WHISTLEBLOWING PROCEDURE

1. SCOPE OF APPLICATION

This procedure (the "**Procedure**") applies to Thaleia S.p.A. ("**Thaleia**" or the "**Company**") and its subsidiaries, if any. Thaleia will make every effort to ensure that affiliated companies also adopt the Procedure for reports of unlawful conduct as defined by Legislative Decree No. 231/01 and violations of the Organizational Management and Control Model and the Code of Ethics.

2. PURPOSE

The Procedure aims to regulate the process of receiving, analyzing, and handling "internal" Reports (as further defined) submitted by anyone, including anonymously, and to describe the protections that the law offers to individuals who submit Reports and to those involved in them.

3. GENERAL PRINCIPLES

Confidentiality and Privacy Protection

All individuals involved in receiving and processing Reports must ensure the utmost confidentiality of the information received, including the identity of Reporters, Reported individuals, others involved or mentioned, the content of the Report, and related documentation, subject to legal obligations.

The processing of personal data concerning individuals involved and/or mentioned in the Reports, as well as Reporters, will be carried out in compliance with Legislative Decree No. 24/2023, EU Regulation No. 679 of April 27, 2016 (GDPR), Legislative Decree No. 196/2003 (Privacy Code), as amended, and Legislative Decree No. 101/2018.

Protective Measures

Individuals submitting a Report under this Procedure are granted specific protections as outlined in paragraph 10 below. Retaliation or discriminatory actions, whether direct or indirect, for reasons related to the Report are strictly prohibited.

4. PROCEDURE

4.1 Recipients

The Procedure applies to the following individuals (the "**Recipients**"):

- Corporate executives and members of corporate bodies;
- Employees;
- Partners, clients, suppliers, consultants, collaborators, and, more generally, anyone with an interest-based relationship with the Company.

The "**reporting person**" [as defined in Art. 2, para. 1, lett. g), Legislative Decree No. 24/23 "**Reporter**"] who becomes aware of potentially reportable facts is encouraged to promptly submit a

Report using the methods described below, refraining from undertaking independent analysis or investigation.

The process of receiving, analyzing, processing, and responding to Reports is managed by the **Supervisory Body**.

4.2. Definitions

- **Facilitator**: A natural person who assists a Reporter in the reporting process, operating within the same work environment, and whose assistance must remain confidential.
- **Report Manager**: The person responsible for managing and, where necessary, assigning Reports for review to the appropriate bodies via the IT Platform. The Report Manager may use specifically trained and authorized internal or external resources for operational activities.
- **IT Platform**: A dedicated digital channel for submitting and managing Reports, including anonymously, ensuring the confidentiality of the identity of the Reporter, the Reported individual, and others involved, as well as the content of the Report and related documentation.
- **Retaliation**: Any act, omission, or behavior, even if merely attempted or threatened, related to the Report and resulting in, or potentially resulting in, unjust harm to the Reporter, directly or indirectly. This includes acts, measures, or behaviors occurring in the work context and negatively impacting protected individuals.
- **Reporter**: An individual who submits a Report containing information on Violations acquired within their professional context.
- **Reported**: The individual or entity named in the internal Report as the person to whom the Violation is attributed or as a person otherwise implicated in the reported or publicly disclosed Violation.
- **Report or Reporting**: The written or verbal communication of information on Violations (see par. 4.3 below).
- **Violation**: Acts, omissions, or behavior that harm the public interest or the integrity of the public administration or private entity, as defined by Art. 1, para. 1, lett. a), no. 2), Legislative Decree No. 24/23, constituting conduct relevant under Legislative Decree 231/2001 or violations of organizational and management models specified therein.

4.3. Whistleblowing Report

A “whistleblowing” Report refers to any communication regarding:

- Unlawful conduct relevant under Legislative Decree 231/01;
- Violations of the Organizational Management and Control Model and the Code of Ethics.

Reports should be based on precise and consistent factual elements of which the Recipients are aware due to their professional role. Reports must be made in good faith and contain specific, easily verifiable information.

Reports should be submitted responsibly, in the interest of the common good, and fall within the non-compliance categories for which the system was implemented.

In general, the Company encourages employees to resolve work disputes, where possible, through informal dialogue with colleagues and/or direct supervisors.

4.4. Reporting channels

The Company has activated an IT Platform in the cloud, provided by Whistleblowing Solutions I.S. S.r.l., for managing internal Reports.

The IT Platform can be accessed via the following link, also available on the Company website, https://thaleia.whistleblowing.it/, and allows Reports to be submitted through a guided process:

- **In writing**, using one of the following methods:
  - By regular mail to the address: Thaleia S.p.A., Supervisory Body – Reports, Via Santa Tecla, 4, 20122 Milan;
  - Through the IT Platform, accessible via the website mentioned above.
- **Orally**:
  - Through a direct meeting, upon explicit request from the Reporter made through one of the above channels, with the Report Manager. The content of the meeting, with the Reporter's authorization, will be documented either by recording on a suitable device or by a report prepared by the Report Manager and signed by the Reporter.

4.5 Report Manager

The **Report Manager** is the **Supervisory Body** of Thaleia.

The Report Manager prepares an annual budget estimate for the proper execution of assigned tasks, which is submitted for approval by the governing body.

When conducting investigations, the Report Manager may be supported by relevant organizational units within the Company or by external professionals specifically appointed for this purpose.

If a Report is received by someone other than the Report Manager through channels other than those provided by the Company, the recipient must forward it to the IT Platform within seven days, notifying the Reporter and retaining no copies.

4.6 Content of Reports

Reports should be as detailed as possible to enable appropriate verification. In particular, a Report should include the following elements:

- The identity of the person submitting the Report (if they choose not to remain anonymous), including their organizational unit and/or role within the Company;
- A clear and complete description of the events subject to the Report;

- The date and location of the reported events;
- Elements, if known, that allow identification of the individual responsible for the reported events;
- Any other individuals who may provide information regarding the reported facts;
- Any documents supporting the credibility of the reported facts.

Reports must not concern personal complaints or claims within the scope of employment relationships or issues with superiors or colleagues.

Detailed anonymous Reports (including all necessary objective elements for verification) will be considered for further investigation.

4.7 Management of Reports

Upon receiving a Report, the Report Manager will issue an acknowledgment of receipt to the Reporter within seven days of receiving it. The Report Manager will then proceed with handling the Report or forward it to the Company if it is deemed outside their scope but still relevant to the Company.

Reports undergo the following review process:

Preliminary Evaluation of Admissibility

Upon receiving the Report, the Report Manager conducts an initial assessment to determine its admissibility by verifying:

- Whether the Report falls within the subjective and objective scope of Legislative Decree 24/23;
- The details of the time and place where the reported event occurred, a description of the reported facts, and how these facts were brought to light;
- Identifying details or other information that allows for the identification of the individual responsible for the reported facts.

If sufficient and useful elements emerge to substantiate the Report, the next phase of specific investigation will commence.

If the preliminary assessment concludes there are insufficient details or that the reported facts are unsubstantiated, the Report will be filed with the appropriate justification, with feedback provided to the Reporter within the time limits specified by Legislative Decree 24/23.

Investigation and Specific Inquiries

Once the Report's admissibility is confirmed, the Report Manager will:

i Gather necessary information for evaluation through analysis of the received documentation and information;

ii Initiate specific inquiries, if appropriate, using the Company's relevant departments or external experts;
iii Coordinate with relevant departments regarding any actions to protect the Company's interests (e.g., legal actions, suspension/removal from the supplier list, etc.);
iv Request disciplinary action against the Reporter if the Report is found to be made in bad faith and/or with defamatory intent, possibly confirmed by its lack of merit;
v Submit the findings for the Company's review for appropriate measures;
vi Terminate the investigation at any stage if the Report is deemed unfounded.

The activities described above do not necessarily follow a sequential order.

If the assistance of third-party professionals or specialized support from other Company personnel is required, any data that could identify the Reporter or other involved individuals must be obscured.

All investigation phases must be accurately recorded and archived.

The processing of personal data concerning individuals involved and/or mentioned in Reports, as well as Reporters, is carried out in compliance with Legislative Decree No. 24/2023, EU Regulation No. 679 of April 27, 2016 (GDPR), Legislative Decree No. 196/2003 (Privacy Code), and Legislative Decree No. 101/2018. These obligations also apply to internal individuals other than the Report Manager involved in managing the Report.

Feedback to the Reporter

The Report Manager will provide feedback to the Reporter within three months from the date of acknowledgment of receipt, or if no acknowledgment is issued, within three months from the expiration of the seven-day acknowledgment deadline.

The feedback may include:

- Confirmation that the Report has been archived, with an explicit indication of the reasons;
- Confirmation that the Report's validity has been established and that it has been forwarded to the relevant bodies;
- Information about the steps taken so far and those planned.

In this latter case, the Report Manager will also inform the Reporter of the final outcome of the investigation.

4.8 Conflict of Interest

If a Report concerns one of the Report Managers, it will be managed by members who are not in conflict, thus excluding the person to whom the Report pertains.

4.9 Protection and Responsibility of the Reporter

The new decree extends protection to the following individuals:

- Employees under a standard employment contract;
- Self-employed workers performing activities for the Company;
- Freelance professionals and consultants working with the Company;
- Volunteers and interns, both paid and unpaid, working in private sector entities;
- Shareholders.

Protection applies to all these individuals during their probation period, prior to or after establishing an employment relationship or other legal relationship.

The identity of the Reporter is protected in all contexts following submission through internal channels or any external Reports or complaints known to the Report Manager.

In disciplinary proceedings initiated against the Reported person, the Reporter's identity may be disclosed, with the Reporter's express consent, to the relevant department when the disciplinary allegation is partly or entirely based on the Report (submitted through reporting channels or a complaint) and when knowledge of the Reporter's identity is deemed essential for the defense of the Reported. In such cases, the Reporter is notified in writing of the reasons for disclosing confidential data.

In proceedings before the Court of Auditors involving the Reported, the Reporter's identity is protected until the investigation closes. Afterward, the accounting authority may disclose the identity for use in the proceedings.

In criminal proceedings against the Reported, the Reporter's identity is protected under official secrecy until the conclusion of preliminary investigations. If the judiciary, for investigative purposes, requires the identity of the Reporter, the competent company function will provide it.

If the Report Manager finds evidence of the Reporter's bad faith, confidentiality protection is removed, and the Reported is informed of the Reporter's identity to allow for a potential complaint for slander or defamation.

No retaliation or discrimination, direct or indirect, may occur against anyone who submits a Report in good faith. Retaliatory actions include:

- Dismissal, suspension, or equivalent measures;
- Demotion or denial of promotion;
- Changes to duties, relocation, salary reduction, or modification of working hours;
- Suspension or restriction of access to training;
- Negative performance evaluations or references;
- Disciplinary measures or other penalties, including monetary fines;
- Coercion, intimidation, harassment, or ostracism;
- Discrimination or unfavorable treatment;

- Failure to convert a fixed-term contract into a permanent one, where the employee had a legitimate expectation of conversion;
- Non-renewal or early termination of a fixed-term contract;
- Early termination or cancellation of a contract for goods or services;
- Revocation of a license or permit.

Penalties apply to individuals who violate Reporter protection measures and to those who file malicious or grossly negligent Reports, or Reports proven to be false, defamatory, or made solely to damage the Company, the Reported, or others.

The Company reserves the right to take appropriate legal action in any case.

Protection is also extended to:

- Facilitators;
- Individuals in the Reporter's work environment, those who have reported to judicial or accounting authorities, or those who have publicly disclosed a report and who share a close emotional bond or family relationship up to the fourth degree;
- Colleagues in the same work environment with an ongoing, frequent relationship with the Reporter or the individual who filed a report to judicial or accounting authorities or publicly disclosed it;
- Entities owned by the Reporter or individuals who have reported to judicial or accounting authorities or made public disclosures, as well as entities operating in the same work environment as these individuals.

4.10. Protection of the Reported Person

The Report is not sufficient to initiate any disciplinary proceedings against the Reported Person. If, following concrete evidence gathered regarding the Report, it is decided to proceed with the investigative activity, the Reported Person may be contacted and will be assured the opportunity to provide any necessary clarification.

4.11. External Reporting

The primary Reporting channel to be used is the internal one made available by the Company.

The National Anti-Corruption Authority (ANAC) activates an external reporting channel that guarantees, including through the use of encryption tools, the confidentiality of the identity of the Reporting Person, the involved person, and the person mentioned in the Report, as well as the content of the Report and related documentation. The same confidentiality is ensured even when the Report is made through channels other than those indicated in the first sentence or is received by personnel other than those assigned to handle the Reports, to whom it is transmitted without delay.

The Reporting Person may submit an external Report if, at the time of its submission, one of the following conditions applies:

a) there is no mandatory internal Reporting channel within their working context, or it is not active or, even if active, does not comply with the provisions of Article 4 of the Decree;
b) the Reporting Person has already made an internal Report pursuant to Article 4, and it has not been followed up;
c) the Reporting Person has reasonable grounds to believe that an internal Report would not be effectively followed up or that such a Report could result in retaliation;
d) the Reporting Person has reasonable grounds to believe that the violation may pose an imminent or obvious threat to the public interest.

External Reports are made in writing via the ANAC's designated online platform or orally through telephone lines or voice messaging systems, or, at the request of the Reporting Person, through a direct meeting scheduled within a reasonable timeframe. All necessary information for making an external Report, as well as management methods, are published on ANAC's institutional website.

If the above conditions are not met, the subject does not benefit from the protections provided by the Decree.

4.12. Reporting to the Judicial Authorities

It remains the case that the Reporting Person may freely approach the relevant national authorities, judicial and accounting.

4.13. Periodic Reporting

In the periodic report required by the Organizational Models pursuant to Legislative Decree 231/01, the Supervisory Body provides a summary of the Reports received, appropriately anonymized.

This report contains, for relevant reports pursuant to Legislative Decree no. 231/01, the outcomes of the analyses.

4.14. Sanctions

Sanctions are provided against those who violate the measures to protect the Reporting Person, as well as against the Reporting Person in the case of Reports made with intent or gross negligence or found to be false, unfounded, defamatory, or made solely to harm the Company, the Reported Person, or other parties involved in the Report.

Without prejudice to other responsibilities, ANAC imposes the following administrative fines on the responsible party:

a) from 10,000 to 50,000 euros when it is determined that retaliation has occurred, that the Report was obstructed or attempted to be obstructed, or that the confidentiality obligation under Article 12 was violated;

b) from 10,000 to 50,000 euros when it is determined that Reporting channels have not been established, that procedures for submitting and managing Reports have not been adopted, or that the adoption of

such procedures is not compliant with Articles 4 and 5, as well as when it is determined that no verification and analysis activities have been carried out on the received Reports;

c) from 500 to 2,500 euros, in the case of Article 16, paragraph 3, unless the Reporting Person has been convicted, even in the first instance, for defamation or slander or similar offenses committed by reporting to judicial or accounting authorities.

The Company has provided, in its disciplinary system adopted pursuant to Article 6, paragraph 2, letter e), of Legislative Decree no. 231/2001, sanctions against those found to be responsible for the aforementioned violations.

In any case, the right to a fair hearing is guaranteed.

4.15. Documentation Retention and Privacy Protection

To ensure the management and traceability of Reports and related activities, the Report Manager maintains all supporting documentation of the Report for a period of 5 years from the closure of the Report.

Any personal and sensitive data contained in the Report, including those related to the identity of the Reporting Person or other individuals, will be processed in compliance with data protection laws, such as purpose limitation and data minimization, and Reports cannot be used beyond what is necessary to appropriately follow up.

Personal data processing is carried out in compliance with the following principles:

- process data lawfully, fairly, and transparently;
- collect data solely for the purpose of managing and following up on Reports, public disclosures, or complaints made;
- ensure that data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. In this regard, personal data that is not useful for processing a specific Report is not collected or, if accidentally collected, is deleted without delay;
- ensure data accuracy and, if necessary, update it;
- retain data in a form that allows identification of the data subjects for the time necessary to process the specific Report and in any case no longer than five years from the date of communication of the final outcome of the Reporting procedure;
- process data in a manner that ensures adequate security of personal data, including protection through appropriate technical and organizational measures against unauthorized or unlawful processing and accidental loss, destruction, or damage (use of encryption tools);
- ensure the updating of the processing activities register, integrating it with information related to the acquisition and management of Reports;
- ensure the prohibition of tracking Reporting channels;
- ensure, where possible, the tracking of authorized personnel's activity in compliance with safeguards for the Reporting Person.

4.16. Policy Update

The Policy and the Platform's functionality will be subject to periodic review by the Company's General Manager or CEO to ensure constant alignment with the applicable regulations.

The Company will also consider, for the purposes of modifications/integrations to this Policy, any suggestions made by the Supervisory Body.

3. AMBITO DI APPLICAZIONE

La presente procedura (la "**Procedura**") si applica a Thaleia S.p.A. ("**Thaleia**" o "**Società**") e sue eventuali società controllate. Thaleia si attiverà al meglio per far sì che anche eventuali società partecipate adottino per quanto possibile la Procedura in relazione alle segnalazioni di condotte illecite rilevanti ai sensi del D.lgs. n. 231/01 e di violazioni del Modello di Organizzazione Gestione e Controllo e del Codice Etico.

4. OGGETTO

La Procedura si propone di disciplinare il processo di ricezione, analisi e trattamento delle Segnalazioni (come più oltre definite) "interne", da chiunque inviate e trasmesse, anche in forma anonima, nonché

di descrivere le forme di tutela che il nostro ordinamento offre ai soggetti che inviano Segnalazioni e ai soggetti coinvolti nelle Segnalazioni.

3. PRINCIPI GENERALI

Tutela della riservatezza e della privacy

Tutti i soggetti coinvolti nella ricezione e trattamento delle Segnalazioni devono garantire l'assoluta riservatezza delle informazioni ricevute attraverso le Segnalazioni e, in particolare, dell'identità dei Segnalanti, dei Segnalati, delle persone coinvolte e/o menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione, fatti salvi gli obblighi di legge.

Il trattamento dei dati personali delle persone coinvolte e/o citate nelle Segnalazioni nonché dei soggetti Segnalanti viene effettuato in conformità a quanto previsto dal D.lgs. 24/2023, dal Regolamento UE n. 679 del 27 aprile 2016 (GDPR), dal D.lgs. 196/2003 (Codice della Privacy) e s.m.i. e dal D.lgs. 101/2018.

Misure di protezione

Nei confronti del soggetto che effettua la Segnalazione ai sensi della presente Procedura sono accordate specifiche tutele, come indicate nel paragrafo 10 che segue. In particolare, non è consentita, né tollerata, alcuna forma di ritorsione o misura discriminatoria, diretta o indiretta, per motivi collegati alla Segnalazione.

4. PROCEDURA

4.1 Destinatari

La Procedura si applica ai seguenti soggetti (i "**Destinatari**"):

- i vertici aziendali ed i componenti degli organi sociali;
- i dipendenti;
- i partner, i clienti, i fornitori, i consulenti, i collaboratori e, più in generale, chiunque sia in relazione d'interessi con la Società.

La "***persona segnalante***" [*ex* art. 2, comma l, lett. g), D.lgs. n. 24/23 "**Segnalante**"] a conoscenza di fatti potenzialmente oggetto di segnalazione è invitata ad effettuare la Segnalazione con tempestività mediante le modalità di seguito descritte astenendosi dall'intraprendere iniziative autonome di analisi e/o approfondimento.

Il processo di ricezione, analisi, trattamento e riscontro è gestito dall'**Organismo di Vigilanza**.

4.2. Definizioni

- **Facilitatore**: una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- **Gestore delle Segnalazioni**: soggetto a cui è affidata la responsabilità di gestire e, ove necessario, assegnare agli organi competenti l'istruttoria delle Segnalazioni ricevute mediante l'apposita Piattaforma Informatica. Nella gestione delle attività operative il Gestore delle Segnalazioni può avvalersi del supporto di risorse interne o esterne specificamente formate e autorizzate;

- **Piattaforma Informatica**: canale informatico dedicato all'invio e alla gestione delle Segnalazioni, anche in forma anonima, che garantisce la riservatezza dell'identità del Segnalante, dei Segnalati e delle persone comunque coinvolte, nonché del contenuto della Segnalazione e della relativa documentazione;
- **Ritorsione**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione e che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto. Come meglio precisato al paragrafo che segue, si tratta di atti, provvedimenti o comportamenti che si verificano nel contesto lavorativo e che arrecano un pregiudizio ai soggetti tutelati;
- **Segnalante**: la persona fisica che effettua la Segnalazione di informazioni sulle Violazioni acquisite nell'ambito del proprio contesto lavorativo;
- **Segnalato**: la persona fisica o giuridica menzionata nella Segnalazione interna come persona alla quale la Violazione è attribuita o come persona comunque implicata nella Violazione segnalata o divulgata pubblicamente;
- **Segnalazione o segnalare**: la comunicazione scritta od orale di informazioni sulle Violazioni (v. *infra* par. 4.3);
- **Violazione:** comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono [*ex* art. 1, comma l, lett. a), n. 2) D.lgs. n. 24/23] nelle condotte illecite rilevanti ai sensi del D.lgs. 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6) dell'art. 1, lett. a), n. 2), D.lgs. 24/23.

4.3. La Segnalazione whistleblowing

La Segnalazione "*whistleblowing*" riguarda qualsiasi comunicazione di:

- condotte illecite rilevanti ai sensi del D.lgs. n. 231/01;
- violazioni del Modello di Organizzazione Gestione e Controllo e del Codice Etico;

fondata su elementi di fatto precisi e concordanti, di cui i Destinatari siano venuti a conoscenza in ragione delle funzioni svolte.

Le Segnalazioni devono essere effettuate in buona fede e devono essere circostanziate con informazioni precise in modo da risultare facilmente verificabili.

Le Segnalazioni devono essere fatte con spirito di responsabilità, avere carattere di interesse per il bene comune, rientrare nelle tipologie di non conformità per cui il sistema è stato implementato.

In linea generale la Società esorta i propri dipendenti a risolvere eventuali controversie lavorative, ove possibile, attraverso il dialogo, anche informale, con i propri colleghi e/o con il proprio responsabile diretto.

4.4. I canali per le Segnalazioni

La Società, per la gestione delle Segnalazioni interne, ha attivato la Piattaforma Informatica in *cloud* fornita da Whistleblowing Solutions I.S. S.r.l..

La Piattaforma Informatica è raggiungibile tramite il seguente link, disponibile anche sul sito della Società, _____ e consente di effettuare, attraverso un percorso guidato, Segnalazioni:

- in **forma scritta**, con uno dei seguenti strumenti alternativi:
  - Tramite posta ordinaria al seguente indirizzo: Thaleia S.p.A., Organismo di Vigilanza – Segnalazioni, Via Santa Tecla, 4, 20122 Milano;
  - Attraverso la Piattaforma Informatica accedendo alla pagina internet di cui sopra;
- In **forma orale**:
  - Con un incontro diretto, previa espressa richiesta del Segnalante avanzata tramite uno dei succitati canali, con il Gestore delle Segnalazioni. Il contenuto dell'incontro, previa autorizzazione del Segnalante, verrà documentato mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure verrà riportato in un verbale redatto dal Gestore della Segnalazione e sottoscritto dal Segnalante.

4.5. Gestore delle Segnalazioni

Il **Gestore delle segnalazioni** è **l'Organismo di Vigilanza di Thaleia.**

Il Gestore formula annualmente la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati. Tale previsione è sottoposta all'approvazione dell'organo dirigente.

Nello svolgimento dell'istruttoria, il Gestore delle Segnalazioni può essere supportato dalle strutture organizzative aziendali di volta in volta competenti ovvero dai professionisti esterni allo scopo incaricati.

Nel caso in cui un soggetto diverso dal Gestore delle Segnalazioni riceva una Segnalazione attraverso canali ulteriori rispetto a quelli predisposti dalla Società, questi dovrà trasmetterla entro 7 giorni alla Piattaforma Informatica dandone contestuale notizia al Segnalante e senza trattenerne copia.

4.6. Contenuto delle Segnalazioni

Le Segnalazioni devono essere il più possibile circostanziate al fine di consentire le dovute verifiche. In particolare, una Segnalazione deve contenere i seguenti elementi:

- le generalità del soggetto che effettua la Segnalazione (se ritiene di non rimanere anonimo), con indicazione dell'unità organizzativa di appartenenza e/o dell'attività svolta per la Società;
- una chiara e completa descrizione dei fatti oggetto di Segnalazione;
- data e luogo dei fatti riportati;
- elementi che, ove noti, consentano di identificare il soggetto che ha posto in essere i fatti segnalati;
- indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto della Segnalazione;
- allegazione di eventuali documenti che possano confermare la fondatezza dei fatti riportati.

Le Segnalazioni non possono riguardare doglianze di carattere personale o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro o rapporti col superiore gerarchico o con i colleghi.

Eventuali Segnalazioni anonime circostanziate (contenenti tutti gli elementi oggettivi necessari alla successiva fase di verifica) saranno prese in considerazione per approfondimenti.

4.7. Gestione delle Segnalazioni

Il Gestore, ricevuta la Segnalazione, rilascia alla persona Segnalante un avviso di ricevimento della Segnalazione entro 7 giorni dalla data di ricezione e provvederà alla successiva gestione della Segnalazione stessa o all'inoltro alla Società qualora ritenuta non di competenza, ma comunque di interesse per la Società.
Le Segnalazioni sono soggette al seguente *iter* istruttorio.

Vaglio di Procedibilità e di Ammissibilità
Ricevuta la Segnalazione, il Gestore compie un primo vaglio circa la procedibilità e l'ammissibilità della stessa valutando:

- che la Segnalazione rientri nel perimetro soggettivo ed oggettivo del D.lgs. 24/23;
- l'indicazione delle circostanze di tempo e luogo in cui si è verificato il fatto oggetto della Segnalazione, una descrizione dei fatti oggetto della Segnalazione e delle modalità con cui si è venuti a conoscenza dei fatti riportati;
- generalità o altri elementi che consentono di identificare il soggetto cui attribuire i fatti segnalati.

Laddove emergano o siano comunque desumibili elementi utili e sufficienti per ritenere fondata la Segnalazione, verrà avviata la successiva fase degli approfondimenti specifici.
Qualora a conclusione della fase di analisi preliminare emerga l'assenza di elementi sufficientemente circostanziati o l'infondatezza dei fatti richiamati, la Segnalazione sarà archiviata con le relative motivazioni, fatto salvo il riscontro all'interessato che dovrà essere fornito entro i termini previsti dal D.lgs. 24/23.

Istruttoria e approfondimenti specifici:
Una volta vagliata l'ammissibilità della Segnalazione, il Gestore provvederà a:

i. acquisire gli elementi informativi necessari alle valutazioni attraverso l'analisi della documentazione e delle informazioni ricevute;
ii. avviare le analisi specifiche avvalendosi, se opportuno, delle strutture competenti della Società o di esperti esterni;
iii. concordare con le funzioni interessate eventuali iniziative da intraprendere a tutela degli interessi della Società (ad es. iniziative giudiziarie, sospensione/cancellazione dall'albo fornitori etc.);
iv. richiedere l'avvio di un procedimento disciplinare nei confronti del Segnalante, nel caso di Segnalazioni in relazione alle quali siano accertate la malafede del Segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa Segnalazione;
v. alla conclusione dell'approfondimento svolto, sottoporre i risultati alla valutazione della Società affinché vengano intrapresi i più opportuni provvedimenti;

vi concludere l'istruttoria in qualunque momento se, nel corso dell'istruttoria medesima, sia accertata l'infondatezza della Segnalazione.

Le attività sopra descritte non sono necessariamente svolte in maniera sequenziale.

Qualora si renda necessario avvalersi dell'assistenza di professionisti terzi o del supporto specialistico del personale di altre funzioni aziendali ogni tipologia di dato che possa consentire l'identificazione del Segnalante o di altri soggetti coinvolti deve essere oscurata.

Tutte le fasi dell'attività di accertamento devono essere tracciate e archiviate correttamente.

Il trattamento dei dati personali delle persone coinvolte e/o citate nelle Segnalazioni nonché dei Segnalanti viene effettuato in conformità a quanto previsto dal D.lgs. n. 24/2023, dal Regolamento EU n. 679 del 27 aprile 2016 (GDPR), dal D.lgs. 196/2003 (Codice della Privacy) e dal D.lgs. 201/2018. Tali obblighi sono estesi anche ai soggetti interni diversi rispetto al Gestore coinvolti nella gestione della Segnalazione.

Riscontro al Segnalante

Il Gestore fornirà al segnalante un riscontro entro tre mesi dalla data di avviso di ricevimento o – in mancanza di tale avviso – entro tre mesi dalla data di scadenza del termine di sette giorni per tale avviso.

Il riscontro potrà avere ad oggetto:

- l'avvenuta archiviazione della Segnalazione, con espressa indicazione dei motivi;
- l'avvenuto accertamento della fondatezza della Segnalazione e la trasmissione agli organi competenti;
- l'attività svolta sino a questo momento e l'attività che si intende svolgere.

In quest'ultimo caso il Gestore comunicherà al Segnalante anche il successivo esito finale dell'istruttoria.

4.8. Conflitto di interessi

Qualora la Segnalazione dovesse riguardare uno dei Gestori, la stessa sarà gestita dai componenti che non si trovino in conflitto e, quindi, con esclusione di colui al quale la Segnalazione si riferisce.

4.9. Tutela e responsabilità del Segnalante

Il novero dei soggetti a cui è assicurata la tutela nel nuovo decreto ricomprende:

- lavoratori subordinati;
- lavoratori autonomi che svolgono la propria attività presso la Società;
- liberi professionisti e consulenti che prestano la propria attività presso la Società;
- volontari e tirocinanti, retribuiti e non, che prestano la propria attività presso i soggetti del settore privato;
- azionisti.

Per tutti i soggetti la tutela si applica anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico.

L'identità del Segnalante viene protetta in ogni contesto successivamente all'invio della Segnalazione attraverso i canali interni, ovvero successivamente a eventuali Segnalazioni esterne ovvero denunce di cui il Gestore delle Segnalazioni sia venuto a conoscenza.
Nell'ambito del procedimento disciplinare avviato nei confronti del Segnalato, l'identità del Segnalante può essere rivelata, previo consenso espresso del Segnalante, alla funzione competente allorquando la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla Segnalazione (effettuata attraverso i canali di Segnalazione ovvero mediante denuncia) e la conoscenza dell'identità del Segnalante risulti assolutamente indispensabile alla difesa del Segnalato. In tali ipotesi, è dato avviso al Segnalante, mediante comunicazione scritta, delle ragioni della rivelazione dei dati riservati.
Nel caso di avvio di procedimento di fronte alla Corte dei Conti nei confronti del Segnalato, l'identità del Segnalante non viene rivelata fino alla chiusura dell'istruttoria. Dopo questo termine l'identità del Segnalante può essere disvelata dall'autorità contabile per essere utilizzata nel procedimento.
Nell'ambito, invece, del procedimento penale avviato nei confronti del Segnalato, l'identità del Segnalante è coperta dal segreto d'ufficio fino alla chiusura delle indagini preliminari. Qualora l'autorità giudiziaria per esigenze istruttorie volesse conoscere il nominativo del Segnalante, la funzione aziendale competente provvede a comunicare l'identità dello stesso.
Qualora il Gestore delle Segnalazioni accerti la mala fede del Segnalante, la tutela della riservatezza viene meno e il Segnalato viene informato dell'identità del Segnalante, al fine di accordargli il diritto di sporgere querela per calunnia o diffamazione.

Nessuna ritorsione o discriminazione, diretta o indiretta, può derivare in capo a chi abbia in buona fede effettuato una Segnalazione. Per ritorsioni sono intesi:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso.

Inoltre, sono previste sanzioni nei confronti di chi viola le misure di tutela del Segnalante, così come sono previste sanzioni nei confronti del Segnalante, nel caso di Segnalazioni effettuate con dolo o colpa grave o che si dovessero rivelare false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare la Società, il Segnalato o altri soggetti interessati dalla Segnalazione.

La Società si riserva, in ogni caso, la facoltà di intraprendere le opportune iniziative anche in sede giudiziaria.
Le tutele sono estese anche:

- ai Facilitatori;
- alle persone del medesimo contesto lavorativo della persona Segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona Segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà della persona Segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

4.10. Tutela del Segnalato

La Segnalazione non è sufficiente ad avviare alcun procedimento disciplinare verso il Segnalato. Qualora, a seguito di concreti riscontri acquisiti riguardo alla Segnalazione, si decida di procedere con l'attività istruttoria, il Segnalato potrà essere contattato e gli verrà assicurata la possibilità di fornire ogni eventuale e necessario chiarimento.

4.11. Segnalazione esterna

Il canale di Segnalazione da utilizzare in via prioritaria è quello interno messo a disposizione dalla Società.
L'Autorità nazionale anticorruzione (ANAC) attiva un canale di **segnalazione esterna** che garantisca, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona Segnalante, della persona coinvolta e della persona menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione. La stessa riservatezza viene garantita anche quando la Segnalazione viene effettuata attraverso canali diversi da quelli indicati nel primo periodo o perviene a personale diverso da quello addetto al trattamento delle Segnalazioni, al quale viene in ogni caso trasmessa senza ritardo.
La persona Segnalante può effettuare una Segnalazione esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di Segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall'articolo 4 del Decreto;
b) la persona Segnalante ha già effettuato una Segnalazione interna ai sensi dell'articolo 4 e la stessa non ha avuto seguito;

c) la persona Segnalante ha fondati motivi di ritenere che, se effettuasse una Segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa Segnalazione possa determinare il rischio di ritorsione;
d) la persona Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le Segnalazioni esterne sono effettuate in forma scritta tramite la relativa piattaforma informatica predisposta dall'ANAC oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona Segnalante, mediante un incontro diretto fissato entro un termine ragionevole. Sul sito istituzionale dell'ANAC sono pubblicate tutte le informazioni necessarie per l'effettuazione della Segnalazione esterna, nonché le modalità di gestione della stessa.
In assenza dei presupposti sopra elencati il soggetto non beneficia delle tutele previste dal Decreto.

4.12. Denuncia all'Autorità Giudiziaria

Resta fermo che il Segnalante può liberamente rivolgersi alle autorità nazionali competenti, giudiziarie e contabili.

4.13. Riporto periodico

Nella relazione periodica prevista dai Modelli Organizzativi *ex* D.lgs. 231/01, l'OdV fornisce un riepilogo delle Segnalazioni pervenute, opportunamente anonimizzate.
Tale report contiene, per le segnalazioni di rilievo *ex* D.lgs. n. 231/01, gli esiti delle analisi.

4.14. Sanzioni

Sono previste sanzioni nei confronti di chi viola le misure di tutela del Segnalante, così come sono previste sanzioni nei confronti del Segnalante, nel caso di Segnalazioni effettuate con dolo o colpa grave o che si dovessero rivelare false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare la Società, il Segnalato o altri soggetti interessati dalla Segnalazione.
Fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie:

a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la Segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'articolo 12;
b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di Segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle Segnalazioni ovvero che l'adozione di tali procedure non è conforme a quelle di cui agli articoli 4 e 5, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle Segnalazioni ricevute;
c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3, salvo che la persona Segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.

La Società ha previsto, nel proprio sistema disciplinare adottato ai sensi dell'articolo 6, comma 2, lettera e), del decreto n. 231/2001, sanzioni nei confronti di coloro che accertano essere responsabili degli illeciti citati.

È, in ogni caso, garantito il diritto al contraddittorio.

4.15. Conservazione della documentazione e tutela della *privacy*

Al fine di garantire la gestione e la tracciabilità delle Segnalazioni e delle relative attività, il Gestore della Segnalazione cura l'archiviazione di tutta la documentazione di supporto della Segnalazione per un periodo di 5 anni dalla chiusura della Segnalazione.

Gli eventuali dati personali e sensibili contenuti nella Segnalazione, inclusi quelli relativi alla identità del Segnalante o di altri individui, verranno trattati nel rispetto delle norme per la protezione dei dati personali, quali quello di limitazione delle finalità e minimizzazione dei dati, e le Segnalazioni non possono essere utilizzate oltre quanto necessario per dare alle stesse adeguato seguito.

Il trattamento dei dati personali avviene nel rispetto dei seguenti principi:

- trattare i dati in modo lecito, corretto e trasparente;
- raccogliere i dati solo al fine di gestire e dare seguito alle Segnalazioni, divulgazioni pubbliche o denunce effettuate;
- garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In tal senso, i dati personali che manifestamente non sono utili al trattamento di una specifica Segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza indugio;
- assicurare che i dati siano esatti e, se necessario, aggiornati;
- conservare i dati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della specifica Segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di Segnalazione;
- effettuare il trattamento in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (ricorso a strumenti di crittografia);
- assicurare l'aggiornamento del registro delle attività di trattamento, integrandolo con le informazioni connesse a quelle di acquisizione e gestione delle Segnalazioni;
- garantire il divieto di tracciamento dei canali di Segnalazione;
- garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del Segnalante.

4.16. Aggiornamento della *policy*

La Policy e la funzionalità della Piattaforma saranno oggetto di revisione periodica a cura del Direttore Generale o dell'Amministratore Delegato della Società per garantirne il costante allineamento alla normativa di riferimento.

La Società terrà anche conto, ai fini di modifiche/integrazioni della presente Policy, di eventuali suggerimenti formulati dall'Organismo di Vigilanza.