COMUNE DI PIANO DI SORRENTO

Città Metropolitana di Napoli

Atto organizzativo di attuazione della disciplina del Whistleblowing

Premessa

1. **Normativa e Linee Guida ANAC.**

La disciplina del Whistleblowing risponde all'esigenza di fornire particolare tutela a determinati soggetti che, venuti a conoscenza in ragione del loro rapporto di lavoro o di collaborazione con l'Ente, di fatti o comportamenti illeciti, li segnalino alle autorità competenti.

L'istituto è stato introdotto in Italia dalla legge 6 novembre 2012, n. 190 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"), che ha inserito l'art. 54-bis all'interno del d.lgs. 30 marzo 2001 n. 165. La disciplina è stata successivamente integrata dal decreto-legge 24 giugno 2014 n. 90, convertito nella legge 11 agosto 2014, n. 114, che ha modificato l'art. 54 bis inserendo anche l'Autorità Nazionale Anticorruzione (Anac) tra i soggetti destinatari delle segnalazioni.

Successivamente, la menzionata norma è stata riformulata ad opera della legge 30 novembre 2017 n. 179 ("Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"), che ha introdotto una regolamentazione più organica della materia. Le menzionate modifiche normative sono state accompagnate dall'emanazione di Linee Guida da parte di Anac aventi l'obiettivo di fornire indicazioni in merito agli accorgimenti da adottare al fine di dare attuazione alla disciplina. In particolare, dapprima Anac è intervenuta con la determinazione n. 6 del 28 aprile 2015 recante "Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblowing)".

A seguito della riforma dell'art. 54 bis ad opera della citata legge n. 179/2017, con Deliberazione n. 469 del 09/06/2021 Anac ha approvato le "Linee guida in materia di tutela

degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d. lgs 165/2001 (c.d. whistleblowing)".

L'istituto del Whistleblowing è stato infine rinnovato con l'adozione del D.lgs. n. 24/2023, emanato in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione dei c.d. Whistleblower, individuati **nei dipendenti, nei lavoratori autonomi, nei liberi professionisti e consulenti che prestano la propria attività a favore dell'ente pubblico, nei lavoratori e collaboratori delle imprese fornitrici di beni e servizi che realizzano opere in favore del medesimo.**

Con il recepimento della richiamata direttiva, il legislatore nazionale ha ampliato la portata oggettiva (gli illeciti e le violazioni che possono essere oggetto di segnalazioni) e soggettiva (coloro che sono legittimati a realizzare la segnalazione) del whistleblowing, e, contestualmente, si è posto l'obiettivo, attraverso un sistema di tutele definite, di favorire l'emersione di violazioni delle disposizioni normative nazionali ed europee, assicurando, al tempo stesso, una rafforzata protezione della riservatezza dell'identità del segnalante e di chi con lo stesso condivida la conoscenza dei fatti, come il c.d. facilitatore.

La nuova disciplina è, quindi, orientata, da un lato, a garantire la manifestazione della libertà di espressione e d'informazione, che comprende il diritto di ricevere e di comunicare informazioni, nonché la libertà e il pluralismo dei media. Dall'altro, è strumento per contrastare e prevenire la corruzione e la cattiva amministrazione.

Chi segnala fornisce, pertanto, informazioni che possono portare all'indagine, all'accertamento e al perseguimento dei casi di violazione di norme, rafforzando in tal modo i principi di trasparenza e responsabilità delle amministrazioni.

La segnalazione, di conseguenza, risponde ad una duplice ratio, consistente da un lato nel delineare un particolare status giuslavoristico in favore del soggetto che segnala illeciti e, dall'altro, nel favorire l'emersione dall'interno dell'Amministrazione, di fatti illeciti, promuovendo forme più incisive di contrasto alla corruzione. Nell'ambito del Whistleblowing è intervenuta l'Autorità Nazionale Anticorruzione (ANAC), che con deliberazione n. 311 del 12 luglio 2023, ha dettato le "Linee guida in materia di protezione delle persone chesegnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali". Tali linee guida sostituiscono le precedenti disposizioni di cui alla Delibera ANAC n. 469 del 9 giugno 2021. Inoltre, sono in corso di consultazione le nuove Linee Guida di Anac, in materia di whistleblowing, che hanno lo scopo di integrare e completare le disposizioni contenute nella delibera n.311, al fine di armonizzare le pratiche operative e garantire una maggiore coerenza interpretativa tra i vari strumenti e istituti disciplinati dal D.lgs. n.24/2023.

2. Regolamentazione interna

Il Piano per la prevenzione della corruzione e della trasparenza inserito nel PIAO 2023/2025, approvato con deliberazione di Giunta Comunale n. 64 del 12.04.2023 aveva previsto, ai sensi dell'art. 54 bis del D.lgs. 165/2001, rubricato "*Tutela del dipendente pubblico che segnala illeciti*", come modificato dalla L. n. 179/2017, un canale di segnalazione mediante indirizzo di posta elettronica dedicato, con gestione delle segnalazioni da parte del RPCT, prevedendo altresì la prossima predisposizione di apposita piattaforma dedicata per le segnalazioni.

Il Piano per la prevenzione della corruzione e della trasparenza inserito nel PIAO 2024/2026, approvato con deliberazione di Giunta Comunale n. 90 dell'11.04.2024, ha aggiornato la regolamentazione interna dell'Ente adeguandola alle innovazioni normative apportate all'istituto dal D.lgs. n. 24/2023. E' stato dato atto della avvenuta attivazione di piattaforma dedicata "Whistleblowing intelligente" per la gestione delle segnalazioni attraverso un *iter* procedurale definito, con termini certi per l'avvio e la conclusione dell'istruttoria. La piattaforma, accessibile attraverso apposito link nella home page del sito web istituzionale, garantisce la tutela della riservatezza dell'identità del segnalante, consentendogli la verifica dello stato di avanzamento dell'istruttoria, nonché la sicurezza delle informazioni raccolte. La sezione del PTPCT dedicata al "Whistleblowing" delinea le modalità di presentazione di presentazione delle segnalazioni e le misure di protezione garantire al segnalante. La regolamentazione della procedura è stata inserita anche nella Sezione 2 "Valore Pubblico, Performance e Anticorruzione Sezione 2.3. Rischi corruttivi e trasparenza" – Misure di segnalazione e protezione. Whistleblowing" del PIAO 2025/2027, approvato con deliberazione di Giunta Comunale n. 67 del 27.03.2025.

3. Finalità

Con il presente atto il Comune di Piano di Sorrento intende ulteriormente aggiornare la procedura per la presentazione e la gestione delle segnalazioni di condotte illecite (Whistleblowing), ai sensi del D.Lgs. n. 24/2023 ed in conformità alle Linee Guida ANAC approvate con delibera n. 311 del 12 luglio 2023 in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Obiettivo della procedura è dunque, da un lato quello di fornire al segnalante chiare indicazioni operative aggiornate e dall'altro, quello di informarlo circa le forme di tutela e riservatezza che gli vengono riconosciute e garantite in conformità del D.Lgs. 10 marzo 2023 n. 24.

La predetta procedura ha tenuto conto dell'aggiornamento del trattamento dei dati personali in relazione al whistleblowing ed è stata sottoposta, nel rispetto delle Linee Guida di cui alla deliberazione dell'ANAC n. 311 del 12 luglio 2023, alla valutazione d'impatto sulla protezione dei dati DPIA (Data Protection Impact Assessment), in conformità a quanto richiesto dall'art. 35 del GDPR - Regolamento generale sulla protezione dei dati personali.

4. Chi è il whistleblower.

Il whistleblower *("soffiatore di fischietto")* è "*la persona fisica che segnala, divulga o 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, di cui è venuta a conoscenza nell'ambito del proprio contesto lavorativo*".

5. Chi può segnalare (ambito soggettivo).

Sono legittimati a segnalare i soggetti che operano nel contesto lavorativo del Comune di Piano di Sorrento, in qualità di:

- dipendenti, a qualsiasi titolo, del Comune di Piano di Sorrento, a tempo determinato o indeterminato;
- lavoratori autonomi e i titolari di un rapporto di collaborazione che svolgono la propria attività lavorativa presso l'amministrazione comunale;
- lavoratori o i collaboratori di soggetti che forniscono beni o servizi o che realizzano opere in favore del Comune di Piano di Sorrento;
- liberi professionisti e i consulenti, i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso l'amministrazione comunale;
- soggetti con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero di fatto, presso il Comune di Piano di Sorrento.

Non sono prese in considerazione le segnalazioni presentate da altri soggetti, ivi inclusi i rappresentanti di organizzazioni sindacali, in quanto l'istituto del whistleblowing è indirizzato alla tutela della singola persona fisica che agisce in proprio, non spendendo la sigla sindacale. In questo caso le segnalazioni sono archiviate in quanto prive del requisito soggettivo previsto dalla normativa.

6. Quando si può segnalare.

La segnalazione, denuncia o la divulgazione pubblica può essere effettuata in costanza del rapporto di lavoro o di altro tipo di rapporto giuridico, ma anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto giuridico.

Ai sensi dell'art. 3, comma 4 del D.Lgs. n. 24/2023, la tutela dei soggetti segnalanti si applica nei seguenti casi:

a) quando il rapporto giuridico è in corso;
b) quando il rapporto giuridico che qualifica il segnalante e lo lega al Comune di Piano di Sorrento non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
c) durante il periodo di prova;
d) successivamente allo scioglimento del rapporto giuridico, se le informazioni sono state acquisite nel corso dello stesso.

7. Cosa si può segnalare.

Sono oggetto di segnalazione le informazioni sulle violazioni, compresi i fondati sospetti, di normative nazionali o dell'Unione europea che ledono **l'interesse pubblico o l'integrità dell'amministrazione pubblica**. Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse che il whistleblower, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti. Tali elementi possono essere anche irregolarità e anomalie (indici sintomatici) che il segnalante ritiene possano dar luogo ad una delle violazioni previste dal Decreto.

Il legislatore, a tale proposito, ha tipizzato all'art. 2 del Decreto le fattispecie di violazioni:

a) v*iolazioni del diritto nazionale con riferimento a:*

- *illeciti civili;*
- *illeciti amministrativi;*
- *condotte illecite rilevanti ai sensi del D.Lgs. n. 231/2001;*
- *violazioni dei modelli di organizzazione e gestione previsti nel d.Lgs. n. 231/2001 (laddove vigente);*
- *illeciti penali;*
- *illeciti contabili;*

b) *violazioni del diritto dell'Unione europea in riferimento a:*

- *illeciti commessi in violazione della normativa dell'UE – indicata nell'Allegato 1 al D.Lgs.n. 24 del 2023 - relativa 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'UE di cui all'Articolo 325 del TFUE*

- *(lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) specificati nel diritto derivato pertinente dell'Unione europea (regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE);*

- *atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). Sono comprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;*

- *atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione europea nei settori indicati nei punti precedenti.*

Le informazioni possono riguardare sia le violazioni commesse, sia quelle non ancora commesse che il whistleblower, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti.

Possono essere oggetto di segnalazione, divulgazione pubblica o denuncia anche quegli elementi che riguardano condotte volte ad occultare le violazioni.

Non sono ricomprese tra le informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonchè le informazioni acquisite solo sola base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio).

Inoltre, ai sensi dell'art.1, co. 2 del Decreto, **non possono essere oggetto di segnalazione, divulgazione pubblica o denuncia** le seguenti fattispecie:

- le contestazioni, rivendicazioni o richieste legate a un **interesse di carattere personale del soggetto segnalante** o del soggetto che ha sporto una denuncia all'autorità giudiziaria 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;

- le segnalazioni di violazioni laddove **già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali** indicati nella parte II dell'allegato al decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al decreto;

- segnalazioni di violazioni **in materia di difesa nazionale e di ordine e sicurezza nazionale**, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dall'Unione europea.

8. Gli elementi e le caratteristiche delle segnalazioni.

Ai fini dell'applicazione dell'istituto del whistleblowing e del sistema di tutela ad esso connesse, le segnalazioni devono essere rispondenti a determinate caratteristiche, diversamente non potranno essere accordate le tutele previste dal D.Lgs. n. 24/2023.

La segnalazione deve essere il più possibile chiara e circostanziata. Il segnalante deve quindi fornire tutti gli elementi utili alla ricostruzione del fatto, affinché sia possibile accertare la fondatezza di quanto segnalato.

La segnalazione dovrà contenere i seguenti elementi:

- dati anagrafici, incarico/ruolo e recapiti del segnalante;

- circostanza di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;

- chiara e completa descrizione del fatto;

- generalità o altri elementi che consentano di identificare il soggetto o i soggetti che hanno posto in essere i fatti segnalati;

- indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;

- indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;

- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

E' possibile allegare documenti che possono fornire elementi di fondatezza dei fatti segnalati, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), nel caso in cui quanto segnalato non sia adeguatamente circostanziato, può chiedere elementi integrativi al segnalante tramite il canale whistleblowing.

9. Segnalazioni anonime.

La piattaforma whistleblowing consente la presentazione di segnalazioni anonime, ovvero, quelle da cui non è possibile ricavare l'identità del segnalante. Tali segnalazioni **non sono riconducibili alle segnalazioni whistleblowing, sono equiparate a segnalazioni ordinarie** e sono prese in considerazione solo nel caso in cui risultino manifestamente fondate e dalle quali emergano elementi utili per la ricostruzione e l'accertamento di illeciti a vario titolo rilevanti.

Al segnalante anonimo non sono applicabili le misure di protezione e tutela previste dal D.Lgs. n. 24/2023.

Le segnalazioni anonime ricevute sono registrate e conservate **non oltre cinque anni** decorrenti dalla data di ricezione di tali segnalazioni, rendendo così possibile rintracciarle, nel caso in cui il segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito

ritorsioni, a causa di quella segnalazione anonima o denuncia anonima, in tal caso il segnalante può beneficiare della tutela che il Decreto garantisce a fronte delle predette ritorsioni.

10. Le persone autorizzate al trattamento delle segnalazioni.

Al **RPCT** è affidata, ai sensi dell'art. 4, comma 5 del D.Lgs. n.24/2023, la gestione del canale interno, ed è l'unico soggetto individuato quale destinatario delle segnalazioni.

Il Responsabile può avvalersi della collaborazione di personale interno adeguamento formato.

In particolare, i soggetti che gestiscono le segnalazioni devono:

- essere autorizzati al trattamento dei dati personali e quindi essere destinatari di una specifica formazione in materia di privacy sul trattamento dei dati personali;
- assicurare indipendenza e imparzialità;
- ricevere un'adeguata formazione professionale sulla disciplina del whistleblowing, anche con riferimento a casi concreti.

Nel caso in cui il RPCT non possa gestire la segnalazione per conflitto di interessi, la gestione sarà curata, in tutte le sue fasi, dal funzionario con incarico di Vicesegretario.

Il RPCT svolge anche il ruolo di "Custode dell'identità" del segnalante e ha sempre la possibilità di accedere ai suoi dati identificativi per gli usi consentiti o richiesti dalla legge. L'accesso ai dati identificativi del segnalante è motivato e la motivazione viene registrata all'interno della piattaforma informatica. Il segnalante riceve avviso delle motivazioni per le quali i suoi dati identificativi sono stati messi in chiaro.

11. Segnalazioni inviate a un soggetto diverso dal RPCT.

Qualora la segnalazione sia presentata ad un soggetto diverso dal RPCT, laddove il segnalante dichiari di voler beneficiare delle tutele in materia di whistleblowing o tale volontà sia desumibile dalla segnalazione, la stessa sarà considerata *"segnalazione whistleblowing*", andrà trasmessa **entro sette giorni dal suo ricevimento al RPCT,** dandone contestuale notizia al segnalante. Diversamente detta segnalazione sarà considerata come ordinaria.

12. I canali di segnalazione interni ed esterni.

La segnalazione degli illeciti può avvenire utilizzando uno dei seguenti canali:

- **interno** (nell'ambito del contesto lavorativo);

- **esterno** presso ANAC;

- **divulgazione pubblica** (tramite la stampa, i mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);

- **denuncia** all'Autorità giudiziaria o contabile.

La scelta del canale di segnalazione non è rimessa alla discrezione del whistleblower in quanto in via prioritaria è favorito il canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6 del D.Lgs. n. 24/2023, è possibile effettuare una segnalazione esterna.

13. Il canale interno e le modalità di segnalazione.

Le segnalazioni interne possono essere effettuate mediante piattaforma informatica denominata "Whistleblowing Intelligente". Tale piattaforma consente al Responsabile per la Prevenzione della Corruzione e della Trasparenza (RPCT) di ricevere le segnalazioni di illeciti e irregolarità e di dialogare con il segnalante, garantendone la riservatezza in tutte le fasi della procedura.

In particolare, la piattaforma garantisce, 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.

"Whistleblowing Intelligente" utilizza, sia per le segnalazioni, sia per le eventuali comunicazioni successive, un protocollo di crittografia che meglio garantisce sicurezza e confidenzialità tecnologica del processo di segnalazione.

Attraverso il protocollo di crittografia, i dati del segnalante vengono secretati in una sezione dedicata della piattaforma, inaccessibile, in prima istanza, anche al Responsabile del trattamento delle segnalazioni e agli eventuali soggetti autorizzati.

Il segnalante può accedere alla suindicata piattaforma attraverso il link: https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=NXRMRV&dipendente=0 con la possibilità di scegliere l'accesso al canale di segnalazione con identità certificata attraverso lo SPID (preferibile) oppure con identità autodichiarata non obbligatoria.

Il segnalante può monitorare lo stato di avanzamento dell'istruttoria accedendo al sistema di gestione delle segnalazioni ed utilizzando il codice identificativo ricevuto.

Il canale integrato "Whistleblowing Intelligente" consente di raccogliere e gestire:

- segnalazioni scritte
- registrazioni vocali
- richieste di incontri diretti fissati entro un termine ragionevole

Al momento della ricezione della segnalazione, la piattaforma registra la data e l'ora di acquisizione ed assegna un codice identificativo alfanumerico con il quale si può accedere alla segnalazione e dialogare in maniera bidirezionale con il soggetto ricevente. Tutte le informazioni contenute sulla piattaforma sono **crittografate** e possono essere lette solo dal soggetto abilitato alla ricezione della segnalazione il RPCT.

Se il segnalante fornisce all'interno della segnalazione un indirizzo di posta elettronica, la piattaforma gli invierà le notifiche con un link attraverso il quale potrà accedere alla

segnalazione senza dover digitare il codice univoco di segnalazione. Il Comune di Piano di Sorrento non è nella condizione di poter fornire il codice univoco di segnalazione in caso di smarrimento e neanche di generarne uno nuovo.

Il segnalante è tenuto a compilare in modo esaustivo, chiaro, preciso e circostanziato le sezioni del modulo di segnalazione, fornendo le informazioni obbligatorie e il maggior numero possibile di quelle facoltative.

È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni, In particolare è necessario risultino chiare:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione la descrizione del fatto;

- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

È utile anche allegare documenti e file multimediali che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché fornire l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Entro **sette giorni** dal ricevimento della segnalazione verrà data comunicazione al segnalante, tramite piattaforma, della presa in carico della segnalazione.

Per le segnalazioni trasmesse al di fuori della piattaforma Whistleblowing Intelligente, il Comune di Piano di Sorrento garantisce comunque la riservatezza mediante l'acquisizione al protocollo in apposito registro riservato.

La segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e seguenti della legge 241/1990, all'accesso civico generalizzato di cui all'art. 5 co. 2 del d.lgs. 33/2013, nonché all'accesso di cui all'art. 2-undecies co. 1 lett. f) del codice in materia di protezione dei dati personali.

Il canale integrato Whistleblowing Intelligente consente al segnalante di effettuare una registrazione vocale per raccontare la segnalazione in un limite di tempo di venti minuti. La segnalazione così raccolta sarà gestita allo stesso modo della segnalazione acquisita tramite la compilazione dell'apposito form predisposto sul canale integrato Whistleblowing Intelligente.

Il segnalante potrà scegliere, in alternativa, il modulo per la richiesta di incontro al fine di rilasciare verbalmente una segnalazione di condotte illecite. Il RPCT riceve avviso di richiesta di incontro e accede alla piattaforma per comunicare data, ora e luogo dell'incontro. La piattaforma si incaricherà di inviare al segnalante i dati per l'incontro.

Durante l'incontro, previa presentazione dell'informativa del trattamento dei dati personali e delle informazioni necessarie per reperire il testo completo di tale informativa, il RPCT

acquisisce il racconto verbale del segnalante tramite registrazione vocale oppure verbalizzando le dichiarazioni del segnalante.

La registrazione vocale dell'incontro o, in alternativa, il verbale sottoscritto dal segnalante, saranno allegati alla richiesta di incontro andando così a configurare un terzo tipo di segnalazione gestito dal canale unificato di segnalazione utilizzato dal Comune di Piano di Sorrento, che sarà gestita e trattata come le segnalazioni del tipo precedentemente illustrate.

Nella piattaforma informatica sono riportati i link all'informativa specifica sul trattamento dei dati personali (inserire link) e al presente atto organizzativo (inserire link).

14. I canali di segnalazione esterna.

Solo ove si verifichino particolari condizioni specificamente previste dal legislatore i segnalanti possono fare ricorso al canale esterno attivato presso ANAC ai sensi dell'art. 7 D.Lgs. 24/2023 e al ricorrere dei requisiti richiesti dall'art. 6 D.Lgs. 24/2023.

Le modalità di segnalazione all'ANAC sono disponibili nella pagina dedicata sul sito dell'ANAC: https://www.anticorruzione.it/-/whistleblowing. Nell'ottica di consentire di scegliere il canale di segnalazione più adeguato in funzione delle circostanze specifiche del caso, è stata prevista anche la possibilità di effettuare una **divulgazione pubblica**, ma solamente in presenza di particolari condizioni assolutamente residuali e rigidamente disciplinate dall'art. 15 del D. Lgs. 24/2023, come di seguito riportate:

- nel caso in cui ad una segnalazione interna, alla quale il Comune di Piano di Sorrento non ha dato riscontro in merito alle misure previste o adottate per dare seguito alla segnalazione medesima nei termini previsti (90 giorni dalla data dell'avviso di presa in carico o, in mancanza di tale avviso, entro 90 giorni dalla scadenza del termine di sette giorni dalla presentazione della segnalazione), ha fatto seguito una segnalazione esterna ad ANAC la quale, a sua volta, non ha fornito riscontro al segnalante entro termini ragionevoli (90 giorni o, se ricorrono giustificate e motivate ragioni, 180 giorni dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento);

- nel caso in cui è stata già effettuata direttamente una segnalazione esterna all'ANAC, la quale, tuttavia, non ha dato riscontro al segnalante in merito alle misure previste o adottate per dare seguito alla segnalazione medesima entro termini ragionevoli (90 giorni o, se ricorrono giustificate e motivate ragioni, 180 giorni dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento);

- nel caso in cui è stata effettuata direttamente una divulgazione pubblica in quanto, sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze del caso concreto, ritiene che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse: si pensi, ad esempio, ad una situazione di emergenza o al rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richiedono che

la violazione sia svelata prontamente e abbia un'ampia risonanza per impedirne gli effetti;

- nel caso in cui viene effettuata direttamente una divulgazione pubblica poiché, sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze del caso concreto, si ritiene che la segnalazione sul canale interno e/o esterno possa comportare il rischio di ritorsioni oppure possa non avere efficace seguito perché, ad esempio, si eme che possano essere occultate o distrutte prove oppure che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa: si consideri, a titolo esemplificativo, il caso in cui chi riceve la segnalazione di una violazione, accordandosi con la persona coinvolta nella violazione stessa, proceda ad archiviare detta segnalazione in assenza dei presupposti.

Nella divulgazione pubblica, ove il soggetto riveli volontariamente la propria identità non viene in rilievo la tutela della riservatezza, ferme restando tutte le altre forme di protezione previste dal decreto per il whistleblower.

Il decreto riconosce inoltre ai soggetti tutelati anche la possibilità di valutare di rivolgersi alle Autorità nazionali competenti, giudiziarie e contabili, per inoltrare una denuncia di condotte illecite di cui questi siano venuti a conoscenza nel proprio contesto lavorativo.

E' importante sottolineare che per i pubblici ufficiali e gli incaricati di pubblico servizio che hanno un obbligo di denuncia, in virtù di quanto previsto dal combinato disposto dall'art. 331 c.p.p. e degli artt. 361 e 362 c.p., la segnalazione indirizzata al RPCT o ad ANAC, non sostituisce, laddove ne ricorrano i presupposti, quella alla competente Autorità giudiziaria.

15. Modalità di gestione della segnalazione.

a) Esame preliminare della segnalazione ricevuta

Il RPCT provvede ad una prima verifica finalizzata a determinare l'ammissibilità e la ricevibilità della segnalazione, secondo quanto prescritto dal D.Lgs. n. 24/2023.

L'esame preliminare, in particolare, ha lo scopo di accertare da un lato se esistono i presupposti per accordare le tutele al segnalante e, dall'altro, se la segnalazione contiene elementi meritevoli di essere approfonditi in fase istruttoria.

Nel corso del predetto esame viene, in particolare, verificato:

- se il segnalante riveste, o meno, una delle qualifiche indicate al precedente paragrafo 5);

- se la segnalazione rientra nell'ambito delle "***condotte illecite***";

- se le suddette condotte riguardano situazioni di cui il soggetto è venuto a conoscenza nel proprio **contesto lavorativo,** per tale si intendono le attività lavorative, presenti o passate, svolte nell'ambito dei rapporti di rapporti giuridici di cui all'art. 3, co. 3 e 4 del D.Lgs n. 24/2023, attraverso le quali, indipendentemente dalla natura di tale 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 (art. 2, lett. i);

- se la segnalazione consente l'individuazione delle circostanze di tempo e luogo in cui si è verificato il fatto oggetto di segnalazione e, quindi, una descrizione precisa dei fatti oggetto della segnalazione e, ove presenti, anche delle modalità attraverso cui il segnalante è venuto a conoscenza dei fatti;

- se la segnalazione è stata inoltrata "***nell'interesse pubblico e/o nell'interesse dell'integrità della P.A***.", per cui saranno archiviate le doglianze di carattere esclusivamente personale del segnalante o le rivendicazioni.

Resta ferma la possibilità per il RPCT di chiedere alla persona segnalante, ove ritenuti necessari, ulteriori elementi a supporto della propria segnalazione.

In mancanza di uno o più dei suddetti elementi ovvero nei casi di:

- manifesta incompetenza del Comune di Piano di Sorrento sulle questioni segnalate;
- accertato contenuto generico della segnalazione tale da non consentire la comprensione dei fatti;
- segnalazione corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione senza descrizione esaustiva dei fatti e/o elementi essenziali;
- Mancata trasmissione delle integrazioni richieste;

il RPCT **dichiara inammissibile la segnalazione e la archivia**, fornendo al segnalante la motivazione della decisione.

Il sistema automaticamente tiene traccia delle interlocuzioni con la persona segnalante e fornisce informazioni sullo stato di avanzamento dell'iter di esame della segnalazione.

b) Istruttoria e accertamento della segnalazione

Il RPCT, una volta valutata l'ammissibilità della segnalazione, procede all'istruttoria interna effettuando tutte le opportune verifiche, analisi e valutazioni specifiche circa la fondatezza o meno dei fatti segnalati.

Tale attività di accertamento può essere svolta:

- direttamente, acquisendo gli elementi informativi necessari alle valutazioni dall'analisi della documentazione/informazioni già ricevute con la segnalazione;

- attraverso eventuali documenti integrativi richiesti al fine di circostanziare meglio la segnalazione;

- mediante il coinvolgimento degli uffici, in considerazione delle specifiche competenze

tecniche e professionali che risultano necessarie per il caso di specie;

- tramite audizione di eventuali ulteriori soggetti interni.

Nel caso in cui il RPCT si avvalga del supporto specialistico del personale degli uffici, viene comunque garantita la riservatezza del segnalante di cui all'art. 12 del D.lgs n.24/2023.

La comunicazione con il segnalante avverrà unicamente all'interno della piattaforma Whistleblowing Intelligente. Nessun altro mezzo sarà utilizzato. Le richieste di integrazioni/chiarimenti interrompono il conteggio dei tempi di esame della segnalazione. Detti tempi riprendono in automatico alla risposta da parte del segnalante.

La piattaforma consente al soggetto designato alla trattazione della segnalazione di tenere un diario in cui segnare le date e il tipo di attività istruttorie svolte, come ad esempio: l'acquisizione di documentazione; interlocuzioni e altre attività utili al solo fine di accertare l'attendibilità della segnalazione.

*c) **Decisione.***

Una volta completata l'attività di accertamento il RPCT, qualora ravvisi elementi di manifesta infondatezza della segnalazione, dispone l'archiviazione con adeguata motivazione.

Laddove, invece, ravvisi elementi di fondatezza della segnalazione provvede a formale riscontro contenente le risultanze dell'istruttoria condotta ed i profili di illiceità riscontrati, nonché a comunicarlo agli organi preposti interni e/o enti/istituzioni esterne, per i relativi seguiti:

- all'Ufficio Procedimenti Disciplinari (UPD), in quanto competente, per l'esercizio dell'azione disciplinare e l'applicazione delle eventuali sanzioni in relazione alla gravità dei fatti riscontrati (**se si ravvisa un'ipotesi di illecito disciplinare**);

- all'Autorità giudiziaria ordinaria competente (**se si ravvisa un'ipotesi di reato)**, nel rispetto della tutela della riservatezza come previsto dalla normativa. Il segnalante sarà preventivamente informato tramite piattaforma che la sua segnalazione è stata inviata all'Autorità giudiziaria. Nel caso in cui il RPCT provveda all'inoltro della segnalazione alla competente procura, le eventuali successive integrazioni effettuate dal segnalante dovranno essere direttamente trasmesse dal RPCT all'Autorità giudiziaria individuata;

- alla Corte dei Conti (**se si ravvisa l'ipotesi di un illecito contabile**).

Nell'invio ai diversi destinatari, il RPCT mantiene segreta l'identità del segnalante, nei termini e alle condizioni previste dal D.Lgs. n.24/2023 e non rileva nessun fatto o circostanza da cui è possibile risalire all'identità del segnalante.

Nelle comunicazioni con i diversi interlocutori, verrà sempre indicato che si tratta di segnalazione di whistleblowing da trattare nei limiti indicati nel D.Lgs. n. 24/2023.

L’iter dell'esame e verifica della segnalazione viene concluso **entro tre mesi dalla data del ricevimento della segnalazione** e il RPCT, entro tale termine, fa pervenire al segnalante, mediante la piattaforma, apposita **comunicazione di riscontro**, ai sensi dell’art.5, lett. d) del D.Lgs. n. 24/2023. Tale termine non è perentorio, perché può verificarsi che alcuni accertamenti e analisi richiedano tempi maggiori, in tal caso il riscontro alla persona segnalante assume un carattere interlocutorio ed è volto ad informarlo circa lo stato di avanzamento dell’istruttoria da parte del RPCT.

Il RPCT provvede a comunicare alla persona segnalante l’esito finale dell’istruttoria della segnalazione.

E’ sempre possibile per il segnalante ritirare la segnalazione mediante apposita comunicazione da trasmettere attraverso la piattaforma dedicata. In tale specifico caso, gli accertamenti eventualmente già avviati a seguito della segnalazione si arresteranno, salvo si tratti di questioni procedibili d’ufficio.

Il verbale delle risultanze istruttorie sarà redatto direttamente all'interno della piattaforma, evitando così upload e download di file in modo tale da meglio garantire la protezione e riservatezza delle informazioni ivi contenute.

16. La tutela della riservatezza del segnalante.

In conformità a quanto disposto dall’art. 12 del D.Lgs. n. 24/2023, **l'identità della persona segnalante** e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità, **non possono essere rivelate**, senza il consenso espresso della stessa persona segnalante, a persone diverse dai soggetti incaricati della trattazione delle segnalazioni.

Solo in due casi espressamente previsti dal comma 6 del richiamato art.12, per rivelare l’identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione:

- nel **procedimento disciplinare** laddove il disvelamento dell’identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l’addebito disciplinare;

- nei **procedimenti instaurati** in seguito a segnalazioni interne o esterne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

La tutela della riservatezza è assicurata anche in ambito giurisdizionale e disciplinare.

Il divieto di rivelare l’identità del segnalante è riferita non solo al nominativo del segnalante, ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, nella misura in cui il loro disvelamento anche indirettamente, possa consentire l'identificazione del segnalante.

Il trattamento di tali elementi è quindi improntato alla massima cautela, a cominciare dall’oscuramento dei dati qualora per ragioni istruttorie altri soggetti ne debbano essere messi a conoscenza.

La segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e seguenti della legge 241/1990, all'accesso civico generalizzato di cui all'art. 5 co. 2 del d.lgs. 33/2013 nonché all'accesso di cui all'art. 2-undeciesco. 1 lett. f) del codice in materia di protezione dei dati personali.

17. Tutela della riservatezza dell'identità di altri soggetti.

Il D.Lgs. n. 24/2023 estende le tutele della riservatezza dell'identità, oltre ai soggetti di cui al precedente paragrafo 4), anche a quei soggetti che potrebbero essere destinatari di ritorsioni, in ragione del ruolo assunto nell'ambito del processo di segnalazione, divulgazione pubblica o denuncia e/o del particolare rapporto che li lega al segnalante o denunciante, come di seguito riportato:

- al **facilitatore** (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);

- alle **persone** del medesimo contesto lavorativo del segnalante e a lui legate da uno stabile **legame affettivo o di parentela entro il quarto grado**;

- alle **persone** del medesimo contesto lavorativo del segnalante e che hanno con lui un **rapporto abituale e corrente**;

- agli **enti di proprietà** del segnalante o per i quali la stessa persona lavora, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

18. La tutela da ritorsioni.

L'art. 17 del D.Lgs. n.24/2023 prevede, a tutela del whistleblower, il **divieto di ritorsione.** Di seguito viene riportato un elenco esemplificativo e non esaustivo di **condotte ritorsive**:

- licenziamento, sospensione o misure equivalenti;

- retrocessione di grado o mancata promozione;

- mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;

- sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;

- note di demerito o referenze negative;

- adozione di misure disciplinari o di altra sanzione, anche pecuniaria;

- coercizione, intimidazione, molestie o ostracismo;

- discriminazione o comunque trattamento sfavorevole;

- 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;

- mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;

- 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;

- 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;

- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;

- annullamento di una licenza o di un permesso;

- richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La gestione delle comunicazioni delle presunte ritorsioni, anche solo tentate o minacciate, **compete esclusivamente ad ANAC**, alla quale è affidato il compito di accertare se esse siano conseguenti alla segnalazione, denuncia, divulgazione pubblica effettuata.

Le Linee Guida ANAC n. 311 del 12 luglio 2023 indicano le condizioni per l'applicazione della tutela dalle ritorsioni. Le stesse Linee Guida definiscono le modalità attraverso cui il segnalante – o altro soggetto tra quelli sopra indicati - può presentare la comunicazione di ritorsioni all'ANAC. Qualora la comunicazione sulle ritorsioni sia pervenuta a soggetti diversi da ANAC, è necessario che gli stessi la trasmettano per competenza all'Autorità Nazionale Anticorruzione.

In particolare, la tutela è garantita quando la segnalazione, la divulgazione pubblica e la denuncia, effettuate da parte di uno dei soggetti individuati dal legislatore soddisfano alcune condizioni e requisiti, come di seguito specificati:

- i segnalanti o denuncianti devono ragionevolmente credere, anche alla luce delle circostanze del caso concreto e dei dati disponibili al momento della segnalazione, divulgazione pubblica o denuncia, che le informazioni sulle violazioni segnalate, divulgate o denunciate siano veritiere;

- il whistleblower ha agito sulla base di motivi fondati tali da far ritenere ragionevolmente che le informazioni sulle violazioni segnalate, divulgate o denunciate siano pertinenti in quanto rientranti fra gli illeciti considerati dal legislatore;

- vi sia uno stretto collegamento tra la segnalazione, la divulgazione pubblica o la denuncia e il comportamento/atto/omissione sfavorevole subito direttamente o indirettamente dalla persona segnalante o denunciate.

La tutela è riconosciuta anche quando il soggetto ha segnalato, effettuato divulgazioni pubbliche o denunce pur non essendo certo dell'effettivo accadimento dei fatti segnalati o denunciati e/o dell'identità dell'autore degli stessi o riportando anche fatti inesatti per via di un errore materiale.

Inoltre, ai fini della tutela, nessuna rilevanza assumono i motivi personali e specifici che hanno indotto le persone a effettuare la segnalazione, la divulgazione pubblica o la denuncia.

Sono inclusi tra i soggetti che possono comunicare all'ANAC di aver subito ritorsioni anche coloro che avendo un legame qualificato con il segnalante, denunciate o divulgatore pubblico, subiscono ritorsioni in ragione di detta connessione.

Sono escluse dalla possibilità di segnalare le ritorsioni all'ANAC le organizzazioni sindacali e le associazioni di ogni natura. Resta fermo che i rappresentanti sindacali beneficiano, in quanto tali, della possibilità di comunicare all'ANAC ritorsioni, sia se esse sono conseguenza di una segnalazione, denuncia, divulgazione pubblica dagli stessi effettuata in qualità di lavoratori, sia se assumono il ruolo di facilitatori, non spendendo la sigla sindacale, e quindi subiscano ritorsioni per aver fornito consulenza e sostegno alla persona segnalante, denunciante o che ha effettuato una divulgazione pubblica.

Ferme restando le specifiche ipotesi di limitazione di responsabilità, la tutela prevista in caso di ritorsioni viene meno 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 casi di dolo o colpa grave.

Laddove la sentenza di condanna in primo grado dovesse essere riformata in senso favorevole al segnalante nei successivi gradi di giudizio, quest'ultimo potrà ottenere nuovamente la tutela prevista solo a seguito del passaggio in giudicato della pronuncia che accerta l'assenza della sua responsabilità penale per i reati di calunnia e/o diffamazione collegati alla segnalazione.

Solo ove intervenga, in sede giudiziaria, l'accertamento della responsabilità per dolo o colpa grave in merito alla condotta calunniosa o diffamatoria messa in atto attraverso la segnalazione, il Comune di Piano di Sorrento potrà sanzionare disciplinarmente il segnalante nei limiti consentiti dalla natura del rapporto giuridico in essere.

19. Limitazioni di responsabilità penale, civile e amministrativa per chi segnala.

Ai sensi dell'art. 20 del D.Lgs. n. 24/2023 non incorre in alcun tipo di responsabilità civile, penale e amministrativa il segnalante che riveli o diffonda informazioni sulle violazioni coperte dall'obbligo di segreto (diverso da quello di cui all'articolo 1, co. 3, del D.Lgs. n. 24/2023), o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero riveli o diffonda informazioni sulle violazioni che offendono la reputazione della persona coinvolta o denunciata, quando ricorrono le due seguenti condizioni:

- se al momento della rivelazione o diffusione, vi siano fondati motivi per ritenere che la le informazioni siano necessarie per svelare la violazione;

- la segnalazione sia stata effettuata nel rispetto delle condizioni di cui all'art. 16 del D.Lgs. n. 24/2023.

In ogni caso, la responsabilità penale e ogni altra responsabilità, anche di natura civile o

amministrativa, non è esclusa per i comportamenti, gli atti o le omissioni non collegati alla segnalazione, alla denuncia all'Autorità Giudiziaria ordinaria o contabile o alla divulgazione pubblica o che non sono strettamente necessari a rilevare la violazione

20. La tutela dei soggetti coinvolti o persone menzionate nella segnalazione.

Il D.Lgs. n. 24/2023 prevede all'art 12, comma 7 che la tutela dell'identità sia garantita anche ai soggetti coinvolti o alle persone menzionate nella segnalazione, ovvero alla persona alla quale la violazione è attribuita (soggetto segnalato) nel rispetto delle medesime garanzie previste per il segnalante.

A sostegno della persona coinvolta e del suo diritto di difesa, l'art. 12, comma 9 del D. Lgs n. 24/2023 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 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.

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.

21. Conservazione della documentazione inerente alla segnalazione e cancellazione.

Le segnalazioni interne e la relativa documentazione, come previsto dall'art. 14 D.Lgs. 24/2023, sono conservate (*periodo di data retention*) per il tempo necessario al trattamento della segnalazione e comunque **non oltre cinque anni,** a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'art.12 del predetto decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del Regolamento (UE) 2016/679 e 3, comma 1, lettera e), del d.lgs. n.51/2018. Decorso tale termine la predetta documentazione viene cancellata, ad eccezione degli atti e documenti che afferiscono ai procedimenti avviati e alle iniziative assunte dall'Ufficio procedimenti

disciplinari (U.P.D.) (procedimento disciplinare, trasmissione degli atti alle autorità competenti, ecc.) che abbiano avuto origine in tutto o in parte dalla segnalazione.

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

Le modalità di conservazione e le relative misure di sicurezza adottate sono contenute nell'apposita DPIA.

22. Obblighi di sicurezza e trattamento dei dati personali.

La Società Tecnolink S.r.l. è ideatrice e proprietaria della piattaforma informatica Whistleblowing Intelligente in uso presso il Comune di Piano di Sorrento in modalità Software as a Service (SaaS).

Il Comune di Piano di Sorrento è l'unico titolare del trattamento relativo ai dati inerenti alle procedure di whistleblowing. La società Tecnolink S.r.l, nella persona del suo legale rappresentante pro tempore, è stata nominata Responsabile del trattamento dei dati personali *(vedi nomina a responsabile esterno del trattamento di dati personali allegata)*

Il Comune di Piano di Sorrento, nell'ambito di quanto previsto nell'atto di nomina, verifica e controlla le modalità operative con cui il Responsabile assicura il trattamento dei dati personali in piena conformità a quanto previsto dal REGOLAMENTO (UE) 2016/679 in particolar modo per le parti richiamate dalle Linee Guida ANAC in materia di Whistleblowing adottate con delibera n. 311/2023.

L'Ente ha provveduto ad effettuare la specifica valutazione d'impatto (DPIA) sui dati personali derivante dal trattamento del whistleblowing.

La piattaforma Whistleblowing Intelligente consente ai soggetti interessati di trattare i dati personali secondo i principi fondamentali del già citato Regolamento UE, in particolare:

- garantisce il divieto di tracciamento; nel caso in cui l'accesso avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione con la piattaforma;

- garantisce il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione;

- evita il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante.

Le misure tecniche adottate dal fornitore sono riportate nell'allegato 3 del presente documento.

23. Divieto di rinunce e transazioni.

Il Comune di Piano di Sorrento rispetta il divieto di rinunce e transazioni non sottoscritte in sede protetta (giudiziarie, amministrative sindacali) dei diritti e dei mezzi di tutela ivi previsti. Tale previsione risponde all'esigenza di implementare e rendere effettiva la protezione del whistleblower, quale soggetto vulnerabile, nonché degli altri soggetti tutelati, che, per effetto della segnalazione, divulgazione o denuncia, potrebbero subire effetti pregiudizievoli.

Ne consegue, quindi, che non sono validi in primis gli atti di rinuncia e le transazioni, sia integrali che parziali (ad esempio in virtù di accordi o altre condizioni contrattuali), aventi ad oggetto il diritto di effettuare segnalazioni, divulgazioni pubbliche o denunce nel rispetto delle previsioni di legge.

Analogamente, non è consentito imporre al whistlebower, così come agli altri soggetti tutelati, di privarsi della possibilità di accedere a mezzi di tutela cui hanno diritto (tutela della riservatezza, da eventuali misure ritorsive subite a causa della segnalazione, divulgazione pubblica o denuncia effettuata o alle limitazioni di responsabilità conseguenti alla segnalazione, divulgazione o denuncia al ricorrere delle condizioni previste). A maggior ragione tali tutele non possono essere oggetto di rinuncia volontaria.

24. Disposizioni finali e rinvio.

Il Comune promuove un'efficace attività di sensibilizzazione, comunicazione e formazione sui diritti e gli obblighi relativi alla segnalazione degli illeciti, a tutela del pubblico interesse, nell'ambito dei percorsi di formazione sull'anticorruzione e etica pubblica.

Le violazioni degli obblighi previsti dal presente atto sono fonte di responsabilità disciplinare.

Nella sezione "**Valore pubblico, performance e anticorruzione sottosezione rischi corruttivi e trasparenza"** dei prossimi PIAO verrà data indicazione del numero delle segnalazioni whistleblowing ricevute e la relativa fase di lavorazione. Inoltre, tali dati verranno anche riportati nella Relazione annuale del RPCT, di cui all'art.1, comma 14, della legge 190/2012, garantendo la riservatezza dell'identità del segnalante.

Per quanto non espressamente indicato dalla presente procedura, si fa rinvio al D.lgs. n. 24/2023, alle Linee Guida ANAC approvate con Delibera n. 311 del 2023 e al Codice di Comportamento dell'Ente.

Allegato 1

Nomina di Tecnolink Srl quale Responsabile esterno del trattamento

Allegato 2

"Descrizione tecnica e funzionale della piattaforma Whistleblowing Intelligente"

Allegato 3

RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Dati di contatto del Responsabile esterno del trattamento dei dati:

- Sede Legale: Via P. Bagetti, 10 – 10143 Torino
- Numero di telefono: 011 19878715
- Posta certificata: tecnolink@mypec.eu
- Persona di riferimento: Antonio Cappiello
- Indirizzo email: cappiello@anticorruzioneintelligente.it
- Luogo fisico di archiviazione dei dati: UE
- Modalità' di conservazione dei dati: conservazione digitale

MISURE DI SICUREZZA ADOTTATE DAL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

A seguito dell'utilizzo del servizio in cloud Whistleblowing Intelligente https://wb.anticorruzioneintelligente.it/ possono essere acquisiti dati relativi a persone identificate o identificabili.

Cookies

Nessun dato personale degli utenti viene in proposito acquisito dalla piattaforma.
Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.
L'uso di c.d. cookies di sessione, c.d. "tecnici" (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del servizio.

I c.d. cookies di sessione utilizzati evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

ULTERIORE RESPONSABILE DEL TRATTAMENTO

I dati personali raccolti dalla piattaforma https://wb.anticorruzioneintelligente.it/ sono trattati dalla Società:

Interzen Consulting s.r.l., con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680), in persona dell'amministratore delegato pro tempore regolarmente nominata da Tecnolink S.r.l con atto formale come sub responsabile del trattamento dei dati personali.

PIANO DI GESTIONE DEL RISCHIO PRIVACY

Il Responsabile indirettamente e il sub responsabile direttamente attuano le seguenti misure:

- si accertano che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali non tratti tali dati se non è stato istruito in tal senso dal responsabile stesso e vincolato contrattualmente (o ex lege) alla riservatezza/segreto;
- applicano le misure minime di sicurezza ICT per le pubbliche amministrazioni individuate dall'AGID;
- applicano misure tecniche di crittografia dei dati personali, dei documenti e del DB;
- garantiscono la riservatezza e l'integrità adottando strumenti e tecnologie di accesso mediante sistemi di autenticazione forte;
- adottano mezzi che permettono di garantire la continuità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- adottano mezzi che permettono di garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
- adottano delle misure tecniche per la gestione dei log a norma di legge;

PERIODO DI CONSERVAZIONE

I dati personali saranno conservati sino al termine dell'incarico di erogazione del Servizio di "Whistleblowing Intelligente". A cura del Responsabile della gestione delle segnalazioni saranno eliminate le segnalazioni che eccedono il tempo di conservazione indicato in fase di configurazione.

Durante il periodo contrattuale e anche per il mese successivo, il cliente ha la possibilità di scaricare ogni singola segnalazione e/o l'insieme delle segnalazioni in forma tabellare per gli usi che ritiene più opportuni.
Allo scadere del contratto, decorsi 30 giorni nei quali il cliente non ha manifestato formalmente la volontà di rinnovare il servizio, Tecnolink cancellerà definitivamente i dati trattati.

DETTAGLIO MISURE DI SICUREZZA

1° LIVELLO – SISTEMI ESTERNI DI PREVENZIONE	
Scansione online delle vulnerabilità	**Nessus® Essentials: soluzione per la rilevazione delle vulnerabilità di Tenable®, Inc. Nel 2021 Tenable è stato un Software Vendor di Gartner rappresentativo della Vulnerability Assessment.**

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER	
Service Provider	**Microsoft Azure.**
Tipologia di servizio cloud	**Public Cloud**

Certificazioni del cloud service provider	**Consulta la documentazione di conformità di Microsoft Azure.**
Localizzazione dei data center utilizzati	**West Europe (Netherlands)**
Livelli di sicurezza adottati dal service provider	**Operazioni eseguite da Microsoft per proteggere l'infrastruttura di Azure.**
Ridondanza dei dati del service provider	**Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region).**

3° LIVELLO – INFRASTRUTTURA I.T.	
Firewall	**PfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.**
Back-up	**Procedura di back-up delle Virtual Machine:** ● **1. Frequenza: ogni 4 ore.** ● **2. Modalità di archiviazione: ridondanza geografica GRS (GEO-REDUNDANT-STORAGE). Copia dei dati in modo sincrono tre volte all'interno di un'unica posizione fisica nell'area primaria usando l'archiviazione con ridondanza locale. Copia quindi i dati in modo asincrono in un'unica posizione fisica nell'area secondaria. All'interno dell'area**

	secondaria i dati vengono copiati in modo sincrono tre volte usando l'archiviazione con ridondanza locale. ● **3. Area Primaria: West Europe (Netherlands).** ● **4. Area Secondaria : North Europe (Ireland).** ● **5. Retention Backup: 15 giorni.**
disaster recovery	**Procedura di Disaster Recovery delle Virtual Machine:** **1. Modalità: Cross Region Restore.** **2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria).** **3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).**
	RTO (Recovery Time Objective, il tempo necessario per il ripristino del sistema): 2 giorni lavorativi (tempo minimo)
	RPO (Recovery Point Objective, quantità massima di dati - espressa in ore - che l'azienda perde a seguito del verificarsi di un evento disastroso, poiché non rientrati nella normale procedura ciclica di back-up): 4 ore (tempo massimo)

4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	**Antivirus Microsoft Forefront**
Server virtuale	**L'accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.**

5° LIVELLO – CODICE APPLICATIVO	
Sicurezza informatica del produttore	**Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, il produttore ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati della soluzione Whistleblowing Intelligente presso lo STAR Registry (Security, Trust, Assurance, and Risk) della Cloud Security Alliance.** **Visualizza la scheda di qualificazione del Marketplace ACN Cloud** **Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance** **Visualizza la scheda del produttore su Cloud Security Alliance**
Sistema di autenticazione	**Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente** **Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi:** **SPID (Sistema Pubblico di Identità Digitale)**
IP filtering	**Utenti collegati. Possibilità di visualizzare tutti gli utenti autenticati (non i Segnalanti) sulla piattaforma Whistleblowing Intelligente con i seguenti dati: cognome, nome, ruolo, indirizzo IP, ultimo accesso effettuato.**

6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE	
Criptaggio database e documenti	**1. Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decrittazione avviene solo quando viene visualizzato.** **2. Documenti. Criptazione e decriptazione mediante chiave privata.**
Protocollo HTTPS	**L'HyperText Transfer Protocol Secure (over Secure Socket Layer) è un protocollo per la comunicazione su Internet che protegge integrità e riservatezza dei dati scambiati tra la piattaforma e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.**