Procedura per la Gestione delle Segnalazioni
ex Decreto Legislativo10 marzo 2023 n. 24
e successive modifiche

SIPPIC S.p.A.

Revisione	Data approvazione	Firma (Amministratore)
0	15/12/2023	
1		
2		
3		
4		
5		
6		
7		
8		

SOMMARIO

PREMESSA

Sippic S.p.A., nel perseguimento dei propri obiettivi di *business* è, da sempre, sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e si impegna a contrastare condotte illecite, sia attraverso la diffusione e la promozione di valori e principi etici, sia mediante l'effettiva attuazione di regole di condotta e processi di controllo, in linea con i requisiti fissati dalle normative applicabili e con le migliori prassi di riferimento. Per tale ragione la Società ha adottato, e mantiene costantemente aggiornati, un Modello 231 nonché un Codice Etico.

Al fine di rafforzare il proprio sistema organizzativo e di buon governo (oltre che al fine di adempiere agli obblighi normativi specificatamente vigenti in materia), SIPPIC S.p.A. promuove e incentiva le segnalazioni di illeciti e/o fatti, anche solo potenzialmente, contrari al diritto della UE, alla Legge e alle normative interne aziendali da parte di chiunque, nell'ambito delle attività lavorative svolte presso la Società, ne abbia conoscenza.

La presente procedura ha, dunque, lo scopo di disciplinare il processo di ricezione e gestione delle segnalazioni pervenute attraverso i canali di seguito indicati, nonché di definire le tutele e le misure di protezione poste a tutela dei Segnalanti.

In conformità a quanto previsto dal D. Lgs. 24/2023, i canali di segnalazione interna descritti nella presente procedura nonché le modalità di funzionamento degli stessi sono stati comunicati alle organizzazioni sindacali.

RIFERIMENTI NORMATIVI

La Procedura è finalizzata ad attuare il Decreto Legislativo n. 24 del 10 marzo 2023 - "*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 recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*" – oltre che all'articolo 6 del D.Lgs. 231/2001

Ogni trattamento di dati personali viene effettuato in conformità al Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – "GDPR") e al D. Lgs. 30 giugno 2003, n. 196 (Codice della Privacy).

La presente Procedura è stata redatta ispirandosi, oltre che al dettato normativo, alle Linee guida "*... in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne*", approvate da ANAC con Delibera n. 311 del 12 luglio 2023.

DEFINIZIONI

Ai fini della corretta comprensione della Procedura di gestione delle segnalazioni è necessario definire il significato attribuito a termini qui utilizzati:

- **Segnalazione**: comunicazione, scritta od orale, avente ad oggetto potenziali violazioni di informazioni sulle violazioni effettuata tramite canali di segnalazione interni o esterni.
- **Segnalazione *Whistleblowing***: si tratta di segnalazione di violazioni che consistono in comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente privato richiamate dall'art. 2, comma 1, lett. a) del D. Lgs. 24/2023.
- **Segnalazione Ordinaria**: segnalazione che non rientra nel perimetro delle Segnalazioni *Whistleblowing* per l'ambito oggettivo o soggettivo, cioè le segnalazioni

inerenti a temi diversi da quelli specificati al par. 4 o pervenute da soggetti diversi da quelli indicati al par. 5 della Procedura o che presentino uno dei requisiti di esclusione previsti dal D. Lgs. 24/2023 o per le quali il Segnalante non abbia dichiarato la propria identità o non abbia dichiarato di voler beneficiare della riservatezza della sua identità e di avvalersi delle tutele previste dal D. Lgs. 24/2023.

• **Segnalazione interna**: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite i canali di segnalazione istituiti dalla Società.

• **Segnalazione esterna**: la comunicazione, scritta od orale, delle informazioni sulle Violazioni presentata tramite il canale di segnalazione esterna attivato da ANAC ai sensi dell'art. 7 del D. Lgs. n. 24/2023. La Segnalazione esterna non può riguardare le violazioni del D. Lgs. 231/2001 a meno che non possano rientrare in una violazione per cui è ammessa la segnalazione esterna (ad esempio, violazione degli interessi finanziari dell'unione europea).

• **Divulgazione pubblica**: rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone. La Divulgazione pubblica non può riguardare le violazioni del D. Lgs. 231/2001 a meno che non possano rientrare in una violazione per cui è ammessa la segnalazione esterna (ad esempio, violazione degli interessi finanziari dell'unione europea).

• **ANAC**: Autorità Nazionale Anticorruzione.

• **Contesto lavorativo**: le attività lavorative o professionali, presenti o passate, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile;

• **Segnalante o *Whistleblower***: la persona fisica che effettua la Segnalazione o la Divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.

• **Segnalato**: soggetto che, all'interno della Segnalazione, viene individuato quale responsabile dell'illecito o della violazione oggetto di Segnalazione.

• **Persona coinvolta**: la persona fisica o giuridica menzionata nella Segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.

• **Facilitatore**: la persona fisica che assiste il Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata. LG ANAC prevedono espressamente che "*... il termine "assistenza" fa riferimento a un soggetto che fornisce consulenza o sostegno al Segnalante e che opera nel medesimo contesto lavorativo del Segnalante. A titolo esemplificativo, il facilitatore potrebbe essere il collega dell'ufficio del Segnalante o di un altro ufficio che lo assiste in via riservata nel processo di segnalazione. Il facilitatore potrebbe essere un collega che riveste anche la qualifica di sindacalista se assiste il Segnalante in suo nome, senza spendere la sigla sindacale. Si precisa che se, invece, assiste il Segnalante utilizzando la sigla sindacale, lo stesso non riveste il ruolo di facilitatore. In tal caso resta ferma l'applicazione delle disposizioni in tema di consultazione dei rappresentanti sindacali e di repressione delle condotte antisindacali ...*";

Persone del medesimo contesto lavorativo: secondo le LG ANAC l'espressione

persone del medesimo contesto lavorativo si riferisce a persone legate da una rete di relazioni sorte in ragione del fatto che esse operano o hanno operato in passato, nel medesimo ambiente lavorativo del Segnalante o denunciante, ad esempio ex colleghi, collaboratori ecc...

Colleghi di lavoro: secondo le LG ANAC "... *Nel caso di colleghi di lavoro, il legislatore ha previsto che si tratti di coloro che, al momento della segnalazione, lavorano con il Segnalante (esclusi quindi gli ex colleghi) e che abbiano con quest'ultimo un rapporto abituale e corrente. La norma si riferisce, quindi, a rapporti che non siano meramente sporadici, occasionali, episodici ed eccezionali ma attuali, protratti nel tempo, connotati da una certa continuità tali da determinare un rapporto di "comunanza", di amicizia ...*".

Enti di proprietà del Segnalante, denunciante o di effettua una divulgazione pubblica, le LG ANAC hanno precisato che "... *si ritiene che tale concetto possa intendersi in senso ampio ricomprendendo quindi sia i casi in cui un soggetto è titolare di un ente in via esclusiva, sia in compartecipazione maggioritaria con terzi ...*".

• **Gestore della segnalazione o Gestore**: la persona, l'ufficio interno autonomo ovvero il soggetto esterno, cui è affidata la gestione del canale di segnalazione interna. Il Gestore della segnalazione è specificamente formato per la gestione del canale.

• **Piattaforma**: Piattaforma web accessibile all'indirizzo che consente di effettuare le Segnalazioni scritte in modo sicuro grazie alla crittografia e alla non accessibilità da parte di soggetti diversi dai Gestori della segnalazione.

• **Riscontro**: comunicazione al Segnalante di informazioni relative al seguito che viene dato o che si intende dare alla Segnalazione.

Seguito: azione intrapresa dal soggetto cui è affidata la gestione della segnalazione per valutare la sussistenza dei fatti, l'esito delle indagini e le eventuali misure adottate.

• **Ritorsione**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare al Segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

I) I SOGGETTI DESTINATARI DELLA TUTELA NORMATIVA

I.1.) LE PERSONE SEGNALANTI

Le Persone che, nel settore privato, godono delle tutele previste dal Decreto 24/2023 devono individuarsi ne:

1) i lavoratori subordinati di SIPPIC, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96;

2) i lavoratori autonomi, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81, nonché' i titolari di un rapporto di collaborazione di cui all'articolo 409 del codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015, che svolgono la propria attività lavorativa presso SIPPIC;

3) i liberi professionisti e i consulenti che prestano la propria attività presso SIPPIC;

4) i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso SIPPIC S.p.A.

5) le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso SIPPIC S.p.A.
La tutela delle persone segnalanti si applica anche qualora la segnalazione, la denuncia all'Autorità giudiziaria o contabile o la divulgazione pubblica di informazioni avvenga:
a) quando il rapporto giuridico di cui al comma 3 dell'articolo 3 D.Lgs. 24/2023 non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
b) durante il periodo di prova;
c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

I.2.) I SOGGETTI CHE GODONO DELLA PROTEZIONE NORMATIVA DIVERSI DAI SEGNALANTI

Ai sensi dell'articolo 3, comma 5 D.Lgs. 24/2023 le misure di protezione di cui al capo III della norma, si applicano anche:
1) ai facilitatori;
2) 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;
3) 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;
4) 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".

II) AMBITO OGGETTIVO DELLE SEGNALAZIONI *WHISTLEBLOWING*

II.1.) DEFINIZIONE ED OGGETTO DI SEGNALAZIONE *WHISTLEBLOWING*

Le segnalazioni sono definite come le informazioni, compresi i fondati sospetti, su violazioni già commesse o non ancora commesse (ma che, sulla base di elementi concreti come irregolarità o anomalie, potrebbero esserlo), nonché su condotte volte ad occultarle (es. occultamento o distruzione di prove).
Le informazioni sulle violazioni devono riguardare comportamenti, atti od omissioni di cui il Segnalante, o il denunciante, sia venuto a conoscenza **nel proprio contesto lavorativo.**
Secondo le LG ANAC "*...a rilevare è l'esistenza di una relazione qualificata tra il Segnalante ed il soggetto, pubblico o provato, nel quale il primo opera, relazione che riguarda attività lavorative o professionali presenti o anche passate ...*".
Dal punto di vista oggettivo la nuova disciplina si applica alle violazioni delle disposizioni normative nazionali e dell'UE che ledono l'integrità di SIPPIC S.p.A. commesse nell'ambito dell'organizzazione di SIPPIC S.p.A. con cui il Segnalante o il denunciate intrattiene uno dei rapporti giuridici qualificati presi in considerazione dal Legislatore.

Sono escluse dall'ambito di applicazione della nuova disciplina le segnalazioni:
1) legate a un **interesse personale del Segnalante**, che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse pubblico o dell'integrità dell'ente privato o dell'amministrazione pubblica, posto che la nuova disciplina mira a tutelare l'integrità dell'ente persona giuridica e a ricomprendere "... *tutte quelle situazioni in cui si vanifica l'oggetto o le finalità delle attività poste in essere nel settore pubblico e privato per la piena realizzazione delle finalità pubbliche, che ne deviino gli scopi o che ne minino il corretto agire...*".
Le contestazioni escluse in quanto legate a un interesse personale del Segnalante non sono considerate segnalazioni *whistleblowing* e, quindi, potranno essere trattate come segnalazioni **ordinarie**.
2) in materia di **sicurezza e difesa nazionale**;
3) relative a **violazioni già regolamentate** in via obbligatoria in alcuni settori speciali, alle quali continua dunque ad applicarsi la disciplina di segnalazione *ad hoc* (servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente).
Resta poi ferma la normativa in materia di: *i)* informazioni classificate; *ii)* segreto medico e forense; *iii)* segretezza delle deliberazioni degli organi giurisdizionali; *iv)* norme di procedura penale sull'obbligo di segretezza delle indagini; *v)* disposizioni sull'autonomia e indipendenza della magistratura; *vi)* difesa nazione e di ordine e sicurezza pubblica; *vii)* nonché di esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati.

II.2.) TIPOLOGIE DI ILLECITI RILEVANTI AI FINI DI UNA SEGNALAZIONE *WHISTLEBLOWING* E CANALI DI SEGNALAZIONE

Secondo l'articolo 3, comma 2 lettera b) D. Lgs. 24/2023 la novella si applica:
A) alle informazioni sulle violazioni della normativa nazionale nei limiti delle condotte illecite rilevanti ai sensi del decreto legislativo 231/01 o violazioni del Modello di SIPPIC S.p.A. Il canale di segnalazione è esclusivamente **INTERNO**
B) alle informazioni sulle violazioni aventi ad oggetto la violazione del diritto UE e della normativa nazionale di recepimento. Si tratta di:
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea indicati nell'allegato A1 al Decreto Legislativo 24/2023 ovvero degli atti nazionali che ne danno attuazione, anche se questi ultimi non sono espressamente elencati nel citato allegato. In particolare, si tratta di illeciti riguardanti i 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 (di cui all'articolo 325 del Trattato sul Funzionamento dell'Unione Europea) come individuati nel diritto derivato (regolamenti, direttive, decisioni, raccomandazioni e pareri) dell'Unione europea;

- atti od omissioni riguardanti il mercato interno che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (articolo 26, paragrafo 2, del Trattato sul Funzionamento dell'Unione Europea), Sono comprese le violazioni delle norme dell'Unione in materia di concorrenza e di aiuti di Stato, nonché' le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o 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;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati ai punti precedenti.
Per le informazioni relative alle violazioni sub B) il canale di segnalazione è **INTERNO, ESTERNO, LA DIVULGAZIONE PUBBLICA, LE DENUNCE ALLE AUTORITÀ GIUDIZIARIA O CONTABILE.**

II.3.) CONTENUTO DELLE SEGNALAZIONI

Quanto al **contenuto**, le segnalazioni devono essere il più possibile **circostanziate**, al fine di consentire la valutazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni.
Ai fini del vaglio di **ammissibilità** della segnalazione, è necessario che risultino chiari i seguenti elementi essenziali:

- i **dati identificativi** della persona Segnalante (nome, cognome, luogo e data di nascita), nonché un recapito a cui comunicare i successivi aggiornamenti;
- le **circostanze di tempo e di luogo** in cui si è verificato il fatto oggetto della segnalazione e, quindi, una descrizione dei fatti oggetto della segnalazione, specificando i dettagli relativi alle notizie circostanziali e ove presenti anche le modalità con cui si è venuto a conoscenza dei fatti oggetto della segnalazione;
- le **generalità** o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Si anticipa (cfr. *infra* **II.7.**) che i dati identificativi della persona Segnalante ed il recapito a cui comunicare i successivi aggiornamenti sono elementi essenziali affinché la segnalazione venga considerata e gestita come *whistleblowing*
È utile anche che alla segnalazione vengano allegati documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.
Tutto ciò premesso, la segnalazione può essere ritenuta **inammissibile** per:

1) mancanza di dati che costituiscono gli elementi essenziali della segnalazione;
2) manifesta infondatezza degli elementi di fatto riconducibili alle violazioni tipizzate dal Legislatore;
3) esposizione di fatti di contenuto generico tali da non consentire la comprensione al Gestore della segnalazione;
4) produzione di sola documentazione senza la segnalazione vera e propria di violazioni.

Il Segnalante deve specificare che si tratta di una segnalazione *whistleblowing*, per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni; in caso di mancata specificazione, la segnalazione verrà considerata ordinaria.

II.4.) IRRILEVANZA DEI MOTIVI PERSONALI DEL SEGNALANTE O DENUNCIANTE.

Secondo LG ANAC i motivi che hanno indotto una persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della trattazione della segnalazione e della protezione da misure ritorsive.

II.5.) LE SEGNALAZIONI ANONIME

Nel caso di ricezione di **segnalazioni anonime,** anche alla luce delle indicazioni dell'ANAC, si specifica che le stesse, qualora risultino puntuali, circostanziate e supportate da idonea documentazione, possono essere equiparate da SIPPIC S.p.A. alle **segnalazioni ordinarie** e, in quanto tali, possono essere trattate in conformità ai regolamenti interni, laddove eventualmente implementati.

In ogni caso, le segnalazioni anonime verranno registrate dal Gestore della segnalazione e la documentazione ricevuta dovrà essere conservata. Infatti, il Decreto 24/2023 prevede che laddove il Segnalante anonimo venga successivamente identificato e abbia subito ritorsioni, allo stesso debbano essere garantite le tutele previste per il *whistleblower*.

II.6.) I CANALI INTERNI DI SIPPIC

SIPPIC S.p.A. ha istituito due canali interni di segnalazione utilizzabili in maniera alternativa.

1) **Canale di segnalazione in forma scritta**: Piattaforma TEAMSYSTEM WHISTLEBLOWING

Il canale scritto, dotato di misure di sicurezza tecniche adeguate agli standard di cui all'art. 32 GDPR, risiede su server – situato nell'Unione Europea – di un soggetto terzo e prevede un percorso guidato per il Segnalante che consentirà allo stesso di inserire le informazioni necessarie per la ricostruzione e valutazione dei fatti e l'utilizzo di misure di crittografia, che garantiscono la riservatezza non solo del Segnalante, ma anche del facilitatore, della persona coinvolta o comunque menzionata nella segnalazione nonché del contenuto della segnalazione e della documentazione.

Con particolare riferimento al canale di segnalazione in forma scritta, SIPPIC S.p.A. ha adottato la piattaforma di segnalazione raggiungibile tramite il seguente link:**//sippicspa.smartleaks.cloud/#/**

che inoltrerà automaticamente l'invio della segnalazione al Gestore della segnalazione (cfr. *infra* par. **II.6.1**), unico soggetto titolato ad accedere alla piattaforma e prendere visione delle segnalazioni.

In caso di utilizzo della piattaforma, il Segnalante dovrà rispondere ad alcune domande, aperte e chiuse, che permetteranno al Gestore di approfondire l'oggetto della stessa oltre che, se correttamente compilate, di rispettare i requisiti richiesti dalla legge per le segnalazioni *whistleblowing*.

La piattaforma consente anche di effettuare l'*upload* della documentazione che il Segnalante ritiene opportuno portare all'attenzione del Gestore a supporto della propria segnalazione. Lo strumento consente, inoltre, l'interazione mediante messaggistica interna alla piattaforma, tra il Segnalante e il Gestore, al fine di approfondire i temi oggetto di comunicazione o integrare/rettificare le informazioni precedentemente rese.

La Piattaforma consente, altresì, al Segnalante di essere sempre aggiornato sullo stato della segnalazione trasmessa e di ottenerne il riscontro.

Al termine della procedura di segnalazione la Piattaforma, infatti, fornirà al Segnalante un codice di 16 cifre che permetterà allo stesso di accedere al sistema e, pertanto, alla propria segnalazione per:
• monitorarne lo stato di avanzamento;
• integrare la propria segnalazione con ulteriori elementi fattuali o altra documentazione;
• avere un contatto diretto con il Gestore avviando anche un eventuale scambio di richieste e informazioni;
• ottenere il riscontro dal Gestore.
La perdita del codice non ha effetti sulla segnalazione, che sarà comunque processata nei tempi e nei modi stabiliti dalla presente procedura.
La disponibilità del codice è essenziale per poter accedere in qualsiasi istante alla propria segnalazione, al fine di monitorare lo stato di avanzamento, per fornire informazioni ulteriori rispetto a quanto già segnalato e prendere conoscenza del Riscontro. In mancanza dello stesso, tali operazioni non saranno disponibili. In tali casi, per motivi di riservatezza a tutela del Segnalante, il codice correlato a ciascuna segnalazione non potrà essere recuperato in alcun modo.
Ove si ritenga opportuno fornire nuove informazioni di cui si è avuta conoscenza o conoscere gli esiti dell'istruttoria, è comunque possibile aprire una nuova segnalazione.

1) **Canale di segnalazione in forma orale**: Piattaforma TEAMSYSTEM WHISTLEBLOWING

Il canale orale assicura, anche attraverso forme di crittografia, la riservatezza della identità del Segnalante e delle persone coinvolte (es. facilitatore, segnalato, eventuali terzi comunque menzionati nella segnalazione) del contenuto della segnalazione e della documentazione ad essa relativa.
Previo consenso del Segnalante alla registrazione, il Gestore della segnalazione conserva la segnalazione all'interno di un dispositivo idoneo alla conservazione ed all'ascolto.
I canali interni sono progettati in modo da consentire un accesso selettivo alle segnalazioni solo da parte del personale autorizzato.

II.6.1.) IL GESTORE DELLA SEGNALAZIONE

Con separato atto SIPPIC S.p.A. ha nominato l'organo collegiale (di seguito indicato come "*il Gestore*") dedito alla gestione delle segnalazioni e dotato di autonomia, indipendenza e competenze tecniche adeguate nella gestione delle segnalazioni.
Il Gestore è autorizzato, altresì, si sensi dell'articolo 28 Reg. Ue 679/2016 (anche GDPR) e 2-*quaterdecies* D.Lgs.196/2003.
La nomina prevede specifiche istruzioni per il corretto trattamento dei dati personali di cui alla segnalazione.
La presenza dell'OdV tra i componenti il Gestore rende superflua la predisposizione dei flussi informativi diretti all'Organismo di Vigilanza (cfr. infra **par. VI**).
Laddove il Gestore versi in una ipotesi di conflitto di interessi rispetto ad una specifica segnalazione (in quanto, ad esempio, uno o più componenti sono soggetti segnalati) si ritiene che ricorra una delle condizioni per effettuare una segnalazione esterna ad ANAC, non potendo essere assicurato che alla segnalazione sia dato efficace seguito.

II.6.2.) LA SEGNALAZIONE INVIATA AD UN SOGGETTO NON COMPETENTE

Qualora la segnalazione interna sia presentata a un **soggetto diverso** da quello individuato ed autorizzato da SIPPIC S.p.A. e sia evidente che si tratti di segnalazione *whistleblowing* (es. esplicitata la dicitura "*whistleblowing*" sulla busta, nell'oggetto o nel testo della comunicazione ovvero tale volontà sia desumibile dalla segnalazione), la segnalazione va considerata "*whistleblowing*". In questo caso, sarà onere del soggetto ricevente:

1) trattare le informazioni di cui ha avuto conoscenza con modalità idonee a garantirne la piena riservatezza;
2) trasmettere la segnalazione al Gestore senza ritardo e, comunque, non oltre 7 giorni dal suo ricevimento, senza trattenerne copia;
3) contestualmente, dare notizia della trasmissione al Segnalante;

II.7.) LA GESTIONE DELLA SEGNALAZIONE

FASE I-RICEZIONE DELLA SEGNALAZIONE

Ricezione della segnalazione: entro 7 giorni dalla presentazione della segnalazione, il Gestore rilascia al Segnalante l'avviso di ricevimento della segnalazione. Tale riscontro non implica alcuna valutazione dei contenuti oggetto della segnalazione ma è unicamente volto a informare il Segnalante dell'avvenuta corretta ricezione della stessa.
L'avviso dev'essere inoltrato al recapito indicato dal Segnalante nella segnalazione; in assenza di tale indicazione e, dunque, in assenza della possibilità di interagire con il Segnalante per i seguiti, la segnalazione non verrà gestita ai sensi della disciplina *whistleblowing* (lasciando traccia di tale motivazione) bensì, eventualmente, trattata come ordinaria

FASE II- ESAME PRELIMINARE

La procedibilità della segnalazione: per poter dare corso al procedimento, il Gestore della segnalazione dovrà, preliminarmente, verificare:

1) che il Segnalante sia un soggetto legittimato ad effettuare la segnalazione;
2) che l'oggetto della segnalazione rientri tra gli ambiti di applicazione della disciplina.

Nel caso in cui la segnalazione riguardi una materia esclusa dall'ambito oggettivo di applicazione, la stessa verrà trattata come ordinaria, dandone comunicazione al Segnalante.

L'ammissibilità della segnalazione

Nel caso in cui l'esame preliminare, si concluda con una valutazione di improcedibilità o inammissibilità (cfr. supra II.3.), il Gestore della segnalazione procederà alla **archiviazione** garantendo, comunque, la tracciabilità delle motivazioni a supporto.
Una volta verificata, invece, la procedibilità e la ammissibilità della segnalazione, il Gestore avvia la **FASE ISTRUTTORIA**

FASE III-ISTRUTTORIA

L'obiettivo della fase di accertamento è di procedere con le verifiche, analisi e valutazioni specifiche circa la fondatezza o meno dei fatti segnalati, anche al fine di formulare eventuali raccomandazioni in merito all'adozione delle necessarie azioni correttive sulle aree e sui processi aziendali interessati nell'ottica di rafforzare il sistema di controllo interno.
Il Gestore della segnalazione assicura lo svolgimento delle necessarie verifiche; a titolo

meramente esemplificativo il Gestore può avviare un dialogo con il *whistleblower*, chiedendogli chiarimenti, documenti ed informazioni ulteriori, sempre tramite il canale a ciò dedicato nelle piattaforme informatiche o anche di persona. Altresì, può acquisire atti e documenti da altre strutture aziendali, avvalersi del loro supporto, coinvolgere terze persone tramite audizioni o altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza prevista dalla norma.
In particolare, ove risulti necessario avvalersi dell'assistenza tecnica di professionisti terzi, nonché del supporto specialistico del personale di altre funzioni/direzioni aziendali è necessario - al fine di garantire gli obblighi di riservatezza richiesti dalla normativa - oscurare ogni tipologia di dato che possa consentire l'identificazione della persona Segnalante o di ogni altra persona coinvolta (si pensi, ad esempio, al facilitatore o ulteriori persone menzionate all'interno della segnalazione).
Nel caso in cui sia necessario il coinvolgimento di soggetti interni diversi dal Gestore (per esempio altre funzioni aziendali), anche ad essi andranno estesi gli obblighi di riservatezza espressamente previsti nella Procedura "*whistleblowing*" e nel Modello 231 di SIPPIC S.p.A. e, espressamente, sanzionati dal Sistema Disciplinare interno adottato da SIPPIC S.p.A.
Qualora i dati identificativi del Segnalante, o delle altre persone coinvolte, siano necessari all'indagine condotta da soggetti esterni (eventualmente coinvolti dal Gestore), i doveri di riservatezza e confidenzialità previsti dal Decreto in capo al Gestore saranno estesi anche a tali soggetti esterni mediante specifiche clausole contrattuali da inserire negli accordi stipulati con il soggetto esterno. Inoltre, in entrambi i casi, andranno assicurate le necessarie designazioni *privacy*.
Qualora la segnalazione abbia a oggetto violazione del Modello Organizzativo 231 o tematiche attinenti ai dati contabili, il Gestore opererà in sinergia con gli organi competenti (ad esempio, il Collegio sindacale), nel rispetto degli obblighi di riservatezza.
Una volta completata l'attività di accertamento, il Gestore della segnalazione può:

- archiviare la segnalazione perché infondata, motivandone le ragioni;
- dichiarare fondata la segnalazione e rivolgersi agli organi/funzioni interne competenti per i relativi seguiti; infatti, al Gestore della segnalazione non compete alcuna valutazione in ordine alle responsabilità individuali e agli eventuali successivi provvedimenti o procedimenti conseguenti.

Tutte le fasi dell'attività di accertamento sono sempre tracciate e archiviate correttamente a seconda della tipologia del canale di segnalazione utilizzato (ad esempio, se è stato utilizzato un canale di posta analogica tutta la documentazione cartacea come documenti, verbali di audizione ecc. dovrà essere correttamente archiviata all'interno di un faldone accessibile al solo gestore), al fine di dimostrare la corretta diligenza tenuta nel dare seguito alla segnalazione.
Inoltre, ai sensi di quanto previsto dal Decreto 24/2023, è necessario che, durante le fasi di istruttoria e di accertamento della segnalazione, sia tutelata la riservatezza dell'identità della persona Segnalante, del segnalato e di tutte le persone coinvolte e/o menzionate nella segnalazione (cfr. **infra III.1**).

FASE IV- RISCONTRO AL SEGNALANTE

Il Gestore della segnalazione deve fornire un **riscontro** al Segnalante, entro 3 mesi dalla data di avviso di ricevimento o - in mancanza di tale avviso - entro 3 mesi dalla data di scadenza del termine di sette giorni per tale avviso.
È opportuno specificare che non è necessario concludere l'attività di accertamento entro

i tre mesi, considerando che possono sussistere fattispecie che richiedono, ai fini delle verifiche, un tempo maggiore. Pertanto, si tratta di un riscontro che, alla scadenza del termine indicato, può essere definitivo se l'istruttoria è terminata oppure di natura interlocutoria sull'avanzamento dell'istruttoria, ancora non ultimata.
Per le definizioni di "*riscontro*" e "*seguito*", si rinvia al paragrafo DEFINIZIONI.
Alla scadenza dei tre mesi, il Gestore della segnalazione può comunicare al Segnalante:
1) l'avvenuta **archiviazione** della segnalazione, motivandone le ragioni;
2) l'avvenuto accertamento del**la fondatezza della segnalazione** e la sua trasmissione agli organi interni competenti.
Non spetta al Gestore della segnalazione accertare le responsabilità individuali, qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati da SIPPIC S.p.A., a pena di sconfinare nelle competenze dei soggetti a ciò preposti o della Magistratura.
3) l'attività svolta fino a questo momento e/o l'attività che intende svolgere.
In tale ultimo, caso è consigliabile comunicare alla persona Segnalante anche il **successivo esito finale** dell'istruttoria della segnalazione (archiviazione o accertamento della fondatezza della segnalazione con trasmissione agli organi competenti), in linea con le LG ANAC 2023.
Tale attività di istruttoria e di accertamento spettano esclusivamente al Gestore delle segnalazioni, comprese tutte quelle attività necessarie a dare seguito alla segnalazione (ad esempio, le audizioni o le acquisizioni di documenti).

II.8.) CONSERVAZIONE DELLA DOCUMENTAZIONE

La segnalazione e la relativa documentazione saranno conservati per il tempo strettamente necessario alla gestione della stessa e comunque non oltre 5 anni dalla chiusura del processo di gestione nella Piattaforma.
I supporti originali delle segnalazioni pervenute attraverso la linea telefonica dedicata e/o attraverso la richiesta di audizione e/o altre modalità sono conservati dal Gestore, attraverso il caricamento sulla Piattaforma sull'apposita sezione competente.

II.9. IL CANALE ESTERNO E LA DIVULGAZIONE PUBBLICA

II.9.1.) IL CANALE ESTERNO PRESSO ANAC

Il Decreto 24/2023 prevede anche per i soggetti del settore privato la possibilità di effettuare una segnalazione attraverso un canale esterno.
L'accesso al canale esterno è consentito solo al ricorrere di determinate condizioni espressamente previste dal Legislatore. In particolare, la persona Segnalante può effettuare una segnalazione a questo canale se, al momento della sua presentazione:
1.) il canale interno, pur essendo obbligatorio non è attivo o, anche se attivato, non è conforme a quanto previsto dal Decreto 24/2023 con riferimento ai soggetti e alle modalità di presentazione delle segnalazioni interne che devono essere in grado di garantire la riservatezza dell'identità del Segnalante e degli altri soggetti tutelati.
2) la persona Segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito da parte della persona o dell'ufficio designati. Si fa riferimento ai casi in cui il canale interno sia stato utilizzato ma il Gestore del canale non abbia intrapreso, entro i termini previsti dal decreto, alcuna attività circa l'ammissibilità della segnalazione, la verifica della sussistenza dei fatti segnalati o la comunicazione dell'esito dell'istruttoria svolta;

3.) la persona Segnalante ha fondati motivi di ritenere ragionevolmente sulla base di circostanze concrete allegate ed informazioni effettivamente acquisibili e, quindi, non su semplici illazioni, che se effettuasse una segnalazione interna: o alla stessa non sarebbe dato efficace seguito in ragione delle specifiche circostanze del caso concreto(si pensi, ad esempio, all'ipotesi in cui vi sia il fondato timore che non sarebbe svolta alcuna attività a causa di un accordo tra chi riceve la segnalazione e la persona coinvolta nella violazione; o a seguito dell'occultamento o distruzione di prove di condotte illecite di cui il Segnalante sia a conoscenza; oppure, all'ipotesi in cui il Gestore della segnalazione sia in conflitto di interessi perché la segnalazione lo riguarda direttamente, come segnalato, oppure come Segnalante). In tali casi sarà possibile accedere al canale esterno onde evitare che alla segnalazione non sia dato efficace seguito; o questa potrebbe determinare il rischio di ritorsione;
4.) la persona Segnalante ha fondato motivo – nei termini indicati al punto *sub* **3.)** - di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse. Si fa riferimento, ad esempio, al caso in cui la violazione richieda in modo evidente un intervento urgente da parte di un'autorità pubblica per salvaguardare un interesse che fa capo alla collettività quale ad esempio la salute, la sicurezza o la protezione dell'ambiente.

II.9.2.) LA PRESENTAZIONE E LA GESTIONE DELLE SEGNALAZIONI

l'ANAC ha disciplinato, nelle Linee Guida e nell'apposito Regolamento (adottato con delibera 301 del 12 luglio 2023), le modalità di presentazione e gestione delle segnalazioni esterne, prevedendo che le stesse possano essere effettuate soltanto dalle persone fisiche legittimate ai sensi del Decreto 24/2023.
Con riguardo alle modalità di presentazione, le segnalazioni possono essere effettuate:
1) tramite piattaforma informatica, delineata come canale prioritario di segnalazione in quanto ritenuto maggiormente idoneo a garantire la riservatezza del Segnalante e della segnalazione; si prevede, infatti, che i dati della segnalazione siano crittografati ed i dati del Segnalante siano oscurati e segregati in apposita sezione della piattaforma, in modo da renderli inaccessibili anche all'ufficio istruttore di ANAC. Sempre al fine di garantire la massima riservatezza si prevede, inoltre, la figura del Custode delle identità. Quest'ultimo è il soggetto che, su esplicita e motivata richiesta del Dirigente dell'Ufficio *Whistleblowing* interno ad ANAC, consente di accedere all'identità del Segnalante, la quale tuttavia non è nota al custode stesso.
2) oralmente, attraverso un servizio telefonico con operatore. Quest'ultimo è un componente dell'Ufficio ANAC competente, che acquisisce la segnalazione telefonica e la inserisce sulla piattaforma ANAC unitamente al file audio della registrazione;
3) tramite incontri diretti fissati entro un termine ragionevole, cui consegue l'inserimento della segnalazione nella piattaforma da parte dell'operatore. Nel Regolamento è precisato che per ricorrere all'incontro diretto è necessaria una richiesta motivata.
Ai fini della ammissibilità, nella segnalazione devono essere indicati:
a) la denominazione e i recapiti del *whistleblower*;
b) i fatti oggetto di segnalazione e l'Amministrazione o Ente in cui essi sono avvenuti;
c) l'Amministrazione o l'Ente nel cui contesto lavorativo il *whistleblower* opera e il profilo professionale da quest'ultimo rivestito;
d) la descrizione sintetica delle modalità con cui il *whistleblower* è venuto a conoscenza dei fatti segnalati.

La segnalazione esterna è considerata inammissibile per i seguenti motivi:
i) manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate nell'art. 2, co. 1, lett. a) del Decreto 24/2023;
ii) manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità;
iii) manifesta incompetenza dell'Autorità sulle questioni segnalate;
iv) accertato contenuto generico della segnalazione esterna, tale cioè da non consentire la comprensione dei fatti, ovvero segnalazione esterna corredata da documentazione non appropriata, inconferente o comunque tale da rendere incomprensibile il contenuto stesso della segnalazione;
v) produzione di sola documentazione in assenza della segnalazione esterna;
vi) mancanza dei dati che costituiscono elementi essenziali della segnalazione esterna;
vii) sussistenza di violazioni di lieve entità.
In ogni caso, l'Ufficio 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 sette giorni dal ricevimento, comunica al Segnalante:

- l'archiviazione predisposta o che intende predisporre;
- la trasmissione all'Autorità competente già effettuata o che intende effettuare;
- l'attività già svolta dall'Ufficio di vigilanza competente interno all'Autorità o l'attività che quest'ultimo intende svolgere. Infine, laddove nei termini di cui al precedente comma l'Ufficio non abbia comunicato la determinazione definitiva sul seguito della segnalazione, ma solo le attività che si intendono intraprendere, lo stesso comunica alla persona Segnalante l'esito finale della gestione della segnalazione, che può consistere nell'archiviazione, nelle risultanze istruttorie dell'Ufficio di vigilanza competente o nella trasmissione alle Autorità competenti.

II.9.3.) LA DIVULGAZIONE PUBBLICA

La normativa introduce anche la possibilità per il Segnalante di effettuare una **divulgazione pubblica** beneficiando della protezione.
Si tratta di una novità estremamente delicata per le imprese, in ragione delle potenzialità lesive per l'ente di una denuncia effettuata in assenza di giustificati motivi o di fondati elementi di prova.
I potenziali effetti lesivi possono inoltre essere acuiti dal fatto che la divulgazione può essere effettuata non solo attraverso la stampa, ma anche attraverso mezzi diffusione in grado di raggiungere un numero elevato di persone, quali ad esempio i *social network* e i nuovi canali di comunicazione (ad es. Facebook, Twitter, ecc.), i quali non sono presidiati da discipline specifiche, regole deontologiche e controlli da parte di apposite autorità di vigilanza.
Ciò rende di estrema importanza da un lato, circoscrivere il più possibile, anche in via interpretativa e attraverso l'informazione e la formazione dei dipendenti, il ricorso a tale istituto; e dall'altro, costruire in modo pienamente efficace e conforme sia alle prescrizioni del Decreto 24/2023 che delle Linee Guida ANAC i canali interni di segnalazione.
Per ricorrere a tale procedura deve ricorrere almeno una delle seguenti condizioni:

- ad una segnalazione interna a cui l'ente non abbia dato riscontro nei termini previsti abbia fatto seguito una segnalazione esterna ad ANAC la quale, a sua volta, non ha fornito riscontro al Segnalante entro termini ragionevoli;
- la persona ha già effettuato direttamente una segnalazione esterna ad ANAC la

quale, tuttavia, non ha dato riscontro al Segnalante in merito alle misure previste o adottate per dare seguito alla segnalazione entro termini ragionevoli.

- che il Segnalante ritenga sussistere fondati motivi di un "*pericolo imminente e palese per il pubblico interesse*", considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti.
- che il Segnalante ritenga sussistere fondati motivi per ritenere che la segnalazione esterna possa comportare un rischio di ritorsione oppure non avere efficace seguito perché ad esempio potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta a ricevere la segnalazione e l'autore della violazione.

In altri termini, si tratta di situazioni particolarmente gravi di negligenza o comportamenti dolosi all'interno dell'ente.

Anche in tali casi, inoltre, i motivi che legittimano il ricorso alla segnalazione esterna devono essere fondati sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili.

Nelle Linee Guida ANAC si precisa, infine, che ove il soggetto che effettui una divulgazione pubblica riveli la propria identità non si pone un problema di tutela della riservatezza, fermo restando che gli verranno garantite le altre tutele previste dal decreto. Mentre se lo stesso ricorre a pseudonimo o *nickname*, l'ANAC tratterà la segnalazione alla stregua di una segnalazione anonima e avrà cura di registrarla, ai fini della conservazione, per garantire al divulgatore, in caso di disvelamento successivo dell'identità dello stesso, le tutele previste se ha subito ritorsioni.

Sebbene sul punto nulla sia detto espressamente, questa puntualizzazione sembra confermare l'idea che, in via generale, spetti all'ANAC valutare se effettivamente la divulgazione pubblica sia stata legittimamente effettuata e nel rispetto dei presupposti richiesti dalla norma.

II.9.4.) LA DENUNCIA ALLA AUTORITA' GIUDIZIARIA

Il Decreto 24/2023, in conformità alla precedente disciplina, riconosce ai soggetti tutelati anche la possibilità di rivolgersi alle Autorità giudiziarie, per inoltrare una denuncia di condotte illecite di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato, come definito nel paragrafo denominato DEFINIZIONI della presente.

In linea con le indicazioni già fornite da ANAC nelle LLGG n. 469/2021, si precisa che qualora il *whistleblower* rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dal Decreto 24/2023, ciò non lo esonera dall'obbligo - in virtù di quanto previsto dal combinato disposto dell'art. 331 c.p.p. e degli artt. 361 e 362 c.p. - di denunciare alla competente Autorità giudiziaria i fatti penalmente rilevanti e le ipotesi di danno erariale. Si rammenta in ogni caso che l'ambito oggettivo degli artt. 361 e 362 c.p., disponendo l'obbligo di denunciare soltanto reati (procedibili d'ufficio), è più ristretto di quello delle segnalazioni effettuabili dal *whistleblower* che può segnalare anche illeciti di altra natura. Resta fermo che, laddove il dipendente pubblico denunci un reato all'Autorità giudiziaria ai sensi degli artt. 361 o 362 c.p. e poi venga discriminato per via della segnalazione, potrà beneficiare delle tutele previste dal decreto per le ritorsioni subite.

Le stesse regole sulla tutela della riservatezza e del contenuto delle segnalazioni vanno rispettate dagli uffici delle Autorità giudiziarie cui è sporta la denuncia.

III) LE TUTELE PREVISTE DAL DECRETO LEGISLATIVO 24/2023

III.1.) LA TUTELA DELLA RISERVATEZZA

L'articolo 4 del d. Lgs. 24/2023 prevede a carico dei soggetti del settore pubblico e privato l'obbligo di attivare *"propri canali di segnalazione che garantiscano, anche attraverso il ricorso a strumenti di crittografia, la riservatezza della identità della persona Segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione"*.

La prima tutela posta dal Legislatore a favore del Segnalante è l'obbligo di garantire la riservatezza della sua identità e di ogni altra informazione, inclusa l'eventuale documentazione allegata, dalla quale possa direttamente o indirettamente risalire all'identità del *whistleblower*.

La medesima garanzia è prevista in favore delle persone coinvolte (cd. segnalato) e/o menzionate nella segnalazione, nonché ai facilitatori (cfr. articolo 2, comma 1 n. 6 lett. h del Decreto 24/2023 l'assistenza fornita dal facilitatore deve essere mantenuta riservata), in considerazione del rischio di ritorsioni.

A tale obbligo sono tenuti:

- i soggetti competenti a ricevere e gestire le segnalazioni;
- l'ANAC;
- le Autorità Amministrative (Dipartimento per la funzione pubblica e Ispettorato Nazionale del Lavoro) cui l'ANAC trasmette, per competenza, le segnalazioni esterne ricevute.

La riservatezza deve essere garantita per ogni modalità di segnalazione, quindi, anche quando avvenga in forma orale.

III.1.1.) APPROFONDIMENTO 1- LA TUTELA DELLA RISERVATEZZA DEL SEGNALANTE

L'obbligo di riservatezza impone che un eventuale disvelamento della identità del Segnalante a favore di persone diverse da quelle competenti a ricevere la segnalazione o a dare seguito ad essa avvenga sempre con il consenso della stessa.

La tutela della riservatezza della identità del Segnalante va assicurata anche in ambito giurisdizionale e disciplinare: il Decreto Legislativo 24/2023 disciplina fino a quale momento nel procedimento penale, in quello innanzi alla Corte dei Conti e nel procedimento disciplinare debba essere garantita la riservatezza.

In particolare, nell'ambito del procedimento disciplinare attivato dall'Ente contro il presunto autore della condotta segnalata, l'identità del Segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

Qualora invece la contestazione sia fondata, in tutto o in parte, sulla segnalazione e l'identità del Segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare o della persona comunque coinvolta nella segnalazione, quest'ultima sarà utilizzabile ai fini del procedimento disciplinare solo previo consenso espresso della persona Segnalante alla rivelazione della propria identità.

In tali casi, è dato preventivo avviso alla persona Segnalante mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati.

Qualora il soggetto Segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione.
Resta ferma in ogni caso, sussistendone i presupposti, la facoltà dell'ente di procedere con la denuncia all'Autorità giudiziaria.
Il Decreto 24/2023, poi, disciplina due casi in cui per rivelare la identità del segnante devono concorrere: *i)* la previa comunicazione scritta delle ragioni alla base della rivelazione dei dati relativi alla sua identità; *ii)* il previo consenso espresso dal Segnalante.
La prima ipotesi ricorre laddove nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, l'identità del Segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare. In tal caso, come già sopra precisato, il Decreto 24/2023, oltre al previo consenso del Segnalante, chiede anche di comunicare, sempre previamente, in forma scritta a quest'ultimo le motivazioni che conducono al disvelamento della sua identità.
La seconda ipotesi ricorre, invece, nel caso in cui nelle procedure di segnalazione interna ed esterna la rivelazione dell'identità del Segnalante sia indispensabile anche ai fini della difesa della persona coinvolta. Anche in questo caso per disvelare l'identità del Segnalante è necessario sia acquisire previamente il consenso espresso dello stesso che notificare allo stesso in forma scritta motivazioni alla base della necessità di disvelare la sua identità.
Dalla previsione dell'obbligo di riservatezza deriva un importante corollario: il rispetto dell'obbligo di riservatezza impone che l'Ente coinvolto nella gestione delle segnalazioni garantisca tale riservatezza durante tutte le fasi del procedimento di segnalazione, ivi compreso l'eventuale trasferimento delle segnalazioni ad altre Autorità competenti.
Sul piano operativo, l'altro importante corollario dell'obbligo di riservatezza è la previsione - sia nell'ambito del canale interno di segnalazione che di quello esterno – di adeguate procedure per il trattamento delle segnalazioni anche mediante sistemi di gestione informatizzata delle stesse, che consentano di tutelare e mantenere riservata l'identità del Segnalante, il contenuto della segnalazione e la relativa documentazione, anche con il ricorso a strumenti di crittografia.
La riservatezza va garantita anche quando la segnalazione viene effettuata attraverso modalità diverse da quelle istituite dai soggetti del settore pubblico e privato e dalla stessa ANAC in conformità al decreto o perviene a personale diverso da quello autorizzato e competente al trattamento della stessa, a cui la segnalazione va trasmessa senza ritardo.

III.1.2.) APPROFONDIMENTO 2- LA TUTELA DELLA RISERVATEZZA DEL SEGNALATO E DI ALTRI SOGGETTI

Il Decreto 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*).
Peraltro, a sostegno della persona *segnalata* e del suo diritto di difesa, l'art. 12, co. 9 della norma ha, altresì, riconosciuto che tale soggetto possa essere sentito o venga sentito, dietro sua richiesta, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.
La normativa non riconosce però al *segnalato* il diritto di essere sempre informato della

segnalazione che lo riguarda; tale diritto, infatti, è garantito nell'ambito del procedimento eventualmente avviato nei suoi confronti a seguito della conclusione dell'attività di verifica e di analisi della segnalazione e nel caso in cui tale procedimento sia fondato in tutto o in parte sulla segnalazione.
D'altro canto, il riconoscimento del diritto del *segnalato* ad essere sempre e comunque informato della segnalazione interna e/o esterna, oltre a non avere un chiaro appiglio normativo, rischierebbe di compromettere lo svolgimento dell'attività istruttoria con particolare riferimento alle successive/eventuali indagini penali.
Il Legislatore ha poi ritenuto di garantire la riservatezza:

- al *facilitatore*, sia per quanto riguarda l'identità, sia con riferimento all'attività in cui l'assistenza si concretizza;
- a persone diverse dal segnalato, ma comunque implicate in quanto menzionate nella segnalazione o nella divulgazione pubblica (si pensi ad esempio a persone indicate come testimoni).

La *ratio* della nuova disciplina va individuata nell'esigenza di salvaguardare i diritti di soggetti che, per effetto della segnalazione, potrebbero subire danni alla loro reputazione o altre conseguenze negative ancor prima che venga dimostrata l'estraneità o meno degli stessi ai fatti segnalati.
La riservatezza del facilitatore, della persona coinvolta e della persona menzionata nella segnalazione va garantita fino alla conclusione dei procedimenti avviati in ragione della segnalazione e nel rispetto delle medesime garanzie previste in favore della persona Segnalante.
Tenuto conto di quanto sopra, come già anticipato, si ribadisce che sia l'Autorità che le amministrazioni e gli enti del settore pubblico e privato devono quindi attivare canali di segnalazione che garantiscano la riservatezza dell'identità di tali soggetti anche tramite il ricorso a strumenti di crittografia, ove si utilizzino strumenti informatici.
In ogni caso, la stessa riservatezza va garantita – come precisato sopra per il Segnalante - anche quando la segnalazione viene effettuata attraverso modalità diverse da quelle istituite in conformità al decreto nonché nei casi in cui la stessa perviene a personale diverso da quello addetto al trattamento, al quale la stessa viene comunque trasmessa senza ritardo.
Fa eccezione a questo dovere di riservatezza delle persone coinvolte o menzionate nella segnalazione il caso in cui le segnalazioni siano oggetto di denuncia alle Autorità giudiziarie. Ciò trova conferma nel fatto che il Legislatore, nel prevedere la tutela della riservatezza nei procedimenti giudiziari, fa riferimento solo all'identità del Segnalante e non anche a quella della persona coinvolta o menzionata nella segnalazione.
La *ratio* di siffatta previsione risponde all'esigenza di consentire alle Autorità giudiziarie di procedere con le proprie indagini avendo un quadro completo del fatto segnalato e acquisendo quante più informazioni possibili per pronunciarsi sul caso di specie.
A tal fine potrebbe rendersi necessario conoscere l'identità delle persone coinvolte o menzionate nella segnalazione. Si pensi, ad esempio, all'ipotesi in cui l'Autorità giudiziaria debba sentire i testimoni sui fatti intorno ai quali è chiamata ad esprimersi. La mancata rivelazione dell'identità di questi ultimi priverebbe l'Autorità di uno degli elementi fondamentali per la risoluzione del caso.

III.2.) LA TUTELA DEI DATI PERSONALI

Ai sensi dell'articolo 13, l'acquisizione e gestione delle segnalazioni deve avvenire in

conformità alla normativa in tema di tutela dei dati personali.
La tutela dei dati personali va assicurata non solo alla persona del Segnalante o denunciante ma anche agli altri soggetti cui si applica la tutela della riservatezza (es. facilitatore, la persona coinvolta, la persona menzionata nella segnalazione) nella qualità di *interessati* dal trattamento dei dati (cfr. art. 4 par. 1 Regolamento UE 679/2016).
I dati oggetto di trattamento sono: dati anagrafici, dati di contatto, tutti i dati personali, anche particolari e giudiziari eventualmente forniti dal segnalante e dal segnalato, nell'ambito della Segnalazione e della gestione della stessa.
Il ricevimento e la gestione delle segnalazioni determinano in capo a Sippic un trattamento dei dati personali:
• di natura comune, di natura particolare (ex "*dati sensibili*") e giudiziari (quali condanne penali e reati), eventualmente contenuti nella segnalazione e negli atti e nei documenti a essa allegati (cfr. Parere del Garante *privacy* sullo "Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne", provv. 6 luglio 2023, n. 304, di seguito, "Parere del Garante privacy");
• relativi a tutte le persone fisiche - identificate o identificabili - a vario titolo coinvolte nelle vicende segnalate (Segnalante, segnalato, facilitatore, eventuali altri terzi), c.d. interessati;
• necessario per dare attuazione agli obblighi di legge previsti dalla disciplina *whistleblowing* la cui osservanza è condizione di liceità del trattamento ex art. 6, par. 1, lett. c) e parr. 2 e 3, art. 9, par. 2, lett. b) e artt. 10 e. 88 del GDPR (v. Parere del Garante privacy);
• realizzato al solo fine di gestire e dare seguito alle segnalazioni (art. 12, co. 1 del Decreto);
- che, in ragione della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del Segnalante previsto dal Decreto, presenta rischi specifici per i diritti e le libertà degli interessati (v. Parere del Garante privacy) e, pertanto, deve essere preceduto da una valutazione d'impatto sulla protezione dei dati, c.d. DPIA (art. 13, co. 6 del Decreto e artt. 35 e 36 del GDPR);

• rispetto al quale, l'esercizio dei diritti degli interessati (es. accesso, rettifica, aggiornamento, cancellazione, limitazione del trattamento, portabilità, opposizione) può essere limitato qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del Segnalante (art. 13, co. 3 del Decreto e art. 2-*undecies* del Codice privacy).
Si rammenta che, al pari degli altri trattamenti dei dati personali, anche quello relativo al ricevimento e alla gestione delle segnalazioni deve essere censito nel registro delle attività di trattamento in conformità all'art. 30 del GDPR. Pertanto, ai fini della implementazione del canale di segnalazione interna, è necessario procedere all'aggiornamento del citato registro.

III.2.1.) RUOLI *PRIVACY* NEL CANALE DI SEGNALAZIONE INTERNO

Il Decreto individua i ruoli ai fini della normativa *data protection* degli enti che attivano il canale di segnalazione interna e dei soggetti coinvolti nella ricezione e nella gestione delle segnalazioni.

Avendo attivato il canale interno, SIPPIC S.p.A. effettua i trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni in qualità di **Titolare del trattamento** (art. 13, co. 4 del Decreto); come tale assicura che le suffette attività di trattamento siano svolte coerentemente alle prescrizioni del Reg. UE 679/2016 (cd. GDPR) e delle normative nazionali vigenti.
Con riguardo al GESTORE delle segnalazioni, SIPPIC provvede a conferire formale incarico per il trattamento dei dati personali attraverso la consegna di una lettera di designazione *ex* articolo 28 GDPR.
La lettera prevede specifiche istruzioni per il corretto trattamento dei dati personali di cui alla segnalazione e la puntuale indicazione delle misure di sicurezza da applicare.
Con riferimento al fornitore della piattaforma di segnalazione, esso ha sottoscritto l'accordo sulla protezione dei dati *ex* articolo 28 GDPR.
I diritti di cui agli articoli da 15 a 22 del GDPR possono essere esercitati nei limiti di quanto previsto dalla normativa vigente, attraverso i canali indicati nella informativa *ex* articolo 13 GDPR resa disponibile tramite i canali di segnalazione e specifica sezione del sito aziendale.
In particolare, la persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che, normalmente, il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento). Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona Segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali.

III.3.) LA TUTELA DALLE RITORSIONI

L'articolo 17 del D.Lgs. 24/2023 sancisce il divieto di ritorsione nei confronti delle persone "*di cui all'articolo 3*" della stessa norma, tali intendendosi il Segnalante, denunciante o colui che ha effettuato la divulgazione pubblica oltre che gli altri soggetti assimilati.
L'articolo 2), comma 1) lettera m) definisce la ritorsione come "*qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o della divulgazione pubblica e che provoca o può provocare alla persona Segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto*"
La novella del 2023 elenca esplicitamente, seppure a titolo non esaustivo "*talune fattispecie che, qualora siano riconducibili all'articolo 2, comma1, lettera m), costituiscono ritorsioni*":
a) licenziamento, sospensione o misure equivalenti;
b) retrocessione di grado o mancata promozione;
c) mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;

d) sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
e) note di demerito o referenze negative;
f) adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
g) coercizione, intimidazione, molestie o ostracismo;
h) discriminazione o comunque trattamento sfavorevole;
i) 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;
j) mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;
k) danni, anche alla reputazione della persona, in particolare sui social media, o 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;
m) conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
n) annullamento di una licenza o di un permesso;
o) richiesta di sottoposizione ad accertamenti psichiatrici o medici.
Gli atti ritorsivi adottati in violazione di tale divieto sono nulli.
L'ANAC è l'autorità preposta a ricevere dal Segnalante e gestire le comunicazioni su presunte ritorsioni dallo stesso subite.
Affinché sia riconosciuta tale forma di tutela, il Decreto 24/2023 prevede le seguenti condizioni:

- che il Segnalante/denunciante al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica avesse "*fondato motivo*" di ritenere le informazioni veritiere e rientranti nel perimetro applicativo della disciplina;
- che la segnalazione, denuncia o divulgazione sia stata effettuata secondo la disciplina prevista dal Decreto 24/2023.
- che esista un rapporto di conseguenzialità tra segnalazione (oppure divulgazione, denuncia) e le misure subite;

Questo implica da parte del Segnalante un'attenta diligenza nella valutazione delle informazioni che non è sufficiente si fondino su semplici supposizioni, "*voci di corridoio*" o notizie di pubblico dominio.
Pertanto, il soggetto che ritenga di aver subito una ritorsione, anche tentata o minacciata, come conseguenza di una segnalazione/divulgazione/denuncia lo comunica all'ANAC, che dovrà accertare il nesso di causalità tra la ritorsione e la segnalazione e, quindi, adottare i conseguenti provvedimenti.
Esistono dei casi in cui il **Segnalante perde la protezione**: *i)* qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale del Segnalante per i reati di diffamazione o di calunnia o nel caso in cui tali reati siano commessi con la denuncia all'autorità giudiziaria o contabile. Nei casi di accertamento di dette responsabilità, al soggetto Segnalante e denunciante, è inoltre, applicata una sanzione disciplinare; *ii)* in caso di responsabilità civile per lo stesso titolo per dolo o colpa grave. In entrambe le ipotesi alla persona Segnalante o denunciante verrà irrogata una sanzione disciplinare.
Le LG. ANAC hanno specificato che la tutela, ancorché tardiva, va applicata anche in caso di sentenza di primo grado non confermata nei successivi gradi di giudizio, nei casi di archiviazione, nonché nei casi di accertata colpa lieve.

Infine, si ricorda che, come già detto, di fronte a una **segnalazione anonima**, il Decreto 24/2023 prevede che la tutela è assicurata qualora la persona Segnalante sia stata successivamente identificata o la sua identità si sia palesata soltanto in un secondo momento.
Sippic S.p.A. si impegna a garantire ai soggetti di cui all'articolo 3 del D.Lgs. 24/2023 il divieto di commissione di qualsiasi atto di ritorsione come conseguenza di una segnalazione, anche attraverso la predisposizione di un idoneo sistema disciplinare in danno di coloro che avranno violato il divieto medesimo.

III.4.) LE LIMITAZIONI DELLA RESPONSABILITA' PER IL SEGNALANTE

Ulteriore tutela riconosciuta dal Decreto 24/2023 al Segnalante, è la limitazione della sua responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni, che altrimenti lo esporrebbero a responsabilità penali, civili e amministrative.
In particolare, il Segnalante non sarà chiamato a rispondere né penalmente, né in sede civile e amministrativa:

- di rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.);
- di rivelazione del segreto professionale (art. 622 c.p.);
- di rivelazione dei segreti scientifici e industriali (art. 623 c.p.);
- di violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.);
- di violazione delle disposizioni relative alla tutela del diritto d'autore;
- di violazione delle disposizioni relative alla protezione dei dati personali;
- di rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta.

Il Decreto 24/2023 pone tuttavia due condizioni all'operare delle suddette limitazioni di responsabilità:
1) al momento della rivelazione o della diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per svelare la violazione oggetto di segnalazione;
2) la segnalazione sia effettuata nel rispetto delle condizioni previste dal Decreto 24/2023 per beneficiare della tutela contro le ritorsioni (fondati motivi per ritenere veritieri i fatti segnalati, la violazione sia tra quelle segnalabili e siano rispettate le modalità e le condizioni di accesso alla segnalazione).
Va evidenziato, quindi, che la limitazione opera se le ragioni alla base della rivelazione o diffusione non sono fondate su semplici illazioni, gossip, fini vendicativi, opportunistici o scandalistici.
In ogni caso, occorre considerare che non è esclusa la responsabilità per condotte che:

- non siano collegate alla segnalazione;
- non siano strettamente necessarie a rivelare la violazione;
- configurino un'acquisizione di informazioni o l'accesso a documenti in modo illecito.

Ove l'acquisizione si configuri come un reato, si pensi all'accesso abusivo a un sistema informatico o a un atto di pirateria informatica, resta ferma la responsabilità penale e ogni altra responsabilità civile, amministrativa e disciplinare della persona Segnalante.
Sarà viceversa non punibile, ad esempio, l'estrazione (per copia, fotografia, asporto) di documenti cui si aveva lecitamente accesso

IV) RINUNCE E TRANSAZIONI

Il Decreto 24/2023 vieta, in generale, rinunce e transazioni dei diritti e dei mezzi di tutela dallo stesso previsti, a meno che non avvengano in particolari condizioni. Tale previsione, sottraendo in parte la disponibilità del diritto dalla sfera del beneficiario della tutela, risponde all'esigenza di implementare e rendere effettiva la protezione del *whistleblower*.

La norma consente, tuttavia, al Segnalante e agli altri soggetti tutelati, di poter rinunciare ai propri diritti e mezzi di tutela o farne oggetto di transazione, solo se ciò avviene nelle sedi protette e, quindi, dinanzi ad un Giudice, a seguito di tentativo obbligatorio di conciliazione, o di accordi di mediazione e conciliazione predisposti in sede sindacale o davanti agli organi di certificazione.

V) IL PROFILO DISCIPLINARE

SIPPIC S.p.A. prevede sanzioni nei confronti:

1) del Segnalante, nel caso di abuso dello strumento di segnalazione;
2) del Segnalato, in caso di accertamento degli illeciti segnalati;
3) del Gestore della segnalazione, nel caso di mancato rispetto della presente procedura;
4) nei confronti di coloro che violano il divieto di riservatezza del Segnalante ed i divieti di ritorsione posti a tutela del Segnalante stesso.

Il sistema di segnalazione è stato integrato nel D.Lgs. 231/01; conseguentemente, in caso di violazioni accertate, vanno estese ed applicate le sanzioni previste nel sistema disciplinare descritto nel Modello 231 di SIPPIC S.p.A. e nella, annessa, parte speciale cui si rimanda.

VI) OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA IN SEGUITO AL DECRETO LEGISLATIVO 24/2023 *(WHISTLEBLOWING)*

Nel caso in cui l'Organismo di Vigilanza non sia individuato come gestore della segnalazione, esso dovrà ricevere:

1) immediata informativa su segnalazioni rilevanti in termini 231 affinché, nell'esercizio della sua attività di vigilanza possa condividere le proprie eventuali osservazioni e partecipare alla istruttoria o comunque seguirne l'andamento;
2) un aggiornamento periodico sulla attività complessiva di gestione delle segnalazioni anche non 231 al fine di verificare il funzionamento del sistema di *whistleblowing* e proporre all'ente eventuali necessità di suo miglioramento.

SIPPIC S.p.A. si occuperà di procedimentalizzare i predetti flussi informativi nel Modello 231.

VII) ATTIVITA' DI FORMAZIONE ED INFORMAZIONE AI SENSI DEL DECRETO LEGISLATIVO 24/2023 (*WHISTLEBLOWING*)

Al fine di garantire una gestione consapevole, accurata e professionale delle segnalazioni, il Decreto 24/2023 mira a sensibilizzare - anche attraverso un'attività di formazione e informazione - i soggetti interni ed esterni a vario titolo coinvolti circa le implicazioni etiche, legali e di riservatezza che scaturiscono dalle procedure di segnalazione.

A tal fine, la norma disciplina i seguenti oneri formativi e informativi:

- l'art. 4, co. 2, prevede che gli uffici o le persone cui è demandata la gestione del canale di segnalazione debbano ricevere una specifica formazione relativa alla gestione del canale;

- l'art. 5, co. 1, lett. e) prevede che gli uffici o le persone cui è demandata la gestione del canale di segnalazione mettano a disposizione della persona Segnalante (a titolo esemplificativo, personale interno, consulenti esterni, azionisti, Partner commerciali, fornitori, ecc.22) informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne od esterne.

VII.1.) OBBLIGHI DI FORMAZIONE

La formazione del personale che gestisce il canale di segnalazione è di fondamentale importanza per assicurare che le segnalazioni ricevute siano trattate in maniera adeguata e in conformità alle disposizioni applicabili.
A tal fine, SIPPIC S.p.A. si impegna a fornire a chi gestisce la segnalazione un'adeguata formazione in relazione ad alcuni argomenti chiave quali, ad esempio:
• **aspetti normativi**, che riguardano i principi e le disposizioni contenute nel Decreto 24/2023, con specifico *focus* in merito agli adempimenti che devono essere svolti dal personale cui è affidata la gestione del canale di segnalazione (ad esempio, le attività previste dall'art. 5 del Decreto), nonché rispetto agli adempimenti in ambito Data Protection;
• **procedure e presupposti**: approfondita panoramica delle policies, delle procedure e delle modalità operative adottate, anche per prassi, da SIPPIC S.p.A. per la gestione del canale di segnalazione (ad esempio, le fasi di gestione delle segnalazioni dal momento della ricezione, alla successiva attività di istruttoria e riscontro al Segnalante);
• **principi generali di comportamento**: al fine di favorire una adeguata comprensione e consapevolezza di alcuni principi generali quali, ad esempio:
▪ **confidenzialità e riservatezza**: necessità di applicare opportune misure tecniche e organizzative da parte del personale cui è affidata la gestione delle segnalazioni, al fine di salvaguardare la confidenzialità delle informazioni durante tutto il processo di gestione delle segnalazioni;
▪**etica ed integrità:** promozione di un ambiente etico e integro all'interno dell'impresa in merito all'importanza di agire con onestà, trasparenza e responsabilità nella gestione delle segnalazioni;
▪ **ascolto attivo, competenze comunicative e collaborazione**: sensibilizzazione del personale cui è affidata la gestione delle segnalazioni circa l'ascolto attivo, la comunicazione empatica e la comprensione degli aspetti psicologici connaturati alla gestione delle segnalazioni, con particolare riguardo alle interlocuzioni con la persona Segnalante, nonché in merito alle opportune ed adeguate pratiche di collaborazione in team con le altre funzioni aziendali coinvolte nella gestione della segnalazione (ad esempio, funzione legale, funzione risorse umane, OdV).
SIPPIC S.p.A. si impegna ad erogare tale formazione con cadenza periodica, al fine di garantirne l'efficacia, integrandola opportunamente in caso di aggiornamenti normativi in merito alle disposizioni rilevanti e applicabili relativamente alla gestione dei canali di segnalazione.
SIPPIC S.p.A., altresì, si impegna ad assicurare un'adeguata formazione (ivi compresa la disciplina sul trattamento dei dati personali) a tutto il personale interno, così da creare un'opportuna consapevolezza circa le finalità e le tutele riconosciute dal Decreto 24/2023, nonché una cultura di integrità e responsabilità all'interno dell'impresa.

VII.2.) OBBLIGHI DI INFORMAZIONE

Il Decreto 24/2023 prevede che vengano messe a disposizione della persona Segnalante informazioni chiare circa il canale, le procedure e i presupposti per effettuare le segnalazioni, interne o esterne.

A tal fine, SIPPIC S.p.A. si impegna a garantire un'adeguata informativa in ordine all'utilizzo del canale interno e di quello esterno gestito da ANAC, con particolare riguardo ai presupposti per effettuare le segnalazioni attraverso tali canali, ai soggetti competenti cui è affidata la gestione delle segnalazioni interne, nonché alle procedure adottate, a tal fine, dalla Società. Tali informazioni verranno esposte nei luoghi di lavoro in un punto visibile, accessibile a tutte le persone (ivi comprese quelle che, pur non essendo presente fisicamente nei luoghi di lavoro, sono legittimate a effettuare segnalazioni di *whistleblowing*) nonché in una sezione apposita del sito web istituzionale della Società e, laddove implementata, della piattaforma informatica.

A titolo esemplificativo e non esaustivo, SIPPIC S.p. A. si impegna a fornire le seguenti informazioni:

- soggetti legittimati a effettuare le segnalazioni;
- soggetti che godono delle misure di protezione riconosciute dal Decreto;
- violazioni che possono essere segnalate;
- presupposti per effettuare la segnalazione interna o esterna;
- indicazioni sul canale di segnalazione implementato da SIPPIC S.p.A. (e le relative istruzioni circa le modalità di funzionamento dello stesso), nonché quello esterno gestito da ANAC;
- chiara indicazione che le segnalazioni devono specificare che si vuole mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni;
- procedure che la persona Segnalante deve seguire per effettuare in maniera corretta una segnalazione (a titolo esemplificativo, gli elementi che la segnalazione deve contenere);
- soggetti competenti cui è affidata la gestione delle segnalazioni interne;
- attività che, una volta correttamente effettuata la segnalazione, devono essere svolte dal soggetto che ha ricevuto e che gestisce la segnalazione;
- tutele riconosciute dal Decreto 24/2023 al Segnalante e agli altri soggetti che godono di protezione ai sensi dell'art. 3 della norma;
- condizioni al verificarsi delle quali è esclusa la responsabilità del Segnalante (anche in sede penale, civile o amministrativa) previste dall'art. 20 del Decreto 24/2023;
- sistema sanzionatorio adottato dalla Impresa e da ANAC in caso di violazione delle disposizioni del Decreto 24/2023.

VIII) INFORMAZIONI DA PUBBLICARE SUL SITO E NEI LUOGHI DI LAVORO DI SIPPIC S.P.A.

Le informazioni sull'utilizzo dei canali interni, di quello esterno presso ANAC e della divulgazione pubblica – - con particolare riguardo ai presupposti per effettuare le segnalazioni attraverso tali canali – sui soggetti cui è affidata la gestione delle segnalazioni nonché sulle procedure; altresì, la chiara indicazione che le segnalazioni devono specificare che si vuole mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni, sono pubblicate sul sito internet di

SIPPIC S.p.A oltre ad essere esposte nei luoghi di lavoro in un punto visibile, accessibile a tutte le interessate dalla normativa.