

PROCEDURA IN MATERIA DI WHISTLEBLOWING

Indice

1. PREMESSA	2
2. RIFERIMENTI NORMATIVI	2
3. SCOPO DELLA PROCEDURA	3
4. DESTINATARI	3
5. DEFINIZIONI	3
6. OGGETTO DELLE SEGNALAZIONI	4
7. ESCLUSIONI	5
8. OBBLIGO DI AGIRE IN BUONA FEDE	6
9. MODALITÀ DI SEGNALAZIONE	7
9.1 Segnalazione interna	7
9.2 Segnalazione esterna	8
9.3 Divulgazione pubblica	9
9.4 Segnalazione anonima	9
10. CONTENUTO DELLA SEGNALAZIONE	9
11. GESTIONE DELLA SEGNALAZIONE	10
11.1 Ricezione della segnalazione	10
11.2 Avvio dell'istruttoria e valutazioni preliminari	10
11.3 Istruttoria: accertamento e indagini	11
11.4 Sospensione dei termini procedurali	11
11.5 Chiusura dell'istruttoria	12
11.6 Tracciamento delle attività e conservazione della documentazione	12
12. TUTELA DEL SEGNALANTE	13
12.1 Tutela della riservatezza del segnalante	13
12.2 Divieto di ritorsione e misure di protezione	15
13. SANZIONI DISCIPLINARI	16
14. NORMATIVA IN MATERIA DI DATA PROTECTION	16
15. AGGIORNAMENTO	18
16. FORMAZIONE	18

1. PREMESSA

La presente procedura è finalizzata a dare attuazione al Decreto Legislativo 10 marzo 2023 n. 24, pubblicato in G.U. in data 15.03.2023, recante il recepimento della Direttiva (Ue) 2019/1937, che riguarda la protezione delle persone che segnalano violazioni del diritto dell'Unione europea.

Tale disciplina, denominata “*Whistleblowing*”, tutela specifiche categorie di soggetti che segnalano informazioni, acquisite nel contesto lavorativo e/o professionale, relative a **violazioni di disposizioni normative nazionali o dell'Unione europea, in grado di ledere l'interesse pubblico o l'integrità di un determinato ente**, pubblico o privato.

È prevista l'istituzione di appositi **canali interni** all'ente per la trasmissione delle segnalazioni, che garantiscano la tutela della riservatezza dell'identità del segnalante, della persona coinvolta o menzionata nella segnalazione, del contenuto della segnalazione e della relativa documentazione.

È sempre possibile sporgere denuncia direttamente all'**Autorità giudiziaria**, ma è altresì prevista la facoltà di effettuare **segnalazioni esterne** tramite il canale gestito dall'Autorità Nazionale Anticorruzione (di seguito “ANAC”), nonché di effettuare **divulgazioni pubbliche** tramite la stampa o mezzi elettronici o di diffusione in grado di raggiungere un numero elevato di persone.

L'ANAC può anche irrogare **sanzioni amministrative pecuniarie** nei casi espressamente previsti dalle normative vigenti e comunque laddove non si ottemperi agli obblighi prescritti dalla disciplina su whistleblowing (v. l'articolo 21 del D.Lgs. n. 24/2023 cit., cui si rinvia).

2. RIFERIMENTI NORMATIVI

- D.Lgs. 30 giugno 2003 n. 196 s.m.i., “*Codice in materia di protezione dei dati personali*”;
- DPCM 6 novembre 2015 n. 5 s.m.i., “*Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva*”;
- Regolamento (Ue) 2016/679 sulla protezione dei dati personali o “*Regolamento Generale sulla Protezione dei Dati*” (di seguito “*RGPD*”);
- Direttiva (Ue) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
- D.Lgs. 10 marzo 2023 n. 24, “*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recanti disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*” (di seguito “*Decreto*”).

3. SCOPO DELLA PROCEDURA

Scopo della presente procedura è quello di disciplinare il processo di trasmissione, ricezione, analisi e gestione delle segnalazioni, compresa l'archiviazione e la successiva cancellazione sia delle segnalazioni, sia della documentazione ad esse riferita e/o pertinente.

4. DESTINATARI

Destinatari della presente procedura sono i seguenti soggetti che siano in possesso di informazioni sulle violazioni come meglio indicate nella procedura stessa:

- i vertici aziendali (organi apicali come dirigenti e quadri) e i componenti degli organi sociali di DATAMATIC S.P.A., con sede legale in Milano, Via Agordat 34, C.F. 01863990154, PEC datamaticspa@pec.it (di seguito, l'Azienda), anche laddove le funzioni siano di mero fatto;
- i dipendenti (a tempo determinato e indeterminato), gli ex dipendenti, i candidati a posizioni lavorative ovvero in trattativa o in fase di selezione, gli stagisti, i soggetti in prova, i soci e i clienti dell'Azienda;
- i partner, i fornitori (in regime di appalto o subappalto) i consulenti, gli agenti, i collaboratori, i somministrati nell'ambito dello svolgimento della propria attività lavorativa e/o professionale presso l'Azienda e tutti coloro che intrattengono, a diverso titolo, rapporti d'affari con l'Azienda.

Rientrano, altresì, tra i destinatari, i soggetti non ricompresi nelle precedenti categorie ma ai quali si applicano le misure di protezione previste dalla presente procedura.

Quanto previsto nel presente documento si applica anche alle segnalazioni "anonime", purché adeguatamente circostanziate.

5. DEFINIZIONI

La seguente tabella indica alcune definizioni particolarmente rilevanti in materia di *whistleblowing*:

Segnalazione	Comunicazione, scritta od orale, di informazioni su violazioni, compresi i fondati sospetti riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse in Azienda, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.
Segnalante	Persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni su violazioni acquisite nell'ambito del proprio contesto lavorativo e/o professionale.
Segnalato	Persona menzionata nella segnalazione ovvero nella divulgazione pubblica, intesa come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.

Tabella 1 – Definizioni rilevanti

6. OGGETTO DELLE SEGNALAZIONI

Per quel che concerne le violazioni, che possono formare oggetto delle segnalazioni, si precisa fin da subito che presso l'Azienda sono impiegati più di 50 e meno di 249 dipendenti, pertanto deve essere effettuato specifico riferimento alle seguenti disposizioni del Decreto:

- Art. 2, comma 1, lett. a), nn. 3), 4), 5) e 6);
- Art. 2, comma 1, lett. q);
- Art. 3, comma 2, lett. a);
- Allegato I al Decreto.

Ne consegue che gli illeciti, che possono costituire oggetto di segnalazione, riguardano le violazioni del diritto comunitario, in particolare:

Violazioni oggetto di segnalazione	Note
<p>Violazioni del diritto dell'UE – I ipotesi:</p> <ul style="list-style-type: none"> • Illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al d.lgs. n. 24/2023 e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato). 	<p>In particolare, si tratta di illeciti relativi ai seguenti settori: contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.</p>
<p>Violazioni del diritto dell'UE – II ipotesi:</p> <ul style="list-style-type: none"> • Atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE. 	<p>Tipici sono i casi di frodi, di corruzione o qualsiasi altra attività illegale connessa o collegata alle erogazioni o alle spese dell'Unione.</p>
<p>Violazioni del diritto dell'UE – III ipotesi:</p> <ul style="list-style-type: none"> • Atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). 	<p>Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi, il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società.</p>
<p>Violazioni del diritto dell'UE – IV ipotesi:</p> <ul style="list-style-type: none"> • Atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori sopra indicati. 	<p>Tipico è il caso di comportamenti contrari alla concorrenza o al libero mercato, come l'impresa che operi in regime di monopolio. Altro caso significativo e più frequente è quello dell'impresa che opera sul mercato in posizione dominante. La normativa comunitaria non impedisce a tale impresa di conquistare, in virtù di propri meriti e proprie capacità, una posizione rilevante sul mercato o su una fetta</p>

consistente di esso a scapito di eventuali concorrenti. Tuttavia, siffatta impresa potrebbe pregiudicare, col proprio comportamento, una concorrenza effettiva e leale nel mercato interno tramite il ricorso alle cosiddette pratiche "abusive" (per es. adozione di prezzi "predatori", sconti "target", vendite abbinate, etc.).

Tabella 2 – Oggetto delle segnalazioni

7. ESCLUSIONI

Sono anzitutto da ritenersi esclusi dalle segnalazioni tutti gli illeciti non espressamente ricompresi nella Tabella 2, di cui all'Articolo 6 della presente procedura.

Sono inoltre da ritenersi irrilevanti e, come tali, non procedibili e suscettibili di immediata archiviazione le segnalazioni indicate nella seguente tabella:

NON OGGETTO DI SEGNALAZIONE	NOTE
<p>Contestazioni, rivendicazioni o richieste legate a un interesse di carattere esclusivamente personale del segnalante oppure che attengono esclusivamente a propri rapporti individuali di lavoro o di impiego con le figure gerarchicamente sovraordinate e/o coi colleghi.</p>	<p>A titolo esemplificativo sono escluse:</p> <ul style="list-style-type: none"> • le segnalazioni riguardanti vertenze di lavoro, discriminazioni tra colleghi, conflitti interpersonali tra la persona segnalante e un altro lavoratore; • aventi toni ingiuriosi o contenenti offese personali o giudizi morali e volte a offendere o ledere l'onore e/o il decoro personale e/o professionale della persona o delle persone a cui i fatti segnalati sono riferiti; • aventi finalità puramente diffamatorie o calunniose; • aventi natura discriminatoria, in quanto riferite a orientamenti sessuali, religiosi, politici, sindacali o all'origine razziale o etnica del segnalato; • fondate su meri sospetti o voci inerenti fatti personali non costituenti illecito.
<p>Le segnalazioni di violazioni se già disciplinate in via obbligatoria dagli atti dell'UE o nazionali indicati nella parte II dell'Allegato al Decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al Decreto.</p>	<p>Il Decreto non si applica alle segnalazioni già disciplinate da direttive e regolamenti dell'UE e dalle disposizioni attuative dell'ordinamento italiano che già disciplinano apposite procedure di segnalazione, con particolare riferimento al settore bancario e dell'intermediazione finanziaria, nei quali è assicurata la protezione delle persone segnalanti con l'obbligo di attivare canali di segnalazione interna ed esterna e ponendo altresì il divieto esplicito di ritorsioni. Sono altresì escluse tutte le discipline speciali che regolano il <i>whistleblowing</i> in specifici settori, come quelli inerenti alla prevenzione del riciclaggio e del finanziamento del terrorismo, alla sicurezza dei trasporti e alla tutela dell'ambiente.</p>
<p>Le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti</p>	<p>In generale, essendo la sicurezza nazionale di esclusiva competenza degli Stati membri, la materia non è ricompresa nell'ambito di applicazione della direttiva (UE) 2019/1937 e, di conseguenza, nel Decreto.</p>

rientrano nel diritto derivato pertinente dell'Unione europea.	
Fatti o circostanze rientranti nell'applicazione di disposizioni nazionali o dell'UE in materia di informazioni classificate, segreto forense o medico e di segretezza delle deliberazioni degli organi giurisdizionali, ovvero rientranti nell'applicazione di disposizioni nazionali in materia di procedura penale, di autonomia e indipendenza della magistratura, delle disposizioni sulle funzioni e attribuzioni del Consiglio Superiore della Magistratura, in materia di difesa nazionale e di ordine e sicurezza pubblica, nonché in materia di esercizio e tutela del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati, di protezioni contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, di autonomia delle parti sociali e del loro diritto di stipulare accordi collettivi, nonché di repressione delle condotte antisindacali.	In particolare si richiamano tutte le disposizioni del Codice Penale in materia di tutela del segreto epistolare (articoli 616, 618, 619 e 620 del Codice Penale), del segreto documentale (articolo 621 del Codice Penale), del segreto professionale (articolo 622 del Codice Penale) e dei segreti scientifici o commerciali (articolo 623 del Codice Penale). Si richiamano altresì le disposizioni del Codice di Procedura Penale (per es. l'articolo 329 sull'obbligo del segreto istruttorio) e quelle dei Codici Deontologici come quello forense e medico.
Reclami commerciali.	Per i reclami di clienti e fornitori in materia di inadempimenti contrattuali e <i>similia</i> esistono procedure apposite attivate presso l'ufficio acquisti ovvero presso l'ufficio <i>marketing</i> .
Richieste di esercizio dei diritti in materia di protezione dei dati personali nei confronti dell'Azienda (v. gli articoli 12, 15, 16, 17, 18, 20, 21 e 22 del RGPD).	Per l'esercizio dei diritti in materia di protezione dei dati personali è stato predisposto specifico canale di comunicazione con il Responsabile della Protezione dei Dati dell'Azienda.
Segnalazioni generiche.	Sono comunque escluse tutte quelle comunicazioni che, sulla base della genericità dei contenuti, non consentono di compiere adeguate verifiche.

Tabella 3 - Esclusioni

8. OBBLIGO DI AGIRE IN BUONA FEDE

Il segnalante deve effettuare segnalazioni il più possibile circostanziate, che offrano il maggior numero di elementi utili a svolgere le dovute indagini e verifiche, nonché il conseguimento di adeguati riscontri.

Dopo aver effettuato una segnalazione, il segnalante che ravvisi la presenza di eventuali errori può darne immediata informazione attraverso lo stesso canale col quale la segnalazione è stata presentata.

Sono invece da ritenersi effettuate in **mala fede** le segnalazioni che, sulla base di elementi oggettivi, si dovessero rivelare volutamente futili, false o infondate, con contenuto diffamatorio o comunque aventi a oggetto informazioni deliberatamente errate o fuorvianti, al solo scopo di danneggiare l’Azienda, il segnalato o altri soggetti interessati dalla segnalazione. In tali casi, l’Azienda attuerà adeguate azioni nei confronti del segnalante, in particolare avvierà gli opportuni **procedimenti disciplinari** nel rispetto di quanto stabilito dai contratti collettivi o individuali di lavoro.

9. MODALITÀ DI SEGNALAZIONE

Le **modalità** di segnalazione sono specificate nei successivi paragrafi.

Si vuole però precisare fin da subito che resta ferma la possibilità di effettuare una denuncia all’Autorità giudiziaria e che l’Azienda è competente esclusivamente per il canale di segnalazione interno.

9.1 Segnalazione interna

Ai sensi dell’art. 4 del Decreto, l’Azienda si avvale della **piattaforma informatica “EQS Integrity Line”**.

La piattaforma è protetta da tecniche crittografiche¹ ed è in grado di registrare nel proprio *database* i dati essenziali delle segnalazioni (ivi inclusi data e *ticket* o numero di pratica) e della loro gestione (tracciata tramite *workflow*) e di assicurare l’archiviazione e la conservazione di tutta la documentazione allegata, prodotta o acquisita in origine e nel corso delle attività d’indagine e di analisi.

La gestione della segnalazione spetta a **soggetti interni all’Azienda**. Tali soggetti competenti per la gestione della segnalazione assumono la veste di “**gestori**” della segnalazione e riceveranno apposite **istruzioni** dall’Azienda non solo sul rispetto della normativa sul whistleblowing, ma anche per quel che concerne sia la tutela della riservatezza del segnalante, sia il rispetto della normativa vigente in materia di protezione dei dati personali, contenuta de RGPD. All’uopo si precisa che i gestori sono stati designati quali “*soggetti autorizzati al trattamento dei dati personali*” ai sensi dell’art. 29 del RGPD e dell’art. 2-*quaterdecies* del D.Lgs. 30.06.2003 n. 196 s.m.i., recante il “*Codice in materia di protezione dei dati personali*”.

¹ La piattaforma consente di trasmettere, anche in maniera anonima, sia una segnalazione propria, sia una segnalazione ricevuta da un terzo, previa presa visione della “*Informativa Privacy*”, raggiungibile tramite apposito link.

Tali soggetti garantiscono la loro assoluta indipendenza, imparzialità, integrità e professionalità.

È facoltà del segnalante richiedere per iscritto al gestore che sia fissato un **incontro diretto** col gestore medesimo oppure col proprio responsabile d'area oppure con la funzione "*Risorse Umane*" oppure col Collegio dei Sindaci, al fine di rappresentare le situazioni di illecito in **forma orale**. L'incontro dovrà essere fissato entro sette giorni dalla richiesta. Dell'incontro sarà redatto apposito verbale.

È diritto del segnalante verificare ed eventualmente integrare e/o modificare il verbale, che alla fine deve essere sottoscritto sia dal segnalante, che dal gestore ovvero dagli soggetti interpellati e/o richiesti dal segnalante stesso. Il verbale sarà quindi conservato con protocollo riservato, in busta chiusa riposta in armadi chiusi a chiave.

Nei casi di **trasmissione per errore** della segnalazione con canali diversi da quelli sopra indicati ovvero a soggetti diversi dai gestori, chiunque riceva la segnalazione deve:

- inoltrarla tempestivamente o, al massimo, entro sette giorni dal ricevimento al proprio responsabile d'area oppure alla funzione "*Risorse Umane*" oppure al Collegio dei Sindaci, avendo cura di trasmetterla con modalità riservate e quindi in originale, in busta chiusa e completa di eventuali allegati;
- fornire contestuale notizia dell'inoltro al segnalante, pur sempre in termini riservati;
- eliminare eventuali copie in formato cartaceo o digitale della segnalazione, essendo assolutamente vietato detenerle;
- astenersi dall'intraprendere qualsiasi iniziativa autonoma di analisi e/o approfondimento;
- tutelare la riservatezza dell'identità del segnalante, delle persone coinvolte e/o comunque menzionate nella segnalazione, del contenuto della segnalazione e della relativa documentazione.

La mancata comunicazione di una segnalazione ricevuta e la violazione dell'obbligo di riservatezza costituiscono una violazione della presente procedura e comportano l'adozione di provvedimenti disciplinari.

9.2 Segnalazione esterna

Il segnalante può presentare la propria segnalazione direttamente all'ANAC tramite il canale di segnalazione esterno, messo a disposizione dalla stessa all'URL **<https://www.anticorruzione.it/-/whistleblowing>**, nei seguenti casi:

- se la segnalazione interna, da lui trasmessa, non ha avuto seguito;
- se ha fondati motivi di ritenere che, ove effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;

- se ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

9.3 *Divulgazione pubblica*

Il segnalante può procedere tramite divulgazione pubblica nei seguenti casi:

- se ha già effettuato una segnalazione interna ed esterna senza aver avuto alcun riscontro;
- se ha fondato motivo di ritenere che, in ragione delle specifiche circostanze del caso concreto, la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito.

9.4 *Segnalazione anonima*

Sono da considerarsi **anonime** le segnalazioni prive di elementi che consentano di identificare il loro autore. Esse saranno prese in considerazione solo se adeguatamente circostanziate² e se rivestano il carattere dell'attualità. Pertanto i gestori devono preliminarmente valutare la gravità della violazione riportata e la credibilità dei fatti rappresentati, nonché verificare la veridicità della violazione da fonti attendibili. Ove tali presupposti non ricorrano, la segnalazione anonima sarà prontamente archiviata.

Si ricordi infine che anche il segnalante anonimo, successivamente identificato e al ricorrere dei relativi presupposti, gode delle tutele previste dalla vigente normativa in materia whistleblowing.

10. CONTENUTO DELLA SEGNALAZIONE

Le condotte illecite segnalate devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza “*in ragione del rapporto di lavoro*” e, quindi, ricomprendono certamente quanto si è appreso in virtù delle mansioni svolte e dell'ufficio, funzione o carica rivestiti, ma anche le notizie che sono state acquisite a causa o in occasione dello svolgimento delle proprie prestazioni lavorative e/o professionali (per es., nel caso di fornitori esterni la segnalazione deve riguardare fatti appresi o conosciuti a causa o in occasione dello svolgimento del rapporto di fornitura; lo stesso vale per i collaboratori, gli agenti, i consulenti, i procacciatori di affari, etc.).

Gli **elementi essenziali** della segnalazione sono indicati nella seguente tabella:

² La segnalazione può ritenersi circostanziata nel caso in cui le informazioni in essa contenute consentano, almeno in astratto, di far emergere fatti precisi e concordanti (per es. ove contengano elementi utili a identificare il soggetto che ha posto in essere i fatti segnalati, cause e finalità delle condotte, anomalie relative al sistema di controllo interno, documentazione a supporto, etc.) e siano relazionate a contesti determinati (per es. ove siano individuabili il luogo e il periodo temporale delle violazioni ovvero l'ambito aziendale, l'ufficio, la funzione o l'occasione in cui si siano verificate).

1	generalità del segnalante (sempre che la segnalazione non sia anonima)
2	chiara e quanto più possibile completa descrizione dei fatti oggetto di segnalazione
3	generalità dell'autore della violazione, se conosciute, o comunque ogni informazione e ogni indicazione utile per individuarne l'identità
4	eventuali altri soggetti che possono riferire ovvero testimoniare sui fatti
5	natura, contesto di riferimento e ogni dettaglio utile per descrivere l'oggetto della segnalazione
6	circostanze di tempo e di luogo, ove conosciute, relative all'oggetto della segnalazione
7	ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati

Tabella 4 – Contenuto della segnalazione

È necessario **allegare**, se disponibile, opportuna documentazione a sostegno della segnalazione come per es.: fotografie, registrazioni audio o video, copie o scansioni di documenti cartacei, copie o duplicati di documenti digitali, e-mail, etc.

11. GESTIONE DELLA SEGNALAZIONE

Le fasi della gestione della segnalazione sono diverse e articolate. Si parte da una fase meramente preliminare di ricezione della segnalazione fino a pervenire alla conclusione delle indagini. Ogni singola fase è documentata e oggetto di *report*.

Nei successivi paragrafi vengono analizzate le singole fasi.

11.1 Ricezione della segnalazione

Quale che sia lo strumento utilizzato per la segnalazione, il segnalante **entro sette giorni** dall'invio della segnalazione riceve un **messaggio** tramite la piattaforma informatica di presa in carico della pratica, cui sarà assegnato un *ticket* oppure numero di protocollo oppure un codice identificativo.

11.2 Avvio dell'istruttoria e valutazioni preliminari

Il termine per l'avvio dell'istruttoria è di **quindici giorni** lavorativi dalla **data di ricevimento della segnalazione**,

I gestori verificano preliminarmente la sussistenza dei **presupposti** giuridici e fattuali, nonché la pertinenza e la presenza di **elementi sufficienti** – e dunque **gravi, precisi e concordanti** – per potere approfondire la segnalazione.

In presenza di elementi sufficienti, i gestori aprono formalmente la fase di indagine e accertamento, cioè la **fase istruttoria** vera e propria. Viceversa in caso di segnalazione non rilevante oppure mancante di elementi sufficienti, si procede all'archiviazione.

11.3 Istruttoria: accertamento e indagini

Il gestore anzitutto cerca di individuare, analizzare e valutare gli elementi a conferma della fondatezza dei fatti segnalati, anche tramite **richiesta di integrazioni** al segnalante. **Chiarimenti** possono essere richiesti a eventuali altri soggetti coinvolti nella segnalazione con l'adozione delle necessarie cautele, a garanzia della riservatezza del segnalante e del segnalato, in particolare devono essere omessi tutti i riferimenti, dai quali sia possibile risalire alla loro identità.

Il gestore, ove necessario, può acquisire **atti e documenti** dai vari uffici dell'Azienda e può avvalersi anche dell'ausilio di soggetti o funzioni interne all'Azienda, ovvero del supporto di professionisti o consulenti legali e/o tecnici esterni, a seconda dell'oggetto della segnalazione, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante e del segnalato, *ut supra* specificato.

Il gestore assicura lo svolgimento dell'istruttoria in maniera equa e imparziale e deve fornire informazioni al segnalante sullo **stato di avanzamento** dell'istruttoria. Altresì il gestore, una volta completata l'istruttoria, deve informare ogni persona coinvolta nell'indagine in merito alle dichiarazioni rese e alle prove acquisite a suo carico ed è messo in condizione di poter replicare alle stesse.

Il gestore chiude la propria istruttoria entro sessanta giorni dalla data di avvio della stessa. L'esito dell'attività istruttoria è comunicato al segnalante al massimo entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Si ricordi infine che il gestore è tenuto a **rivelare l'identità** del segnalante esclusivamente, qualora vi sia in tal senso una specifica richiesta da parte dell'**Autorità giudiziaria**. Di tale circostanza il gestore dà **pronto avviso** al segnalante.

11.4 Sospensione dei termini procedurali

Tutti i termini in precedenza indicati (invio del messaggio di presa in carico, avvio dell'istruttoria, chiusura dell'istruttoria, riscontro finale al segnalante) sono **sospesi** in caso di eventuali richieste di informazioni o documentali al segnalante e/o ad altri soggetti.

I termini si intendono sospesi una sola volta per ogni fase del procedimento e ricominciano a decorrere dall'avvenuto ricevimento di quanto richiesto o, in difetto, dall'inutile decorrere del termine assegnato per provvedere.

Tenuto comunque conto delle eventuali sospensioni, il termine massimo per il riscontro finale al segnalante è di sei mesi.

11.5 Chiusura dell'istruttoria

Al momento della chiusura delle indagini si possono avere esiti diversi.

Anzitutto, nel caso di manifesta infondatezza della segnalazione, il gestore procede all'**archiviazione**.

La seguente tabella riassume i casi di archiviazione:

A-1	irilevanza giuridica della segnalazione (v. Tabella 3 al Paragrafo 7 della presente procedura)
A-2	assenza di elementi di fatto idonei a giustificare accertamenti
A-3	contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti
A-4	segnalazione di illeciti corredata da documentazione non appropriata o inconferente
A-5	mancaza degli elementi essenziali della segnalazione di illeciti (v. Tabella 4 al Paragrafo 10 della presente procedura)
A-6	segnalazioni reiterate da parte dello stesso soggetto su fatti già segnalati
A-7	segnalazione effettuata in mala fede (v. Paragrafo 8 della presente procedura)

Tabella 5 – Casi di archiviazione

La decisione in merito all'archiviazione è formalizzata in apposito verbale, contenente i motivi dell'archiviazione.

Inoltre, in caso di segnalazione effettuata in mala fede (laddove cioè vi siano, all'esito degli accertamenti, elementi oggettivi comprovanti la mancanza di buona fede), oltre all'archiviazione il gestore ne dà immediata comunicazione agli organi competenti ad avviare eventuali procedure disciplinari a carico del segnalante.

Se invece all'esito dell'attività istruttoria è accertata la fondatezza della segnalazione, è redatta una relazione riepilogativa delle verifiche effettuate e delle evidenze emerse, al fine di condividere con l'Azienda l'adozione di azioni sanzionatorie e/o la predisposizione di azioni correttive o di rimedio.

11.6 Tracciamento delle attività e conservazione della documentazione

Il gestore dovrà tracciare riservatamente l'attività istruttoria svolta, assicurando la conservazione delle segnalazioni e di tutta la correlata documentazione di supporto per il tempo strettamente necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione ai sensi dell'articolo 14, comma 1, del Decreto, avendo cura che i dati identificativi del segnalante siano conservati separatamente da ogni altro dato. Nel caso

in cui sia instaurato un **giudizio**, tale termine si prolunga fino alla definizione del giudizio stesso col passaggio in giudicato della decisione a esso inerente.

I documenti in formato elettronico devono essere conservati in un *repository* protetto da credenziali di autenticazione, conosciute solo dai gestori per la gestione della segnalazione.

I documenti cartacei sono archiviati presso un ufficio o archivio, prescelto dall’Azienda, che dovrà sempre essere chiuso a chiave e il cui accesso sarà consentito esclusivamente ai gestori della segnalazione ovvero al responsabile d’area, al personale dell’ufficio Risorse Umane e ai membri del Collegio dei Sindaci eventualmente coinvolti nella gestione della segnalazione.

12. TUTELA DEL SEGNALANTE

La tutela del segnalante è garantita nel caso in cui siano rispettate le indicazioni fornite dalla presente procedura. Non viene invece garantita alcuna protezione al segnalante nel caso in cui egli abbia concorso alla realizzazione della condotta illecita.

Le tutele accordate al segnalante sono estese anche:

- al facilitatore, da intendersi come la persona fisica che assiste il segnalante nel processo di segnalazione e che opera nel medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- alle persone del medesimo contesto lavorativo del segnalante con uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del segnalante che abbiano con questi un rapporto abituale e corrente;
- agli enti di proprietà del segnalante o per i quali il segnalante lavora, nonché agli enti che operano nel medesimo contesto lavorativo.

Nei successivi paragrafi vengono approfonditi taluni aspetti della tutela del segnalante.

12.1 Tutela della riservatezza del segnalante

I gestori, il responsabile d’area e l’ufficio Risorse Umane garantiscono sempre la riservatezza dell’identità del segnalante, del segnalato e di eventuali altre persone coinvolte, nonché del contenuto della segnalazione e della relativa documentazione. Nella piattaforma informatica sono stati implementati strumenti di **crittografia** e l’accesso alla stessa è consentito solo a gestori appositamente autorizzati e muniti di credenziali di autenticazione, consistenti in *password* con requisiti di lunghezza e complessità sufficientemente elevati (lunghezza minima di otto caratteri e obbligo di usare almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere “*unicode*” o speciale).

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

È assolutamente vietato rivelare a persone diverse dai soggetti competenti a ricevere o a dare seguito alle segnalazioni ed espressamente autorizzate a trattare tali dati, l'identità del segnalante o qualsiasi altra informazione da cui essa possa evincersi, direttamente o indirettamente, salvo che il segnalante stesso non abbia espresso il proprio espresso consenso.

Nell'ambito di un **procedimento disciplinare**, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa del soggetto segnalato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del segnalante alla rivelazione della propria identità e solo dopo che questi sia stato informato per iscritto sulle ragioni che rendono necessaria la rivelazione di dati riservati.

Nell'ambito del **procedimento penale**, l'identità della persona segnalante è coperta dal segreto ai sensi dell'articolo 329 del Codice di Procedura Penale, che prescrive l'obbligo del segreto sugli atti compiuti nelle indagini preliminari *“fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari”*.

I diritti dell'interessato, di cui agli articoli da 15 a 22 del RGPD e riferiti a persone diverse dal segnalante, possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. n. 196/2003 cit., al fine di non compromettere la riservatezza del segnalante;

Il fascicolo della segnalazione è sottratto al diritto di accesso ai documenti amministrativi, previsto dall'art. 22 e seguenti della L. 241/1990, nonché al cosiddetto “accesso civico”, previsto dall'art. 5 e seguenti del D.Lgs. 33/2013.

La violazione della riservatezza dell'identità del segnalante è fonte di responsabilità disciplinare.

La tutela del segnalante viene meno nelle ipotesi indicate nella tabella seguente:

→	accertata responsabilità penale del segnalante (anche con sentenza di primo grado) per i reati di calunnia o diffamazione o comunque per reati commessi con la segnalazione
→	accertata responsabilità civile , per lo stesso titolo, nei casi di dolo o colpa grave. L'accertamento della responsabilità penale o civile del segnalante avviene esclusivamente a livello giudiziario

Tabella 6 – Cessazione della tutela del segnalante

12.2 Divieto di ritorsione e misure di protezione

L'Azienda non tollera e anzi combatte ogni genere di minaccia, ritorsione, sanzione non motivata o discriminazione nei confronti del segnalante, del segnalato e di chi abbia collaborato alle attività di riscontro riguardo alla fondatezza della segnalazione.

L'adozione di misure discriminatorie o ritorsive nei confronti del segnalante potrà dare origine a **procedimenti disciplinari** nei confronti del responsabile

Resta ferma la possibilità per il segnalante (e anche per le organizzazioni sindacali) di comunicare all'ANAC le ritorsioni che ritiene di aver subito nell'ambito del proprio contesto lavorativo (v. art. 19, comma 1, del Decreto).

A titolo esemplificativo e non esaustivo costituiscono esempi di misure ritorsive:

- le sanzioni disciplinari, anche solo pecuniarie, e misure equivalenti (licenziamento, sospensione, retrocessione di grado, mancata promozione, mutamento di mansioni, trasferimento, riduzione dello stipendio, restrizioni all'accesso ai corsi di formazione aziendali, note di demerito, referenze negative);
- coercizioni, intimidazioni, molestie, ostracismo;
- discriminazioni o trattamenti sfavorevoli;
- mancata conversione di un contratto a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse maturato un legittimo affidamento a tale conversione;
- mancato rinnovo o risoluzione anticipata di un contratto a termine;
- i danni alla reputazione della persona, in particolare sui *social media* ovvero i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e/o la perdita di redditi;
- la risoluzione anticipata di un contratto di fornitura;
- la revoca di una licenza o di un permesso.

In sede giudiziale gli **atti ritorsivi** adottati sono dichiarati **nulli** e, in caso di **licenziamento** a motivo della segnalazione, denuncia o divulgazione, il segnalante ha diritto alla **reintegrazione** nel posto di lavoro, salvo il diritto al **risarcimento dei danni**.

Nell'ambito di procedimenti giudiziari ovvero anche in controversie stragiudiziali aventi a oggetto misure ritorsive, è onere dell'Azienda provare che le misure ritorsive

sono motivate da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia. Ciò non vale per i soggetti diversi dal segnalante (per es. facilitatori o colleghi), che dovranno dimostrare che le misure sono state poste in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all’Autorità giudiziaria.

13. SANZIONI DISCIPLINARI

Nel rispetto delle leggi e dei contratti, collettivi o individuali, vigenti, possono essere applicate **sanzioni** disciplinari **effettive, proporzionate e dissuasive**:

- nei confronti del segnalato, se le segnalazioni risultano fondate;
- nei confronti del segnalante, se sono effettuate segnalazioni in mala fede;
- nei confronti del soggetto competente, se sono violati i principi di tutela previsti dalla procedura ovvero se sono state ostacolate o si è tentato di ostacolare le segnalazioni.

14. NORMATIVA IN MATERIA DI DATA PROTECTION

La normativa in materia di whistleblowing implica varie attività di trattamento dei dati personali e, per l’effetto, tali attività devono essere effettuate nel rispetto del RGPD e del D.Lgs. n. 196/2003 cit.

L’Azienda assume la qualità di “*Titolare del trattamento*” e i trattamenti effettuati in tale qualità sono considerati necessari in relazione alla specifica tipologia di dati trattati e per specifiche finalità come indicati nella seguente tabella:

Tipologia di dati	Base giuridica
Dati comuni e identificativi	<ul style="list-style-type: none"> • adempimento di un obbligo legale, cui è soggetto il Titolare (articolo 6, paragrafo 1, lett. c), del RGPD) • esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (articolo 6, paragrafo 1, lett. e), del RGPD) • interesse legittimo del Titolare (art. 6, paragrafo 1, lett. f), del RGPD), ove sia necessario per i Titolare difendere un proprio diritto in ogni sede (giudiziale e stragiudiziale)
Categorie particolari di dati³	<ul style="list-style-type: none"> • adempimento di un obbligo legale, cui è soggetto il Titolare (articolo 9, paragrafo 2, lett. b), del RGPD) • esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (articolo 9, paragrafo 2, lett. g), del RGPD) • necessità di accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali (art. 9, paragrafo 2, lett. f), del RGPD)
Dati relativi a condanne penali, reati e connesse misure di sicurezza	<ul style="list-style-type: none"> • trattamento consentito soltanto sotto il controllo dell'autorità pubblica o se autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati (articolo 10 del RGPD)

Tabella 7 – Tipologia di dati trattati e finalità del trattamento

I dati personali non utili e non necessari al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

L'Azienda fornisce a tutti gli interessati coinvolti nella disciplina del whistleblowing e a quelli che rientrano nell'ambito applicativo della presente procedura apposita **informativa** sul trattamento dei dati personali ai sensi degli articoli 13 e 14 del RGPD.

L'Azienda ha designato il Responsabile esterno ai sensi dell'art. 28 del RGPD e ha provveduto alla **nomina per iscritto** dei soggetti autorizzati al trattamento dei dati, dettando agli stessi le necessarie istruzioni (v. Paragrafo 9.1 della presente procedura).

In conformità alla normativa di riferimento, l'Azienda predispone e mantiene aggiornate, sentito il Responsabile della Protezione dei Dati, idonee misure tecniche e organizzative anche con riguardo ai profili di sicurezza, da richiamarsi nel **Registro dei trattamenti**.

Inoltre, ai sensi di quanto previsto dall'articolo 13, comma 2, del Decreto i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

³ Ai sensi dell'articolo 9, paragrafo 1, del RGPD sono definiti "dati particolari" i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Restano ferme le responsabilità disciplinari previste per violazione degli appositi doveri di comportamento e per violazione delle norme sulla tutela della riservatezza del segnalante e di tutti i soggetti coinvolti nella segnalazione.

15. AGGIORNAMENTO

L'Azienda riesamina su base periodica la presente procedura, per garantirne i necessari e opportuni aggiornamenti rispetto alla normativa di riferimento, adeguando altresì le procedure e le prassi interne.

16. FORMAZIONE

La procedura è pubblicata tramite caricamento nel sito web aziendale.

L'Azienda organizza su base annuale corsi di formazione in merito alla presente procedura in modo da assicurare la più ampia conoscenza della disciplina vigente in materia di whistleblowing, del funzionamento e dell'accesso ai canali e agli strumenti messi a disposizione per effettuare segnalazioni e infine delle responsabilità e dei provvedimenti applicabili in caso di violazioni segnalate e accertate.

----- *fine documento* -----