ATTO ORGANIZZATIVO DI ATTUAZIONE DELLA DISCIPLINA DEL WHISTLEBLOWING

Il presente atto organizzativo stabilisce e regola le modalità operative con cui il Comune di Collegno (d'ora innanzi, per brevità, il Comune) applica l'istituto del Whistleblowing di cui all'art. 54 bis del D.Lgs. 165/2001 e s.m.i., così come disciplinato dal d.lgs. del 10 marzo 2023 n. 24 e in piena conformità alle Linee guida approvate dall'ANAC con Delibera n. 469 del 9 giugno 2021 e dando attuazione al proprio PIAO parte III sezione 2 sottosezione 2.3 "Rischi corruttivi e trasparenza".

1. L'informazione e la formazione

Il Comune promuove la cultura della legalità, anche informando e formando il proprio personale sulla normativa riferita al Whistleblowing, con opportune iniziative da svolgersialmeno annualmente.
Tali momenti informativi/formativi possono essere estesi anche ad altre categorie di soggetti come ad esempio gli amministratori, i consulenti e i collaboratori esterni, gli stagisti e i volontari, i dipendenti di società che hanno rapporti in essere con in nostro Ente.

Utilizzando proprio personale adeguatamente formato, o ricorrendo a società esterne di riconosciuto valore e competenza professionale in ambito Whistleblowing, il Comune fornisce informazioni sull'uso del canale interno di segnalazione, sugli obblighi informativi relativi al trattamento dei dati personali nonché sulle misure di protezione di cui al capo III del d.lgs. n. 24/2023

2. I Soggetti a cui sono riconosciute le tutele in caso di segnalazione, denuncia o divulgazione pubblica

La riservatezza e la tutela da azione ritorsiva sono garantiti, in caso di segnalazione, denunciao divulgazione pubblica, ai seguenti soggetti:

- tutti i dipendenti con un qualsiasi contratto di lavoro in essere
- i collaboratori ed i consulenti con qualsiasi tipologia di contratto o incarico
- i volontari e tirocinanti, retribuiti e non retribuiti
- le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto
- i dipendenti e collaboratori delle imprese fornitrici nel caso in cui la segnalazioneriguardi fatti in cui è coinvolto o che riguardino il Comune.

Per tutti i suddetti soggetti, la tutela si applica anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico.
Le informazioni sulle violazioni devono riguardare comportamenti, atti od omissioni di cui il segnalante o il denunciante sia venuto a conoscenza in un contesto lavorativo.
Le tutele sono garantite anche se il segnalante o il denunciante anonimo successivamente viene identificato.

3. I soggetti tutelati diversi da chi segnala, denuncia o effettua divulgazioni pubbliche nei cui confrontivalgono il divieto di ritorsione e le misure di protezione

Le misure di protezione e il divieto di torsione valgono anche nei confronti dei seguenti soggetti:

- facilitatore, persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del contesto lavorativo e la cui assistenza deve essere mantenuta riservata
- persone del medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica e che sono legate ad essi da uno stabile legameaffettivo o di parentela entro il quarto grado

- colleghi di lavoro del segnalante, denunciante o di chi effettua una divulgazionepubblica, che lavorano nel medesimo contesto lavorativo e che hanno con dettapersona un rapporto abituale e corrente
- enti di proprietà - in via esclusiva o in compartecipazione maggioritaria di terzi - del segnalante, denunciante o di chi effettua una divulgazione pubblica
- enti presso i quali lavora il segnalante, denunciante o chi effettua una divulgazionepubblica
- Enti che operano nel medesimo contesto lavorativo del segnalante, denunciante o dichi effettua una divulgazione pubblica.

4. L'oggetto della segnalazione, denuncia o divulgazione pubblica

Sono oggetto di segnalazione, divulgazione pubblica o denuncia le informazioni sulle violazioni che ledono l'interesse pubblico o l'integrità del Comune di Collegno.

Le informazioni possono riguardare sia le violazioni commesse, sia quelle non ancora
commesse che il whistleblower, ragionevolmente, ritiene potrebbero esserlo sulla base dielementi 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, nonché di informazioni acquisite solo sola base di indiscrezioni o vociferazioni
scarsamente attendibili (cd. voci di corridoio).

Sono meritevoli di segnalazione, invece, tutte quelle situazioni in cui si vanifica l'oggetto o la finalità delle attività poste in essere per la piena realizzazione delle finalità pubbliche, che ne deviino gli scopi o che minino il corretto agire del Comune di Collegno e che si configurano
come:

- Violazioni del diritto nazionale
- Illeciti civili
- Illeciti amministrativi
- Condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001
- Illeciti penali
- Illeciti contabili
- Irregolarità

- Violazioni del diritto dell'UE
- Illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al d.lgs. n. 24/2023 e di tutte le disposizioni nazionali che ne danno attuazione
- Atti od omissioni che ledono gli interessi finanziari dell'Unione Europea
- Atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società

5. La divulgazione pubblica

Con la divulgazione pubblica le informazioni sulle violazioni sono rese di pubblico dominio tramite la stampa o mezzi elettronici o comunque attraverso mezzi di diffusione in grado di raggiungere un numero elevato di persone.

La divulgazione pubblica delle violazioni deve avvenire nel rispetto delle condizioni poste dal legislatore affinché, il soggetto che la effettua, possa poi beneficiare delle tutele riconosciute dal decreto.
La protezione dalle ritorsioni sarà riconosciuta se al momento della divulgazione ricorra una delle seguenti condizioni:
ad una segnalazione interna, a cui il Comune non ha dato riscontro in merito alle misure previste o adottate per dare seguito alla segnalazione nei termini previsti (tre mesi dalla data dell'avviso di di presa in carico o, in mancanza di tale avviso, entro tre mesi 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 (tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento)
la persona ha già effettuato 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 entro termini ragionevoli (tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento) la persona effettua 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
la persona effettua direttamente una divulgazione pubblica poiché sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze del caso concreto, 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, teme 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.

6. La segnalazione anonima

Le segnalazioni anonime, ove circostanziate, per il Comune sono equiparate a segnalazioni ordinarie e in tal caso considerate nei propri procedimenti di vigilanza ordinari.

In ogni caso, il segnalante o il denunciante anonimo che dovesse essere successivamente identificato, può comunicare ad ANAC di aver subito ritorsioni e può beneficiare della tutela che il decreto garantisce a fronte di misure ritorsive .

il comune di Collegno , se riceve una segnalazione anonima, la registra e ne conserva la relativa documentazione non oltre cinque anni decorrenti dalla data di ricezione, rendendo così possibile rintracciarla, nel caso in cui il segnalante comunichi ad ANAC di aver subito misure ritorsive a causa di quella segnalazione o anonima.

7. Segnalazioni con contenuti esclusi dall'applicazione della disciplina sul whistleblowing

Non sono considerate oggetto di segnalazione, divulgazione pubblica o denuncia:
le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di

lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiegopubblico con le figure gerarchicamente sovraordinate
le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrinonel diritto derivato pertinente dell'Unione europea

8. La tutela della riservatezza

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità, non possono essere rivelate senza il consensoespresso della stessa persona segnalante.
Restano ferme le responsabilità disciplinari previste per violazione degli appositi doveri di comportamento e per violazione delle norme sulla tutela dei dati personali.
Il Comune assicura la riservatezza anche della persona coinvolta e citata dal segnalante e nei confronti di eventuali facilitatori o altre persone menzionate a diverso titolo nella segnalazione.

La riservatezza del segnalante e della persona coinvolta o menzionata è garantita anche:

a) nel caso di segnalazioni effettuate in forma orale attraverso linee telefoniche o, in alternativa, sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto con la persona autorizzata a raccogliere tale segnalazione
b) quando la segnalazione viene effettuata con modalità diverse da quelle istituite
c) quando la segnalazione perviene a personale diverso da quello autorizzato al trattamento delle segnalazioni, al quale va in ogni caso trasmessa senza ritardo.

Qualora, per ragioni istruttorie, altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata, i soggetti autorizzati alla gestione della segnalazione provvedono ad oscurare l'identità del segnalante e, nel limite del possibile, anche del segnalato e di eventuali altri soggetti citati ed ogni altra informazione dalla quale sia possibile risalire alla loro identità.
Ciò vale anche nei casi in cui il Comune debba trasmettere la segnalazione ad altra autorità competente.
Il Comune prevede forme di responsabilità disciplinare in capo ai soggetti competenti a gestire le segnalazioni in caso di violazione dell'obbligo di riservatezza dell'identità del segnalante e degli altri soggetti la cui identità va tutelata.

9. Il consenso a rivelare l’identità del segnalante nell’ambito del procedimento disciplinare

L’eventuale disvelamento dell’identità della persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, avverrà sempre con il consenso espresso del whistleblower.

Qualora si rendesse necessario svelare l’identità del segnalante nell’ambito di un procedimento disciplinare originatosi a seguito della segnalazione, il segnalante deve esprimere chiaramente e inequivocabilmente il consenso.

Nel canale interno, il sistema informativo predisposto dal ***il comune di Collegno*** registra e rende visibile data e ora in cui il whistleblower ha accordato il consenso a rivelare la sua identità nell’ambito del procedimento disciplinare. Tale consenso non sarà revocabile.

10. Rivelare l'identità all’autorità giudiziaria o contabile

Laddove l’Autorità giudiziaria e/o contabile per esigenze istruttorie richieda di conoscere il nominativo del segnalante, il responsabile della prevenzione della corruzione e della trasparenza provvede a comunicare l’identità del segnalante, così come previsto dalle disposizioni di legge.

È opportuno precisare che il whistleblower è preventivamente informato e acconsente, attraverso il modulo di segnalazione, all’eventualità che la sua segnalazione potrà essere inviata all’Autorità giudiziaria ordinaria e/o contabile e che questa potrebbe richiedere di conoscere il nome del segnalante.

11. Durata di conservazione e possibilità di accesso alla segnalazione

La segnalazione sarà resa disponibile tanto al segnalante quanto al personale autorizzato per 5anni.
Segnalante e personale autorizzato potranno utilizzare la chat asincrona contenuta nel modulo di segnalazione della piattaforma informatica anche quando l’esame della segnalazione si è già concluso con un esito motivato.

12. Obblighi di sicurezza e trattamento dei dati personali

La Società Tecnolink S.r.l. è ideatrice e proprietaria della piattaforma informatica Whistleblowing Intelligente adottata dal ***il comune di Collegno*** in modalità Software as a Service (SaaS).
La piattaforma WHistleblowing INtelligente è registrata nel cloud marketplace dell'Autoritàper la Cybersicurezza Nazionale (ACN)
https://catalogocloud.acn.gov.it/service/657

Il Comune è l'unico titolare del trattamento relativo ai dati inerentile procedure diwhistleblowing.

La società Tecnolink S.r.l nella persona del suo legale rappresentante pro tempore, è stata nominata Responsabile del trattamento dei dati personali https://www.comune.collegno.to.it/Segnalazioni-Whistleblowing

Il Comune, 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. 469 del 9 giugno 2021.

Accedi al seguente URL per consultare il documento di valutazione dei rischi (DPIA) sul trattamento dei dati personali (Se non ancora è stato redatto il DPIA, si può far riferimento a questo link)
https://docs.google.com/document/d/1wfrWG-f0oyUvX-KO4tDV250x1mRbG34L7djali1TvUg/ edit?usp=sharing

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

- garantire 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 stabilitala 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.

Per conoscere nel dettaglio le misure tecniche adottate dal fornitore e le funzionalità della piattaforma whistleblowing intelligente consulta l'allegato 3 del presente documento.

Il Comune assegna specifici compiti e funzioni connessi al trattamento di dati personali in relazione alle procedure di Whistleblowing. Tali compiti specifici sono attribuiti a persone fisiche, espressamente designate, che operano sotto l'autorità del titolare del trattamento.

Qualsiasi scambio e trasmissione di informazioni inerente le segnalazioni che comportano un trattamento di dati personali, deve inoltre avvenire in conformità al regolamento UE 2018/1725.

13. Diritto degli interessati

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 i diritti che normalmente il GDPR 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 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.

Ulteriori informazioni su questo punto sono reperibili sulla specifica informativa sul trattamento dei dati personali reperibile al seguente link https://www.comune.collegno.to.it/Segnalazioni-Whistleblowing

14. Le ritorsioni dalle quali è tutelato il segnalante

La ritorsione è intesa come 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 alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

Il Comune vigila e interviene nell'ambito di quanto le è consentito, al fine di impedire che possano essere messe in atto condotte ritorsive.
Di seguito 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
- pretesa di risultati lavorativi impossibili da raggiungere nei modi e nei tempi indicati
- valutazione della performance artatamente negativa
- revoca ingiustificata di incarichi
- un ingiustificato mancato conferimento di incarichi con contestuale attribuzione adaltro soggetto
- reiterato rigetto di richieste (ad es. ferie, congedi)
- sospensione ingiustificata di brevetti, licenze, etc.

15. Le condizioni per l’applicazione della tutela dalle ritorsioni

Le tutele sono garantite 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
se 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
deve esserci 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, affinché questi siano considerati una ritorsione e, di conseguenza, il soggetto possa beneficiare di protezione

Le tutele vengono riconosciute 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 inesattiper via di un errore genuino.

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.

16. La perdita delle tutele

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 commessi con la segnalazione.

Solo dove 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 potrà sanzionare disciplinarmente il segnalante nei limiti consentiti dalla natura del rapporto giuridico in essere.

17. La protezione dalle ritorsioni

Le presunte ritorsioni, anche solo tentate o minacciate, devono essere comunicate dal whistleblower esclusivamente ad ANAC e nelle modalità comunicate dalla stessa Autorità, alla quale è affidato il compito di accertare se esse siano conseguenti alla segnalazione, denuncia, divulgazione pubblica effettuata.

Nel caso in cui l'Autorità accerti la natura ritorsiva di atti, provvedimenti, comportamenti, omissioni adottati, o anche solo tentati o minacciati, posti in essere dal Comune, ne consegue la loro nullità e l'applicazione della sanzione amministrativa pecuniaria da 10.000 a 50.000 euro.

Si precisa che l'Autorità considera responsabile della misura ritorsiva il soggetto che ha adottato il provvedimento/atto ritorsivo o comunque il soggetto a cui è imputabile il comportamento e/o l'omissione.
La responsabilità si configura anche in capo a colui che ha suggerito o proposto l'adozione di una qualsiasi forma di ritorsione nei confronti del whistleblower, così producendo un effetto negativo indiretto sulla sua posizione (ad es. proposta di sanzione disciplinare).

Compete all'Autorità giudiziaria (giudice ordinario) adottare tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta posta in essere in violazione del divieto di ritorsioni e la dichiarazione di nullità degli atti adottati.

L'atto o il provvedimento ritorsivo può essere oggetto di annullamento in sede di autotutela da parte del Comune indipendentemente dagli accertamenti di ANAC.

18. Le comunicazioni delle azioni ritorsive

La comunicazione di azioni ritorsive che i soggetti ritengono di aver subito a causa della segnalazione, denuncia o divulgazione pubblica, deve essere inviata esclusivamente all'ANAC, così come previsto dal D.lgs. n. 24/2023, secondo le modalità stabilite dall'Autorità stessa.

Chi ritiene di aver subito una ritorsione non deve trasmettere la comunicazione a soggetti diversi da ANAC, per non vanificare le tutele che il d.lgs. n. 24/2023 garantisce, prima fra tutte, la riservatezza.

Sono inclusi tra i soggetti che possono comunicare ad 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 ad ANAC le organizzazioni sindacali e le associazione di ogni natura. Resta fermo che i rappresentanti sindacali beneficiano, in quanto tali, della possibilità di comunicare ad 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 subiscono ritorsioni per aver fornito consulenza e sostegno alla persona segnalante, denunciate o che ha effettuato una divulgazione pubblica.

Deve esserci uno stretto collegamento tra la segnalazione, la divulgazione pubblica, la denuncia e il comportamento/atto/omissione sfavorevole subito, direttamente o indirettamente, dalla persona segnalante, denunciate o che effettua la divulgazione pubblica, affinché si possa configurare una ritorsione e,, di conseguenza, il soggetto possa così beneficiare di protezione.

È quindi necessario che il segnalante fornisca ad ANAC elementi oggettivi dai quali sia possibile dedurre la consequenzialità tra segnalazione, denuncia, divulgazione pubblica effettuata e la lamentata ritorsione.

Le comunicazioni di ritorsioni connesse ad una segnalazione o denuncia che per errore fossero indirizzate al Comune saranno trasmesse immediatamente ad ANAC, dando contestuale notizia di tale trasmissione al soggetto che ha effettuato la comunicazione. Inoltre, il Comune garantisce la riservatezza dell'identità della persona che ha inviato pererrore la comunicazione di ritorsioni,

19. Limitazioni di responsabilità per chi segnala, denuncia o effettua divulgazioni pubbliche

Così come previsto dal decreto n.24/2023, sono previste limitazioni della responsabilità civile, penale e amministrativa rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni più avanti indicate quando queste sono rivelate all'interno di una segnalazione, denuncia o divulgazione pubblica.
Si tratta di limitazioni che operano al ricorrere di determinate condizioni in assenza delle quali vi sarebbero conseguenze in termini di responsabilità penale, civile o amministrativa.
Le categorie di informazioni alle quali ci si riferisce sono le seguenti:

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

Tuttavia, la limitazione di responsabilità opera solo nei casi in cui ricorrono tutte le seguenti condizioni:

a. l'accesso alle informazioni/documenti oggetto di segnalazioni è avvenuto in modo lecito
b. al momento della rivelazione o diffusione delle informazioni vi siano fondati motivi per ritenere che tali informazioni siano necessarie per far scoprire la violazione. La persona, quindi, deve ragionevolmente ritenere, e non in base a semplici illazioni, che quelle informazioni debbano svelarsi perché indispensabili per far emergere la violazione, ad esclusione di quelle superflue, e non per ulteriori e diverse ragioni
c. la segnalazione, la divulgazione pubblica o la denuncia sia stata effettuata nel rispetto delle condizioni previste dal d.lgs. n. 24/2023 per beneficiare delle tutele (fondato motivo di ritenere che le informazioni sulle violazioni fossero vere e rientrassero tra le violazioni segnalabili ai sensi del d.lgs. n. 24/2023; segnalazioni, interne ed esterne, divulgazioni pubbliche effettuate nel rispetto delle modalità e delle condizioni dettate nel Capo II del decreto

Tutte queste condizioni devono sussistere per escludere la responsabilità. Se soddisfatte, il whistleblower non incorre in alcun tipo di responsabilità civile, penale, amministrativa o disciplinare.

20. Le misure di sostegno

Il Comune darà risalto e pubblicità con ogni mezzo ritenuto idoneo, compreso il canale interno di segnalazione, all'elenco degli enti del terzo settore che stipulano una convenzione con ANAC al fine di offrire sostegno ai segnalanti.

In particolare tali enti, inseriti in un apposito elenco pubblicato da ANAC sul proprio sitoistituzionale, prestano assistenza e consulenza a titolo gratuito:

- sulle modalità di segnalazione
- sulla protezione dalle ritorsioni riconosciuta dalle disposizioni normative nazionali eda quelle dell'Unione europea
- sui diritti della persona coinvolta
- sulle modalità e condizioni di accesso al patrocinio a spese dello Stato

21. Le persone autorizzate al trattamento delle segnalazioni

La responsabilità della corretta applicazione della disciplina sul Whistleblowing ricade sul Responsabile della prevenzione della corruzione e della trasparenza.
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

Il responsabile nomina i collaboratori autorizzati a trattare le segnalazioni di whstleblowing.

22. Il canale Interno di acquisizione e gestione delle segnalazioni

La segnalazione interna viene acquisita dal Comune mediante i canali appositamente predisposti:

- Piattaforma informatica
- Segnalazioni orali
- Incontri diretti fissati entro un termine ragionevole

Per le segnalazioni trasmesse con modalità diverse da quelle sopra menzionate, il Comune garantisce comunque la riservatezza mediante l'acquisizione al protocollo, in apposito registro riservato.

Le segnalazioni whistleblowing possono essere trasmesse al Comune da parte dei soggetti legittimati come indicati dall'art. 3 del d.lgs. n. 24/2023.
Si precisa che il segnalante deve essere necessariamente una persona fisica che ha acquisito leinformazioni segnalate nell'ambito del proprio contesto lavorativo.

Non sono prese in considerazione, pertanto, le segnalazioni presentate da altri soggetti, ivi inclusi i rappresentanti di organizzazioni sindacali, associazioni di qualsiasi natura e genere in quanto l'istituto del whistleblowing è indirizzato alla tutela della singola persona che
agisce in suo nome e per suo conto.

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.

Eventuali segnalazioni in cui il segnalante dichiari espressamente di far riferimento al d.lgs. 24/2023, presentate erroneamente ad un soggetto diverso dal Comune che ritiene di non essere competente ratione materiae, devono essere trasmesse a quest'ultimo entro sette giorni dalla data del suo ricevimento, dandone contestuale notizia della trasmissione alla persona segnalante.
Tali segnalazioni sono considerate "segnalazioni whistleblowing" e pertanto sottratteall'accesso documentale e accesso civico o generalizzato.

Allo stesso modo, eventuali segnalazioni presentate ad un soggetto interno del Comune ma diverso da un soggetto autorizzato a trattare segnalazioni di whistleblowing, devono essere immediatamente inoltrate ad uno dei soggetti

autorizzati, adottando tutte le cautele diriservatezza e impegnandosi a non rivelare a nessuno quanto eventualmente appreso.

23. Segnalazioni acquisite attraverso la piattaforma Whistleblowing Intelligente

Il Comune ha istituito un canale interno denominato "Whistleblowing Intelligente" per la ricezione e gestione delle segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica.

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 segregati in una sezione dedicata della piattaforma, inaccessibile, in prima istanza, anche al Responsabile dei soggetti autorizzati.
Nella piattaforma informatica sono riportati i link all'informativa specifica sul trattamento dei dati personali e al presente atto organizzativo https://www.comune.collegno.to.it/Segnalazioni-Whistleblowing

24. I soggetti che operano nel canale di segnalazione

Nella piattaforma sono autorizzati ad operare i seguenti soggetti:

- Responsabile della prevenzione della corruzione e della trasparenza (accesso tramitelogin)
- Eventuali collaboratori del Responsabile i(tramite login ma con accesso limitato allesole segnalazioni assegnate loro dal dal Responsabile)
- Segnalante (senza necessità di effettuare login) il quale può fare segnalazioni e accedervi successivamente, ma esclusivamente se in possesso del codice univoco di segnalazione rilasciato dal sistema al momento in cui la segnalazione è stata effettuata.

25. Fare una segnalazione

Nella home page del sito istituzionale *https://www.comune.collegno.to.it/home* è inserito il link *https://www.comune.collegno.to.it/Segnalazioni-Whistleblowing* una pagina nella quale si può eccedere al canale interno informatizzato per l'invio delle segnalazioni con identità certificata attraverso lo SPID.
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 ifatti segnalati
È utile anche allegare documenti e file multimediali che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggettipotenzialmente a conoscenza dei fatti.
Al segnalante si richiede un comportamento collaborativo tenendo costantemente aggiornato il Comune in ordine all'evoluzione della propria segnalazione secondo le modalità descritte nel documento richiamato nell'allegato 2: "Descrizione tecnica e funzionale della piattaforma Whistleblowing Intelligente"
All'invio della segnalazione, la piattaforma presenta al segnalante una videata con il codice univoco di segnalazione il quale deve essere acquisito e conservato per ricollegarsi alla piattaforma nei momenti successivi, in modo tale da poter:

- integrare/aggiornare in un secondo momento quanto riportato inizialmente nel modulodi segnalazione
- rispondere ad eventuali richieste di chiarimenti/approfondimenti da parte dei soggettiautorizzati
- verificare l'avanzamento dell'iter di gestione della segnalazione
- esprimere o negare il consenso a rivelare la propria identità nell'ambito del procedimento disciplinare originatosi dalla segnalazione

Il Comune non è nella condizione di poter fornire il codice univoco di segnalazione in caso di smarrimento e neanche di generarne uno nuovo.
E' previsto un meccanismo semplificato per permettere al segnalante di rimanere in contatto con la segnalazione se nel modulo ha inserito un suo recapito di posta elettronica, non necessariamente quello abituale di lavoro.

26. Ricezione della segnalazione

Al momento della ricezione della segnalazione, il sistema registra la data e l'ora di acquisizione; assegna alla segnalazione un numero progressivo e un ID di segnalazione.

Nessuno di questi dati può essere manipolato e nessuna segnalazione può essere cancellataprima della scadenza del tempo di archiviazione previsto in 5 anni.

Contemporaneamente, la piattaforma informa il segnalante e il Responsabile dell'avvenutaricezione della segnalazione.

Il Responsabile è l'unico soggetto allertato ed è il solo autorizzato a prendere in carico lasegnalazione entro 7 giorni dalla data di ricezione.

Il Responsabile prende in carico la segnalazione entrando nella piattaforma ed aprendola. Anche in questo caso la piattaforma aggiorna immediatamente il segnalante dell'avvenuta presa in carico.
Dal momento in cui la segnalazione è stata presa in carico, decorrono i tempi per la chiusuradella segnalazione (90 gg)

27. Esame preliminare

L'esame preliminare 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 meritevolidi essere approfonditi in fase istruttoria.

Il Responsabile o il collaboratore da lui designato all'interno della piattaforma, valuta lasussistenza dei requisiti di ammissibilità.
La segnalazione è considerata inammissibile e viene archiviata in via diretta per almeno unodei seguenti motivi:

- manifesta infondatezza per l’assenza di elementi di fatto riconducibili alle violazioni tipizzate nell’art. 2, co. 1, lett. a) e a giustificare ulteriori accertamenti
- manifesta incompetenza del Comune 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 elementiessenziali

Nei casi in cui quanto segnalato non sia adeguatamente circostanziato, il soggetto autorizzato a trattare la segnalazione può chiedere al whistleblower, all’interno della piattaforma,
elementi integrativi e di chiarimento/precisazione.
Il sistema automaticamente tiene traccia delle interlocuzioni con la persona segnalante e fornisce informazioni sullo stato di avanzamento dell’iter di esame della segnalazione

28. Fase istruttoria

Anche durante la fase istruttoria potranno essere sottoposte al segnalante domande, richieste di integrazioni, chiarimenti e tutto quanto può servire a delineare correttamente i contorni della vicenda segnalata.
La comunicazione con il segnalante avverrà unicamente all’interno della piattaformaWhistleblowing Intelligente. Nessun altro mezzo sarà utilizzato.
La piattaforma consente al soggetto designato alla trattazione della segnalazione di tenere undiario 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.

29. Verbale delle risultanze istruttorie e chiusura della segnalazione

Il verbale delle risultanze istruttorie sarà scritto direttamente all'interno della piattaforma,
evitando upload e download di file così da meglio garantire la protezione e riservatezza delleinformazioni ivi contenute.
L’intero iter di esame e verifica della segnalazione si dovrà concludere entro 90 giorni dalladata di presa in carico.

I possibili esiti dell’esame della segnalazione sono i seguenti:
- archiviata per infondatezza
- inviata all’Ufficio Provvedimenti Disciplinari (UPD)

- inviata all'ANAC
- inviata alla Corte dei conti
- inviata all'Autorità giudiziaria

Al momento della chiusura, il soggetto autorizzato ad esaminare la segnalazione scrive ancheuna breve nota sulle motivazioni riguardo all'esito.
La piattaforma comunicherà prontamente al segnalante esito e motivazione.
Nell'invio ai diversi destinatari, il RPCT avrà cura di mantenere segreta l'identità del segnalante e di non rivelare nessun fatto o circostanza da cui si possa risalire all'identità delsegnalante.
Inoltre, nelle comunicazioni con i diversi interlocutori, dovrà sempre essere indicato che si tratta di segnalazione di Whistleblowing da trattare nei limiti indicati nel decreto 24/2023

30. Il Custode dell'identità digitale del segnalante e l'accesso ai dati

Il Responsabile svolge anche il ruolo di "Custode dell'identità" del segnalante e ha sempre lapossibilità di accedere ai suoi dati identificativi per gli usi consentiti o richiesti dalla legge.
L'accesso ai dati identificativi del segnalante da parte del Responsabile 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 statimessi in chiaro.

31. Le segnalazioni orali

L'ente sta provvedendo ad avviare una valutazione al fine di implementare il servizio nel modo più efficace possibile.

32. Segnalazioni raccolte tramite "Incontri diretti

Questa tipologia di segnalazioni viene raccolta nell'ambito di un incontro diretto - previa presentazione dell'informativa del trattamento dei dati personali e delle informazioni necessarie per reperire il testo completo di tale informativa - tramite un operatore che inserisce la segnalazione nella piattaforma informatica, analogamente a quanto previsto per lesegnalazioni orali sopra descritte.

33. Segnalazioni estrapolate

Il Comune monitora i mezzi attraverso cui possono essere effettuate divulgazioni pubbliche (ad esempio consultando i mezzi di stampa o le piattaforme web e social). Nel caso in cui venga intercettata una di divulgazione pubblica inerente, questa viene registrata/catalogata e conservata, rendendo così possibile un richiamo ad essa da parte del
segnalante ed essere tutelato nel caso in cui subisca ritorsioni in ragione della divulgazione.

34. Il canale esterno di segnalazione

il decreto prevede la possibilità di effettuare una segnalazione attraverso un canale esterno.
L'ANAC è competente ad attivare e gestire detto canale che garantisca, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.
In particolare, la persona segnalante può effettuare una segnalazione esterna se, al momentodella sua presentazione:

a. la persona segnalante ha già effettuato una segnalazione interna e la stessa non haavuto seguito da parte della persona o dell'ufficio designati.

Si fa riferimento ai casi in cui il canale interno sia stato utilizzato ma non abbia funzionato correttamente, nel senso che la segnalazione non è stata trattata entro untermine ragionevole, oppure non è stata intrapresa un'azione per affrontare la Situazione

b. 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:

- alla stessa non sarebbe dato efficace seguito. Ciò si verifica quando, ad esempio, il Responsabile o altro soggetto designato a trattare la segnalazione è coinvolto nella violazione, vi sia il rischio che la violazione o le relative prove possano essere occultate o distrutte, l'efficacia delle indagini svolte dalle
autorità competenti potrebbe essere altrimenti compromessa o anche perché si ritiene che ANAC sarebbe più indicata a affrontare la specifica violazione,
soprattutto nelle materie di propria competenza;

- questa potrebbe determinare il rischio di ritorsione (ad esempio anche come conseguenza della violazione dell'obbligo di riservatezza dell'identità del segnalante).

c. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse. Si pensi, ad esempio, al caso in cui la violazione richieda un intervento urgente, per salvaguardare la salute e la sicurezza delle persone o per proteggere l'ambiente

35. Divieto di rinunce e transazioni

Il Comune si attiene al 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

Allegato 1
“Descrizione tecnica e funzionale della piattaforma Whistleblowing Intelligente”

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

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.

SICUREZZA DEL TRATTAMENTO – PIANO DI GESTIONE DEL RISCHIO PRIVACY

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

- si accerta 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
- applica le misure minime di sicurezza ict per le pubbliche amministrazioni individuate dall AGID
- applica misure tecniche di crittografia dei dati personali, dei documenti e del DB
- garantisce la riservatezza e l'integrità adottando strumenti e tecnologie di accesso mediante sistemi di autenticazione forte
- adotta mezzi che permettono di garantire la continuità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- adotta mezzi che permettono di garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico]
- adotta delle misure tecniche per la gestione dei log a norma di legge
- luogo fisico di archiviazione dei dati: UE
- modalità' di conservazione dei dati, conservazione digitale

Si veda il dettaglio delle misure riportato più avanti

PERIODO DI CONSERVAZIONE

I dati personali saranno conservati sino al termine dell'incarico di erogazione del servizio di "Whistleblowing Intelligente" e comunque per un periodo di tempo non superiore ad anni 5.

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	Consultare la documentazione di conformità diMicrosoft 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 digestione 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	
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.**