where they are already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to Legislative Decree 24/23 or by the national acts which implement the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, even if not indicated in Part II of the Annex to Legislative Decree 24/23;

- reports of violations relating to national security, as well as procurement relating to defence or national security aspects, unless such aspects are covered by relevant secondary legislation of the European Union.

4. INTERNAL REPORTING CHANNEL

The Report Manager is Soluzioni Srl-Società Benefit, via 1° Maggio 50, Ancona (AN), appointed Data Controller pursuant to art. 28 GDPR, which has appointed competent, trained, and specialized personnel in this field.

The following reporting channels have therefore been activated pursuant to Legislative Decree 24/2023:

- via an online platform that allows the electronic submission of reports

In completely confidential written form or, if desired, anonymously, ensuring the confidentiality of the Reporter and the person involved, as well as the content of the Report and related documentation, including through encryption. The Reporter's identity will be disclosed to the Report Manager only if the Reporter has given specific consent. The Reporter may forward the Report at any time and track its progress by connecting to the following address: https://soluzioni-azienda.trusty.report/ Internal reporting can only be handled by specialized personnel who will direct the reporting process in accordance with the provisions of the legislation.

The reporting party remains responsible for retaining and not disclosing their login credentials to the portal to check the status of their report on "Your mailbox," where they can also submit further information.

The written reporting channel may be subject to change. In which case, the Organization will update this procedure and promptly notify all interested parties.

- orally via a dedicated telephone number which will put the whistleblower directly in contact with the Whistleblowing Office located at the company's headquarters
Società Soluzioni Srl-Società benefit, via 1° Maggio 50, Ancona (AN) at the following number:

320.5311894 The

verbal reporting channel will be active Monday through Friday from 10:00 am to 12:00 pm and from 4:00 pm to 6:00 pm, upon request from the Whistleblowing Office; except during holidays or weekdays, during which the online reporting channel will remain active. All information exchanged during telephone communication will remain strictly confidential, and any telephone number

The number used by the Whistleblower will not be stored in the address book. It remains possible to request a way to contact the Whistleblower again if necessary for the proper investigation of the Report. The Whistleblowing Office operator receiving the call will prepare a report of the telephone report by completing the appropriate Report form and will record it in the confidential chronological register held by the Office itself, indicating the received Report with a sequential number. This number will be communicated to the Reporting Party, who can use the identification number whenever they wish to contact the Whistleblowing Office for updates on the Report. During the call, the necessary information will be provided so that the Report can be processed as a Whistleblowing Report, and a brief information on the processing of personal data will be read, indicating the information necessary to find the extended information. If this reporting channel is used, notification of receipt of the report and its acceptance, if compatible with regulatory requirements, will occur upon response and completion of the form.

If the Reporting Person uses the Reporting channel via the online platform or via a dedicated telephone number to request a face-to-face meeting, the meeting will take place, guaranteeing complete confidentiality of anything that may emerge during the meeting, at the offices of the headquarters

of Soluzioni Srl-Società Benefit, with registered office in Ancona (AN), via 1° Maggio, n. 50, 60131.

5. RECIPIENT OF THE INTERNAL REPORTING CHANNEL

The Organization has identified the Whistleblowing Office located at the company Soluzioni Srl-Società Benefit, with headquarters in Ancona (AN), via 1° Maggio 50, as the Recipient of the Reports.
60131.

6. MANAGEMENT OF INTERNAL REPORTING

6.1 Preliminary Evaluation of the Report

Upon receipt of the Report, the Whistleblowing Office in charge:

- or carries out a preliminary analysis of its contents (if necessary also with the support of specialized external consultants) in order to assess its relevance in relation to the scope of application of the Whistleblowing Decree and, in general, of the Procedure;
- or archive the Report if it deems that it is not admissible in accordance with the provisions of the Whistleblowing Decree and this Procedure, such as:

  - manifestly unfounded due to the absence of factual evidence attributable to the Typed Violations; -
  established generic content of the Report of Illegal Conduct that prevents understanding the facts, or the Report of Illegal Conduct accompanied by inappropriate documentation or documentation that prevents understanding the content of the Report itself; - production of documentation only in the
  absence of a Report of Illegal Conduct. In this case, the Whistleblowing Office, pursuant to the provisions of Legislative Decree 24/23 and this Procedure, must provide the Reporting Party with written justification for the reasons for dismissing the case;

As required by Article 4 of Legislative Decree 24/23, a Report submitted to a party other than the Recipient must be forwarded immediately (within seven days) to the latter, with the Reporting Party being notified at the same time.

6.2 Report Management Report

management takes place in compliance with the provisions of this Procedure.
In managing the Report, the Whistleblowing Office carries out the following activities:

- o issues the Reporting Party with an acknowledgement of receipt of the Report within seven days from the date of receipt (in the case of using the online platform, in the case of oral communication, confirmation of receipt of the Report is given at the time of the response and with the drafting of the Register);
- or maintains discussions with the Reporter and – if necessary – requests the latter integrations;
- or follows up on received Reports;
- or provides feedback to the Report within three months from the date of the acknowledgement of receipt of the Report or, in the absence of such acknowledgement, within three months from the expiry of the seven-day deadline from the submission of the Report.

The Whistleblowing Office has the right to request the support of internal functions or specialized external consultants, in compliance with the confidentiality requirements set forth in Legislative Decree 24/23 and this Procedure.

The Whistleblowing Office also has the right to request clarifications and/or additions from the Person Involved during the management of the Report.

Furthermore, the Reporting Party reserves the right to provide further information if the reported incident continues, is interrupted, or even worsens. Reports (and related documentation) are retained by the Recipient for the time necessary to process them and, in any case, no longer than five years from the date of communication of the final outcome of the Report management process.

6.3 Internal investigation activities

In order to evaluate a Report, the Whistleblowing Office may conduct the appropriate internal investigations required either directly or by appointing – subject to the obligation of confidentiality – a person internal or external to the Organization.

6.4. Closing the Report

The evidence collected during internal investigations is analyzed to understand the context of the Report, to establish whether a significant violation pursuant to this Procedure and/or Legislative Decree 24/23 has actually occurred, as well as to identify disciplinary measures, measures suitable for remedying the situation that has arisen and/or preventing a similar situation from recurring in the future.

Furthermore, where a violation has been ascertained, the Whistleblowing Office will communicate the findings to the Management or any offices delegated to do so, so that they can proceed with the appropriate investigations.

Following the investigation:

- in the event that elements of manifest unfoundedness are identified, we will proceed to archive the Report with adequate justification, communicating this to the Reporting Party;

- in the event that the Report appears to be well-founded, the internal or external subjects to whom the Report should be forwarded will be identified, for the relevant investigative investigations, the necessary further checks, as well as for the possible adoption of any measures.

6.5 Activities carried out if the Report is not archived

If the Report is not deemed manifestly unfounded, the Whistleblowing Office, possibly with the support of the Company's Legal Department or the corporate functions responsible for the Report received from time to time, will proceed to identify the parties to whom the Report should be forwarded and who are responsible for managing the Report.

In the event that the Report is forwarded to the Judicial or Accounting Authority, if the Judicial or Accounting Authority, for investigative purposes, wishes to know the name of the Reporting Party, if available, the identity of the Reporting Party will be communicated.

Through the privacy policy on the company website in the Whistleblowing section, the Reporting Party, the person involved, or any other individuals mentioned in the Report, and all authorized parties are given advance notice of the possibility that the Report may be sent to the judicial or accounting authorities.

If the Company forwards the Report to the competent judicial or accounting authority, it will notify the Reporting Party, if possible. Any subsequent additions must be forwarded directly by the Reporting Party to the designated judicial authority.

In the event of disciplinary proceedings, the whistleblower's identity cannot be revealed if the challenge to the disciplinary charge is based on investigations that are separate and additional to the Report, even if they arise as a result of it. Conversely, if the challenge is based on the Report and knowledge of the whistleblower's identity, and is essential for the accused's defense, the Report may be used for the purposes of the disciplinary proceedings only with the Whistleblower's consent to disclosure of his or her identity.

In any case, the defendant's defense may deduce and prove, during the hearing or by submitting defense briefs, the indispensability of knowing the identity of the whistleblower.

Please note that if the reporting party refuses to authorize the transmission of personal data, the disciplinary proceedings cannot be continued and, consequently, no action can be taken against the alleged perpetrator of the reported conduct.

In particular, the identity of the whistleblower may be disclosed only with the consent of the interested party and if requested in writing and with a reasoned communication:
ÿ in disciplinary proceedings where disclosure of identity is essential for the defense of the individual accused of the disciplinary charge;
ÿ in proceedings initiated following internal or external reports where such disclosure is also essential for the purposes of the person involved.

6.6 Anonymous reports or reports outside the scope of the reporting party's protection

Anonymous reports, even if reported internally and with detailed information, are treated as ordinary reports.

Anonymous reports that are not adequately detailed and documented will be archived.
Reports that fall outside the scope of whistleblower protection and are submitted through the dedicated whistleblowing channel will be archived as they are not covered by this procedure and the objective scope of the legislation.

7. PROTECTIVE MEASURES

7.1. Protective measures to protect the whistleblower

Reports must be made in good faith. The reporting party's criminal liability remains unaffected if a report constitutes the crime of slander or defamation or other criminal offenses, without prejudice to Legislative Decree 24/23.

the cases of non-punishability of which

Legislative Decree 24/23 provides for the following protection measures for the Whistleblower and the Connected Parties:

1) Prohibition of retaliation for a Report;

2) Support measures, consisting of information, assistance, and free consultancy from third sector entities listed on the ANAC website regarding reporting procedures and regulatory provisions for the benefit of the Reporter and the Person Involved; 3) Protection from retaliation, which includes: o the ability to notify ANAC of any retaliation they believe they have
suffered following a Report; o the provision of nullity of any actions taken in violation of the prohibition of retaliation, which may also be enforced in court;

4) Limitations of liability in the event of disclosure (or dissemination) of violations covered by an obligation of secrecy or relating to the protection of copyright or the protection of personal data, or of information on violations that damage the reputation of the person involved or reported, if: (a) at the time of disclosure (or dissemination) there were reasonable grounds to believe that the disclosure (or dissemination) was necessary to reveal the Violation; and (b) the conditions set out in the following paragraph existed;

5) Limitations of liability, unless the act constitutes a crime, for the acquisition of information on Violations or for access to the same; 6) Sanctions.

7.2 Protection from retaliation

Retaliatory measures, even if only attempted or threatened, must be communicated exclusively to ANAC (Article 19 of Legislative Decree no. 24/2023), which has the exclusive power to determine whether the retaliatory measure is a consequence of the Reporting/Denunciation/Public Disclosure of Information Relating to Violations.

In particular, the following constitute retaliation, among others, if they can be traced back to this configuration:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including pecuniary ones;
- coercion, intimidation, harassment or ostracism;
- discrimination or any unfavorable treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had a legitimate expectation of such conversion;
- failure to renew or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- improper listing 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;
- the early termination or cancellation of the contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request to undergo psychiatric or medical tests.

7.3 Conditions for the application of protective measures

The protective measures listed above apply to the Reporting Person and Related Parties provided that:

1) at the time of the Report, the author of the Report had reasonable grounds to believe that the information on the Violations reported or denounced was true and fell within the scope of Legislative Decree 24/23;

2) The Report was made in accordance with the provisions of Legislative Decree 24/23. Specifically, retaliation refers to the circumstances set forth in Article 17 of Legislative Decree 24/23, including the following, which are provided for purely illustrative and non-exhaustive purposes: a. dismissal, suspension, or equivalent measures;

b. the change of functions; c. the
failure to renew or early termination of a fixed-term employment contract;
d. discrimination or any other unfavorable treatment;
e. the early termination or cancellation of the contract for the supply of goods or services.

8. CONFIDENTIALITY OBLIGATIONS RELATING TO THE IDENTITY OF THE REPORTER

Without prejudice to any further confidentiality obligations under Legislative Decree 24/23, please note that the identity of the Reporting Party and any other information from which such identity may be directly or indirectly deduced may not be disclosed, without the express consent of the Reporting Party, to persons other than those authorized to receive or follow up on Reports and expressly authorized to process such data pursuant to Articles 29 and 32, paragraph 4 of the GDPR and Article 2-quaterdecies of the Privacy Code.

It is also appropriate to consider the following specific confidentiality obligations: a. in criminal
proceedings the identity of the whistleblower is covered by secrecy in the ways and in the
limits pursuant to art. 329 of the Code
of Criminal Procedure in disciplinary proceedings:
a) the identity of the whistleblower cannot be revealed, where the challenge to the disciplinary charge is based on investigations that are separate and additional to the Report, even if resulting from it;
b) If the disciplinary action is based, in whole or in part, on the Report and knowledge of the whistleblower's identity is essential for the defendant's defense, the Report may be used for disciplinary purposes only with the whistleblower's express consent to disclosure of his or her identity. In this case, the whistleblower will be notified in writing of the reasons for disclosing the confidential information.

9. PERSONAL DATA PROTECTION

The processing of personal data in the management of the internal reporting channel and the received reports is carried out in accordance with the GDPR and the Privacy Code.

The Organization has defined its own model for receiving and managing internal reports, identifying suitable technical and organizational measures to ensure a level of security appropriate to the specific risks arising from the processing performed, also based on a data protection impact assessment, pursuant to Article 35 of the GDPR.

The relationship with external suppliers who process personal data on behalf of the Organization is governed by a data processing agreement, pursuant to Article 28 of the GDPR, which defines the duration, nature, and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the data controller, in accordance with Article 28 of the GDPR.

The persons responsible for receiving or following up on Reports pursuant to this Procedure have been authorised to process the personal data relating to the Reports pursuant to Articles 29 and 32 of the GDPR and Article 2-quaterdecies of the Privacy Code.

The Reporting Party and the Persons Involved will be provided with appropriate information pursuant to Articles 13 and 14 of the GDPR.

With regard to the exercise of the data subject's rights and freedoms, if the data subject is the Involved Person, the rights set forth in Articles 15 to 22 of the GDPR may not be exercised (by submitting a request to the Data Controller or by filing a complaint pursuant to Article 77 of the GDPR) if this could result in actual and concrete harm to the confidentiality of the Whistleblower's identity (Article 2-undecies of the Privacy Code and Article 23 of the GDPR) and/or the pursuit of compliance objectives with the legislation regarding the reporting of unlawful conduct. The Involved Person's exercise of these rights (including the right of access) may therefore be exercised to the extent permitted by applicable law and following an analysis by the competent bodies, in order to balance the need to protect the rights of individuals with the need to combat and prevent violations of good corporate governance rules or applicable regulations. Personal data that are clearly not useful for processing a specific Report are not collected or, if collected, must be deleted immediately.

10. SANCTIONS

Anyone who commits any of the following conduct is subject to financial penalties: 1) committing retaliatory acts against the Reporting Person or Related Persons in relation to Reports; 2) obstructing or attempting to obstruct the submission of the Report; 3) violating the
confidentiality obligations set forth in the Procedure and in Legislative Decree 24/23; 4)
failing to establish reporting channels in accordance with the requirements set forth in Legislative Decree
24/23; 5) failing to adopt a procedure for submitting and managing reports or failing to comply with the same with
Legislative Decree 24/23; 6) failing to verify and analyze the Reports received.

Furthermore, a disciplinary sanction is envisaged against the Reporting Person when (outside of specific cases provided for by Legislative Decree 24/23) the following is ascertained: - even with a first instance sentence,
criminal liability for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial authority
that is to say
- civil liability, for the same reason, in cases of fraud or gross negligence.

11. EXTERNAL REPORTING CHANNEL

ANAC activates an external channel for reporting which guarantees, through the use of encryption tools, the confidentiality of the identity of the reporting person, of the person involved and of the person mentioned in the Report, as well as of the content of the Report and of the related

documentation.

External reports must be sent to ANAC as the only body competent for their management, with the exception of reports to the judicial authorities.

Whistleblowing reports may be submitted to ANAC by authorized persons as indicated in Article 3 of Legislative Decree No. 24/2023. It should be noted that pursuant to Article 2, paragraph 1, letter g), *"Reporting Person"* means *"the natural person who makes the Report or publicly discloses information on violations acquired in the context of their work":* the Reporting Person must necessarily be a natural person.

Therefore, reports submitted by other individuals, including representatives of trade unions, are not taken into consideration, as the whistleblowing mechanism is intended to protect individuals acting on their own initiative, not through their union affiliation. In the latter case, the reports are archived as they lack the subjective requirement required by law and, if they concern matters falling under the jurisdiction of ANAC, are treated as ordinary reports.

Please note that the Report and the attached documentation are exempt from the right of access and the access referred to in Article 2-undecies, paragraph 1, letter f) of the Personal Data Protection Code.

The external report is acquired by ANAC through the specifically designated channels.
It's about:

- IT platform (at the ANAC website)
- Oral reports
- Direct meetings scheduled within a reasonable timeframe

Please note that recourse to the external reporting channel established at ANAC can only occur if:
1) the internal reporting channel indicated in the Procedure is not active; 2) the Reporter has already made a Report to the channel indicated in the Procedure and it has not been followed up; 3) the Reporter has reasonable grounds to believe that, if he or she were to make an internal Report through the channel provided for in this Procedure, it would not be followed up or the Report could give rise to the risk of retaliation; -

4) The Reporting Party has reasonable grounds to believe that the Violation to be reported may constitute an imminent or manifest danger to the public interest. To use this external reporting channel or to seek public disclosure, please refer to the ANAC guidelines and official website.

12. PUBLIC DISCLOSURE

Without prejudice to the rules on professional secrecy of journalists with reference to the source of the news, the Reporting Person who makes a public disclosure benefits from the protection provided in favour of the Reporting Person if, at the time of the disclosure
public, one of the following conditions applies:

• the reporting person has previously made an internal and external Report or has directly made an external Report, under the conditions and in the manner established by law (articles 4 and 7 of Legislative Decree no. 24/2023) and no response has been given within the terms established by the same law

(Articles 5 and 8 of Legislative Decree no. 24/2023) regarding the measures envisaged or adopted to follow up on reports;
• the Reporting Person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest;
• the Reporting Person has reasonable grounds to believe that the external Report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the specific case, such as those in which evidence may be hidden or destroyed or in which there is a well-founded fear that the person receiving the Report may be in collusion with the perpetrator of the violation or involved in the violation itself.

Public disclosure means that information about violations is made public through the press, electronic media, or any other means of dissemination capable of reaching a large number of people. Public disclosure of violations must comply with the conditions established by the legislator so that the person making the disclosure can benefit from the protections afforded by the decree.

If the subject voluntarily reveals his or her identity, the protection of confidentiality is not relevant.

13. REPORT TO THE JUDICIAL OR ACCOUNTING AUTHORITY

Persons protected by Legislative Decree no. 24/2023 may contact the judicial or accounting authorities to file a report of unlawful conduct they have become aware of in a work context.

14. INFORMATION AND TRAINING

Information on this Procedure is made accessible and available to all, including in a dedicated section of the company website. Information on the Procedure is also made available during the hiring and departure of an employee. Training on whistleblowing and, more generally, on the provisions of this Procedure is also included in the Organization's compliance training plans.

This procedure may be modified or updated in the future; in which case, the Organization will make the new procedure available through the same channels.