Gestione delle segnalazioni

Whistleblowing

Procedura di sicurezza PRS_99

Redazione, Variazioni, e Approvazioni

Redazione

Autore:
Data di creazione: 08/08/2023
Ultimo aggiornamento:
Codice:
Versione: 1.0
Stato:

Variazioni

Data	Autore	Versione	Variazione
08/08/2023	BERTI FABIO	1.0	CREAZIONE DOCUMENTO INIZIALE

Approvazioni

Nome	Funzione	Data	Firma

Indice dei contenuti

INTRODUZIONE

1 SCOPO E CAMPO DI APPLICAZIONE

1.1 OBIETTIVO

Lo scopo di questa procedura è di assicurare che It.City gestisca in modo conforme alla normativa di riferimento le segnalazioni di *whistleblowing* rientranti nell'ambito oggettivo di cui al D.Lgs. n. 24 del 10 marzo 2023 che ha attuato la Direttiva (UE) 2019/1937 riguardante "*la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*".

1.2 AMBITO DI APPLICAZIONE

Questo documento si applica al responsabile anticorruzione e trasparenza (RPCT) e riguarda la gestione delle segnalazioni di comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica.
La Società rispetta - e tutti i Dipendenti e i Terzi sono tenuti a rispettare - tutte le leggi e le normative internazionali, nazionali e locali applicabili.

Il presente Documento si applica a tutta la Società, è onere della stessa darne corretta diffusione e comunicazione sia interna che esterna. A tal proposito, la Procedura è pubblicata sul sito web, alla sezione Società Trasparente / *whistleblowing.*
La Procedura è stata adottata con determina dall'Amministratore Unico numero 73 del 30.09.2023.

2 RIFERIMENTI

- Direttiva (UE) 2019/1937 del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione
- Decreto Legislativo n. 24 del 10 marzo 2023 attuazione della direttiva (UE) 2019/1937 del 23 ottobre 2019
- Decreto Legislativo n. 196 del 30 giugno 2003 Codice in materia di protezione dei dati personali" e successivi provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali e normative successive o particolari.
- Decreto Legislativo n. 101 del 10 agosto 2018 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679
- Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.
- Decreto Legislativo n. 231 dell'8 giugno 2001 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
- Modello di Organizzazione, Gestione e Controllo ex D. lgs. 231/2001 della Società IT.City S.p.A. a socio unico

3 DEFINIZIONI

Software as a Service (SaaS): Il modello SaaS offre una soluzione software completa acquistabile con pagamento da un provider di servizi cloud, gli utenti si connettono all'app tramite Internet, in genere con un Web browser.

4 DISPOSIZIONI GENERALI

il 30 marzo 2023 è entrato in vigore il decreto legislativo n. 24/2023, che introduce la nuova disciplina del *whistleblowing* in Italia. In data 15/07/2023 It.City ha adottato una soluzione cloud (SaaS) che prevede la

condivisione di un unico link che, all'interno della stessa landing page, consente al segnalante di indicare la Società partecipata del Comune di Parma nei cui confronti procedere con la segnalazione.
La piattaforma adottata per segnalare eventuali condotte illecite in violazione di disposizioni europee e nazionali precisate dal D.Lgs. 24/2023 è raggiungibile selezionando il link "*Whistleblowing*" sul portale aziendale: www.itcity.it.

5 RUOLI E RESPONSABILITÀ

Segnalate
è la persona che segnala, divulga ovvero denuncia all'Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato.

Istruttore
Figura preposta per la gestione della segnalazione e della definizione dell'istruttoria: RPCT.

Custode delle identità
Responsabile dell'autorizzazione per l'accesso ai dati identificativi dei segnalanti.

6 IL DECRETO LEGISLATIVO N. 24 DEL 10 MARZO 2023

6.1 COSA PUÒ ESSERE SEGNALATO

Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti 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;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

Ai sensi del D. Lgs. n. 24 del 2023, le disposizioni regolamentari non si applicano:

- alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate;
- alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali;
- alle 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 rientrino nel diritto derivato pertinente dell'Unione europea.

6.2 CHI PUÒ SEGNALARE

Sono legittimate a segnalare le persone che operano nel contesto lavorativo di un soggetto del settore pubblico o privato, in qualità di:

- dipendenti pubblici;
- lavoratori subordinati di soggetti del settore privato;
- lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
- collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del

settore pubblico o del settore privato;
- volontari e i tirocinanti, retribuiti e non retribuiti,
- azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato;
- colui che lavora sotto la supervisione e direzione di appaltatori, subappaltatori e fornitori.

La normativa estende, altresì, la tutela anche ai:
- facilitatori[1];
- ai colleghi di lavoro che abbiano con il segnalante un rapporto abituale o ricorrente;
- alle persone del medesimo contesto lavorativo del segnalante legate da uno stabile legame affettivo o di parentela entro il quarto grado;
- agli enti di proprietà del segnalante, o presso i quali lavorano.

6.3 QUANDO SI PUÒ SEGNALARE

- quando il rapporto giuridico è in corso;
- durante il periodo di prova;
- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso.

6.4 PROTEZIONE DELLA RISERVATEZZA DEI SEGNALANTI

- L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
- La protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- La segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;
- La protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

Nessuna ritorsione è consentita ai segnalanti. In particolare, costituiscono ritorsioni le seguenti fattispecie:
- 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;
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

[1]Coloro che assistono il Segnalante nel processo di segnalazione ed operano all'interno del medesimo contesto lavorativo.

I segnalanti possono comunicare all'ANAC eventuali ritorsioni che ritenessero di aver subito.

L'Autorità giudiziaria adita adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela della situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta posta in essere e la dichiarazione di nullità degli atti adottati in violazione delle disposizioni di cui al D. Lgs. n. 24/2023.

Si precisa, altresì, che al fine di acquisire elementi istruttori indispensabili all'accertamento delle ritorsioni, l'ANAC può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato della funzione pubblica e dell'Ispettorato Nazionale del Lavoro.

Infine, presso il sito istituzionale di ANAC è istituito l'elenco degli Enti del Terzo Settore che offrono misure di sostegno al segnalante.

6.5 TUTELA DEL SEGNALATO

La normativa di riferimento di cui al D.Lgs. 24/2023 prevede espressamente che la tutela dell'identità sia garantita anche alla persona fisica segnalata, ovvero alla persona alla quale la violazione è attribuita nella divulgazione pubblica (c.d. persona coinvolta).
Pertanto, si adottano particolari cautele al fine di evitare la indebita circolazione di informazioni personali, non solo verso l'esterno, ma anche al suo interno.

6.6 PROTEZIONE DEI DATI PERSONALI

- Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni è effettuato dai soggetti del settore pubblico e privato, nonché da ANAC, in qualità di titolari del trattamento, nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte nelle segnalazioni, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.
- Inoltre, i diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.
- Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui al D. Lgs. n. 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e) sempre in riferimento al D. Lgs. n. 24/2023, del regolamento (UE) 2016/679[2] e art. 3, comma 1, lettera e) del decreto legislativo n. 51 del 2018.[3]

6.7 NON PUNIBILITÀ

Non è punibile chi riveli o diffonda informazioni sulle violazioni: coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero se, al momento della segnalazione, denuncia o divulgazione, avesse ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.

6.8 PERDITA DELLE TUTELE

Le tutele non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
[3] Principi applicabili al trattamento dei dati personali ai sensi del D. Lgs. 18 maggio 2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

casi di dolo o colpa grave; in tali casi alla persona segnalante o denunciante può essere irrogata una sanzione disciplinare.

7 PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI

- ❖ Dare avviso alla persona segnalante del ricevimento della segnalazione entro **sette (7) giorni** dalla data del suo ricevimento;
- ❖ Mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni;
- ❖ Dare diligente seguito alle segnalazioni ricevute;
- ❖ Svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;
- ❖ Dare riscontro alla persona segnalante entro **3 mesi** o, se ricorrono giustificate e motivate ragioni, **6 mesi** dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei 7 giorni dal ricevimento;
- ❖ Comunicare alla persona segnalante l'esito finale della segnalazione.

7.1 AMBITO SOGGETTIVO E OGGETTIVO

La direttiva UE estende il concetto di *whistleblower* (soggetti ai quali si estende la tutela prevista dalla normativa): "*segnalanti che lavorano nel settore privato o pubblico che hanno acquisito informazioni sulle violazioni in un contesto lavorativo*" indipendentemente dalla sussistenza di un rapporto di lavoro diretto.

In quest'ottica il presente documento deve intendersi rivolto alle seguenti categorie di lavoratori:

- dipendenti di It.City S.p.A.;
- collaboratori e consulenti esterni;
- dipendenti e collaboratori delle imprese che svolgono lavori o forniscono beni e servizi in favore di It.City S.p.A.;
- coloro che segnalano o divulgano informazioni acquisite nell'ambito di un rapporto di lavoro con It.City S.p.A. nel frattempo terminato;
- coloro che, in mancanza di un rapporto di lavoro in essere, segnalino informazioni acquisite durante il processo di selezione o in altre fasi delle trattative precontrattuali avviate da It.City S.p.A.

I contenuti della segnalazione possono riguardare la commissione delle violazioni, sopra individuate, o la realizzazione di comportamenti ritorsivi nei confronti dei *whistleblowers*.

7.2 CONDIZIONI DI PROTEZIONE E SEGNALAZIONI ANONIME

Alla luce del quadro normativo attualmente vigente, la segnalazione maturata nel contesto lavorativo di It.City S.p.A., che risulti finalizzata all'emersione di illeciti, comporta:

1. il divieto di adottare misure discriminatorie o ritorsive nei confronti del *whistleblower*;
2. l'attivazione di misure idonee a tutela della sua riservatezza da parte del RPCT che riceve la segnalazione.

Il regime di tutela delineato dal legislatore viene assicurato dal RPCT ogniqualvolta il segnalante abbia fondati motivi di ritenere veri i fatti oggetto di comunicazione ed ha utilizzato uno dei canali previsti dalla normativa.
Nel corso dell'istruttoria, inoltre, il RPCT è tenuto ad osservare il segreto d'ufficio.
Con riguardo, invece, alle segnalazioni anonime, saranno prese in carico anche le comunicazioni non sottoscritte, che risultino manifestamente fondate e dalle quali emergano elementi utili per la ricostruzione e l'accertamento di illeciti a vario titolo rilevanti.

7.3 PROCEDURA INTERNA

Le fasi della procedura interna sono le seguenti.

7.3.1 FASE DELL'INIZIATIVA

I canali per la trasmissione della segnalazione sono:

- la piattaforma informatica all'uopo già adottata;
- l'incontro diretto con il RPCT, a seguito del quale verrà redatto un apposito verbale sottoscritto dal segnalante e custodito nel rispetto della normativa da parte del RPCT.

La piattaforma è accessibile attraverso apposito link rapido "*whistleblowing*" pubblicato sul sito https://itcity.it.

La piattaforma consente di compilare, inviare e ricevere in modo informatizzato il "Modulo di segnalazione". A seguito dell'inoltro della segnalazione, l'autore riceve dal sistema un codice identificativo utile per i successivi accessi. Il segnalante può monitorare lo stato di avanzamento dell'istruttoria accedendo al sistema di gestione delle segnalazioni ed utilizzando il codice identificativo ricevuto.

Qualora la segnalazione interna sia presentata ad un soggetto diverso da quello individuato (ad esempio ad altro dirigente o funzionario in luogo del RPCT), laddove il segnalante dichiari espressamente di voler beneficiare delle tutele in materia di whistleblowing o tale volontà sia desumibile, la segnalazione è considerata "segnalazione *whistleblowing*" e va trasmessa, entro 7 giorni dal suo ricevimento, al RCPT, dando contestuale notizia della trasmissione alla persona segnalante. Diversamente, se il segnalante non dichiari espressamente di voler beneficiare delle sue tutele o detta volontà non sia desumibile dalla segnalazione, essa è considerata quale segnalazione ordinaria.

Si precisa, comunque, che una segnalazione presentata ad un soggetto non competente può essere considerata di *whistleblowing* anche nel caso in cui la volontà di avvalersi delle tutele si desuma da comportamenti concludenti (per esempio dall'utilizzo di una modulistica apposita per le segnalazioni di *whistleblowing*).

7.3.2 FASE DELL'ISTRUTTORIA

Entro 7 giorni dell'assegnazione il RPCT invia al segnalante un avviso di ricevimento e prende in carico la segnalazione per avviare l'istruttoria, da effettuare entro tre mesi dalla data di trasmissione dell'avviso.

Il RPCT analizza la segnalazione al fine di determinarne l'ammissibilità e la fondatezza e, se quanto denunciato non è stato adeguatamente circostanziato, richiede chiarimenti al segnalante mediante l'applicativo informatico.

Una delle prime verifiche che occorre effettuare è se il segnalante rivesta, o meno, la qualifica di dipendente di It.City S.p.A., ovvero se rientri nell'ambito soggettivo individuato dalla normativa di riferimento.

A. Nel caso in cui si rilevi un'evidente e manifesta infondatezza, inammissibilità o irricevibilità si procede ad archiviare la segnalazione. Nello specifico, costituiscono possibili causali di archiviazione:
    - manifesta incompetenza del RPCT sulle questioni segnalate;
    - contenuto generico della segnalazione/comunicazione o tale da non consentire nessun approfondimento;
    - segnalazioni aventi ad oggetto i medesimi fatti trattati in procedimenti già definiti;
    - ambito oggettivo non appartenente alla normativa di riferimento.

B. Nell'ipotesi in cui non ricorra alcuno dei casi di archiviazione sopra riportati il RPCT provvede a verificare la segnalazione ricevuta, anche acquisendo ogni elemento utile alla valutazione della fattispecie, avendo cura di adottare misure idonee ad assicurare la riservatezza dell'identità del segnalante laddove gli approfondimenti richiedano il necessario coinvolgimento di soggetti terzi. Ciò anche attraverso:
    - richiesta di notizie, informazioni, atti e documenti ad altri uffici di It.City S.p.A.;
    - richiesta di chiarimenti, documentazione e informazioni ulteriori al segnalante e/o a eventuali altri soggetti terzi coinvolti nella segnalazione;
    - audizione del *Whistleblower*, ove possibile.

Successivamente procede all'analisi della documentazione e degli elementi ricevuti e a deliberare sul *fumus* di quanto rappresentato nella segnalazione (ciò in quanto il RPCT non accerta i fatti, ma svolge un'attività di

verifica e di *reporting* all'Amministratore Unico della Società).

7.3.3 FASE DECISORIA

Qualora venga rilevata una delle cause di archiviazione sopra elencate, il RPCT provvede a:

A. archiviare la segnalazione con adeguata motivazione. La stessa verrà, quindi, inserita e conservata all'interno dell'applicativo informatico e sarà oggetto di rendicontazione nell'ambito della Relazione finale di monitoraggio ai sensi dell'art. 1, c. 14, della |. n. 190/2012;
B. comunicare al segnalante l'archiviazione e la relativa motivazione mediante il sistema informatico, o mediante incontro diretto, a seguito del quale verrà redatto un apposito verbale sottoscritto dal segnalante e custodito nel rispetto della normativa.

In caso, invece, di accertamento della fondatezza della segnalazione, il RPCT provvede a redigere una relazione contenente le risultanze dell'istruttoria condotta ed eventuali e possibili profili di illiceità riscontrati.

Per garantire la gestione e la tracciabilità delle attività svolte il RPCT assicura la conservazione all'interno del sistema delle segnalazioni e di tutta la correlata documentazione di supporto per un periodo di cinque anni dalla ricezione, assicurando che i dati identificativi del segnalante siano conservati separatamente da ogni altro dato.
Il Titolare del trattamento dei dati (come definito dall'art. 4, Regolamento UE 2016/679) è il RPCT.

7.3.4 MODALITÀ DI GESTIONE DELLE SEGNALAZIONI OGGETTI

Modalità di conservazione dei dati	Le modalità si differenziano a seconda che la segnalazione, e la correlata documentazione, sia pervenuta: ➢ tramite sistema informatico (piattaforma) ➢ tramite incontro diretto (*)
Politiche di tutela della riservatezza	Nel caso di gestione del procedimento attraverso il sistema informatico: la piattaforma utilizza un protocollo di crittografia che garantisce una tutela rafforzata della riservatezza dell'identità del segnalante, del contenuto della segnalazione e della documentazione ivi allegata, nonché dei soggetti coinvolti. Nel caso di segnalazione pervenuta attraverso incontro diretto la segnalazione e la documentazione pervenuta sono inserite nella piattaforma informatica da parte del RPCT. Piattaforma informatica: il contenuto della segnalazione insieme alla documentazione allegata, in un data base, al quale può accedere soltanto il personale autenticato (RPCT). In prima battuta solo il RPCT può visualizzare l'elenco delle segnalazioni e delle comunicazioni acquisite dal sistema non ancora esaminate. Per lo svolgimento dell'istruttoria, l'RPCT può avviare un dialogo con il *whistleblower*, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, sempre tramite il canale a ciò dedicato nelle piattaforme informatiche o anche di persona. Ove necessario, può anche acquisire atti e documenti da altri uffici dell'amministrazione, avvalersi del loro supporto,

	coinvolgere terze persone tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante e del segnalato. L'amministratore del sistema informatico, invece, è colui che provvede alla conduzione applicativa della piattaforma e non accede ai dati del segnalante né alle pratiche presenti nel sistema.
Tempo di conservazione (durata di conservazione di dati e documenti)	cinque anni, a decorrere dalla data della comunicazione dell'esito finale del processo di Segnalazione, nel rispetto degli obblighi di riservatezza a norma di legge.
Tempistica di svolgimento del procedimento *whistleblowing*	Termini: • sette giorni per l'invio dell'avviso di ricevimento; • tre mesi per la gestione dell'istruttoria e la contestuale comunicazione al Segnalante.
Responsabilità relative alla sicurezza informatica delle informazioni	Funzionari amministratori del sistema: sono specifici dipendenti o tecnici di società LASER ROMAE, nominati singolarmente, che devono agire nel rispetto di quanto disposto dal provvedimento del 27 novembre 2008 recante le "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".
Titolarità relative al trattamento dei dati	Nel corso del procedimento titolare del trattamento dei dati (come definito dall'art. 4, Regolamento UE 2016/679) è il RPCT.

Incontro diretto con il Segnalante

Il Segnalante ha facoltà di poter richiedere un incontro diretto con il Gestore della Segnalazione entro un termine ragionevole al fine di poter circostanziare ed argomentare l'oggetto della segnalazione inviata.

Il Gestore provvederà a fissare un incontro con il Segnalante entro massimo 15 giorni a far data dalla richiesta di quest'ultimo.

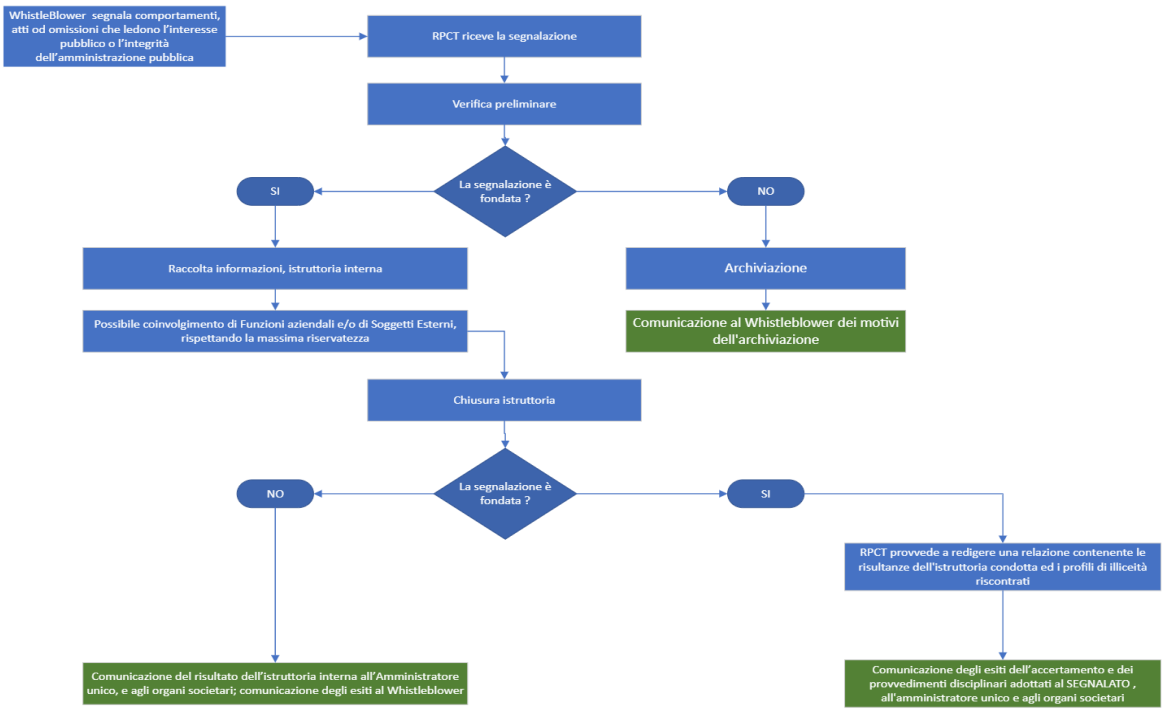
L'incontro con il Segnalante dovrà avvenire in locali aziendali idonei a mantenere la massima riservatezza del Segnalante. Il Gestore ha facoltà di indicare eventualmente fasce orarie adeguate per programmare gli incontri con il Segnalante al fine di garantire la riservatezza di quest'ultimo.

Il Gestore potrà provvedere alla registrazione dell'incontro previo consenso del Segnalante mediante idonei dispositivi alla conservazione e all'ascolto.

Nel caso in cui il Segnalante non presti il proprio consenso alla registrazione o nel caso in cui il Gestore non sia in possesso di strumenti adatti alla registrazione, quest'ultimo dovrà provvedere alla redazione di un verbale che il Segnalante dovrà sottoscrivere. Una copia dello stesso verbale dovrà essere consegnata allo stesso Segnalante.

Tutta la documentazione e le registrazioni degli incontri viene conservata ed archiviata in armadi chiudibili a chiave e accessibili solo ed esclusivamente da parte del Gestore della segnalazione.

7.3.5 FLUSSO OPERATIVO - WORKFLOW



7.3.6 TUTELA DELLA RISERVATEZZA E DIRITTO DI ACCESSO

Tutta la procedura mira ad assicurare la separazione tra i contenuti della segnalazione e gli elementi che consentono di risalire all'identità del *whistleblower*.
Ai fine di garantire la massima tutela della riservatezza, l'accesso alla documentazione è consentito al solo RPCT.
Diversamente, nel caso in cui il RPCT trasmetta gli atti all'Organo per i procedimenti disciplinari, la procedura è subordinata ad una specifica richiesta del secondo il quale rappresenti che la conoscenza dell'identità del segnalante è indispensabile per la difesa dell'incolpato. In tal caso il RPCT, dopo aver verificato che la contestazione risulta fondata, in tutto o in parte, sulla segnalazione, provvederà ad acquisire, attraverso la piattaforma informatica o altro canale con il quale è stata inviata la comunicazione, nel rispetto della normativa, il consenso del segnalante a rivelare l'identità mediante una dichiarazione sottoscritta da quest'ultimo (a cui dovrà essere allegato idoneo documento attestante l'identità del dichiarante).
La procedura attraverso l'accesso agli atti, invece, è regolata dal combinato disposto del comma 4 dell'art. 54 bis del d.lgs. n. 165/2001 e all'accesso ai documenti amministrativi ai sensi della legge 241/1990.
Il divieto di rilevare l'identità del segnalante è da riferirsi non solo al nominativo del segnalante, ma anche a tutti gli elementi della segnalazione nella misura in cui il loro disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante.

8 MISURE SANZIONATORIE

La divulgazione non autorizzata dell'identità del segnalante, del segnalato o di altro soggetto meritevole di tutela (o di informazioni da cui si possa dedurre la loro identità), sarà considerata una violazione della presente Procedura e saranno applicate le sanzioni previste contro coloro che vìolano le misure di protezione. Qualsiasi azione volta a diffondere illegalmente la loro identità è considerata una violazione della presente Procedura ed è soggetta ai relativi procedimenti disciplinari e potrebbe essere sanzionata dalle Autorità competenti.

Ciò premesso, l'ANAC è l'Autorità competente a comminare le seguenti sanzioni amministrative pecuniarie, ai sensi del D. Lgs. 24/2023:

- da € 10.000,00 a € 50.000,00, nel caso in cui fossero state commesse ritorsioni, ovvero ostacolo alla segnalazione o ancora violazione in merito all'obbligo di riservatezza;
- da € 10.000,00 a 50.000,00, nel caso in cui non siano stati istituiti idonei canali di segnalazione, ovvero

le relative procedure, o ancora qualora non fosse stata svolta l'attività di verifica e analisi in merito alle segnalazioni ricevute;

- da € 500,00 a 2.500,00, nel caso di perdita delle tutele, 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.

9 IL SISTEMA DI SEGNALAZIONE ESTERNO

Il segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione, ricorra una delle seguenti condizioni, ai sensi del D. Lgs. 24/2023:

- 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 alle disposizioni di cui al D. Lgs. n. 24/2023;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- 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;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Come già precisato, il segnalante può, altresì, avvalersi del sistema di segnalazione esterno ove sussistesse un conflitto di interesse nei confronti del gestore delle segnalazioni.
L'ANAC ha attivo 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.

10 DIVULGAZIONE PUBBLICA

Il segnalante che effettua una divulgazione pubblica, beneficia della protezione prevista dal D. Lgs. 24/2023 qualora ricorra una delle seguenti condizioni:

- Il segnalante ha previamente effettuato una segnalazione interna ed esterna, ovvero ha effettuato direttamente una segnalazione esterna, alla quale non è stato dato riscontro nei termini di legge in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- Il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- Il segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.