

# COMUNE DI SANT'AGNELLO

Città Metropolitana di Napoli

## ATTO ORGANIZZATIVO DI ATTUAZIONE DELLA DISCIPLINA DEL WHISTLEBLOWING

(Approvato con deliberazione di Giunta Comunale n. 146 del 12/12/2023)

### PREMESSA

La disciplina del Whistleblowing risponde all'esigenza di fornire particolare tutela a coloro che, venuti a conoscenza in ragione del loro rapporto di lavoro di fatti o comportamenti illeciti, li segnalino alle autorità competenti. In linea generale, il regime di tutela accordato al segnalante si sostanzia nella garanzia di riservatezza sull'identità dello stesso, nella protezione da eventuali misure ritorsive adottate dall'amministrazione a causa della segnalazione nonché nella qualificazione della segnalazione come giusta causa di rivelazione di un segreto d'ufficio, aziendale, professionale, scientifico, industriale etc.

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.

Da ultimo, 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)". Successivamente, 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)".

## Definizioni:

Si intende per:

- whistleblower (segnalante): il soggetto individuato dalla legge che segnala agli organi legittimati a intervenire fatti o condotte illecite o irregolari commessi in danno dell'interesse pubblico di cui sia venuto a conoscenza in ragione del rapporto di lavoro;
- whistleblowing: istituto che disciplina procedure specifiche volte a far emergere fatti e condotte illecite interne alla PA e a tutelare il whistleblower;
- segnalato: qualsiasi soggetto a cui vengono imputate condotte illecite nell'ambito della segnalazione;
- PTPCT: Piano Triennale di Prevenzione della Corruzione e della Trasparenza;
- RPCT: Responsabile della Prevenzione della Corruzione e della Trasparenza;
- gruppo di lavoro: composto da personale dipendente, individuato con atto formale del RPCT, chiamato a coadiuvare, qualora necessario, il RPCT;
- custode dell'identità del segnalante: soggetto individuato dall'amministrazione che, nei casi normativamente previsti, su esplicita e motivata richiesta, consente al RPCT di accedere all'identità del segnalante.

## **Scopo e finalità**

Il presente documento stabilisce e regola le modalità operative con cui il Comune di Sant'Agnello applica l'istituto del Whistleblowing così come disciplinato dal d.lgs. del 10 marzo 2023 n. 24, (Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali) in conformità alle Linee guida ANAC.

## **L'informazione e la formazione**

Il Comune di Sant'Agnello promuove la cultura della legalità, anche informando e formando il proprio personale sulla normativa riferita al Whistleblowing. 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.

Utilizzando proprio personale adeguatamente formato, o ricorrendo a società esterne di riconosciuto valore e competenza professionale in ambito Whistleblowing, il Comune di Sant'Agnello 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.

## **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, denuncia o 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 segnalazione riguardi fatti in cui è coinvolto o che riguardino il Comune di Sant'Agnello;

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.

## **I soggetti tutelati diversi da chi segnala, denuncia o effettua divulgazioni pubbliche nei cui confronti valgono 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 legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro del segnalante, denunciante o di chi effettua una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo e che hanno con detta persona 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 divulgazione pubblica;
- Enti che operano nel medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica.

## **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 Sant'Agnello.

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, nonché di informazioni acquisite solo sulla 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 devino gli scopi o che minino il corretto agire del Comune di Sant'Agnello e che si configurano come:

- Violazioni del diritto nazionale
- Illeciti civili
- Illeciti amministrativi
- 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.

### **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 l'Ente 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 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.

### **La segnalazione anonima**

Le segnalazioni anonime, ove circostanziate, per l'Ente 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 Sant'Agnello, 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.*

### **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 impiego pubblico 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 rientrino nel diritto derivato pertinente dell'Unione europea

### **La tutela della riservatezza**

L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità, non possono essere rivelate senza il consenso espresso 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 di Sant'Agnello 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:

1. 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
2. quando la segnalazione viene effettuata con modalità diverse da quelle istituite
3. 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 l'Ente 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.

### **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 dall'Ente 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.

### **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.

*Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei Conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.*

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.

### **Durata di conservazione e possibilità di accesso alla segnalazione**

La segnalazione sarà resa disponibile tanto al segnalante quanto al personale autorizzato per 5 anni. 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.

### **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 Comune di Sant'Agnello in modalità Software as a Service (SaaS).

La piattaforma WHistleblowing INTelligente è registrata nel cloud marketplace dell'Autorità per la Cybersicurezza Nazionale (ACN)

<https://catalogocloud.acn.gov.it/service/657>.

Il Comune di Sant'Agnello è l'unico titolare del trattamento relativo ai dati inerenti le 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. Link di collegamento dal sito istituzionale dell'Ente: <https://www.comune.santagnello.na.it/amministrazione/trasparenza/43/93>.

Il Comune di Sant'Agnello 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 particolare 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:

<https://docs.google.com/document/d/1wfrWGF0oyUvXKO4tDV250x1mRbG34L7diali1TvUg/edit?usp=sharing>

La piattaforma Whistleblowing Intelligente consente ai soggetti interessati di trattare i dati personali 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 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

Il Comune di Sant'Agnello 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.

### **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.

### **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 di Sant'Agnello 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 ad altro soggetto;
- reiterato rigetto di richieste (ad es. ferie, congedi);
- sospensione ingiustificata di brevetti, licenze, etc.

### **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 denunciati 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 denunciata, 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 inesatti per 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.

### **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.

### **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 di Sant'Agnello, 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 di Sant'Agnello indipendentemente dagli accertamenti di ANAC.

### **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 associazioni 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 di Sant'Agnello saranno trasmesse immediatamente ad ANAC, dando contestuale notizia di tale trasmissione al soggetto che ha effettuato la comunicazione. Inoltre, il Comune di Sant'Agnello garantisce la riservatezza dell'identità della persona che ha inviato per errore la comunicazione di ritorsioni.

### **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

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;

- B. 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.

### **Le misure di sostegno**

Il Comune di Sant'Agnello 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 sito istituzionale, prestano assistenza e consulenza a titolo gratuito:

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

### **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 eventualmente 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 rende noto i nominativi dei collaboratori autorizzati a trattare le segnalazioni di whistleblowing integrando il presente documento con apposita sezione dedicata.

### **Il canale Interno di acquisizione e gestione delle segnalazioni**

La segnalazione interna viene acquisita dal Comune di Sant'Agnello 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 di Sant'Agnello 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 le informazioni 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 dichiara espressamente di far riferimento al d.lgs. 24/2023, presentate erroneamente ad un soggetto diverso dal Comune di Sant'Agnello 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 sottratte all'accesso documentale e accesso civico o generalizzato.

Allo stesso modo, eventuali segnalazioni presentate ad un soggetto interno al Comune di Sant'Agnello ma diverso da un soggetto autorizzato a trattare segnalazioni di whistleblowing, devono essere immediatamente inoltrate ad uno dei soggetti autorizzati, adottando tutte le cautele di riservatezza e impegnandosi a non rivelare a nessuno quanto eventualmente appreso.

### **Segnalazioni acquisite attraverso la piattaforma Whistleblowing Intelligente**

Il Comune di Sant'Agnello 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 <https://www.comune.sant-agnello.na.it/amministrazione/trasparenza/43/93/> e al presente atto organizzativo.

### **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, nella persona del Segretario Comunale, (accesso tramite login);
- Eventuali collaboratori del Responsabile (tramite login ma con accesso limitato alle sole segnalazioni assegnate loro 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.

### **Fare una segnalazione**

Nella home page del sito istituzionale <https://www.comune.sant-agnello.na.it/> nella sezione Amministrazione Trasparente, sotto sezione "Altri contenuti - Prevenzione della Corruzione"- Segnalazioni di illecito - whistleblower" è inserito il link ad una pagina di presentazione del servizio <https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=4H07EY&dipendente=1> 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 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 deliberazione 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 l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

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 modulo di segnalazione
- rispondere ad eventuali richieste di chiarimenti/approfondimenti da parte dei soggetti autorizzati
- 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.

È 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.

### **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 cancellata prima della scadenza del tempo di archiviazione previsto in 5 anni.

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

Il Responsabile è l'unico soggetto allertato ed è il solo autorizzato a prendere in carico la segnalazione 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 chiusura della segnalazione (90 gg)

### **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 meritevoli di essere approfonditi in fase istruttoria.

Il Responsabile o il collaboratore da lui designato all'interno della piattaforma, valuta la sussistenza dei requisiti di ammissibilità. La segnalazione è considerata inammissibile e viene archiviata in via diretta per almeno uno dei 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 di Sant'Agnello 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

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

### **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 piattaforma Whistleblowing Intelligente. Nessun altro mezzo sarà utilizzato.

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.

### **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 delle informazioni ivi contenute.

L'intero iter di esame e verifica della segnalazione si dovrà concludere entro 90 giorni dalla data 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 anche una 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 del segnalante.

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.

### **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 la possibilità 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 stati messi in chiaro.

### **Segnalazioni estrapolate**

Il Comune di Sant'Agnello 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.

### **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 momento della sua presentazione:

- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito da parte della persona o dell'ufficio designati. Si fa riferimento ai casi in cui il canale interno sia stato utilizzato ma non abbia funzionato correttamente, nel senso che la segnalazione non è stata trattata entro un termine ragionevole, oppure non è stata intrapresa un'azione per affrontare la situazione;
- la persona segnalante ha fondati motivi di ritenere ragionevolmente sulla base di circostanze concrete allegare 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).
- 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

### **Divieto di rinunce e transazioni**

Il Comune di Sant'Agnello 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 whistleblower, 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.

### **La responsabilità del segnalante**

Le tutele del segnalante non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile di cui all'art. 16 co. 3 del D. Lgs n. 24/2023 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

### **Disposizioni finali**

La procedura e le disposizioni individuate nel presente atto potranno essere sottoposti a eventuale revisione, qualora necessario.

### **Clausola di rinvio**

Per tutto quanto non espressamente previsto nel presente atto, si rimanda al D. Lgs n. 24/2023, alle indicazioni fornite da ANAC in materia e alla normativa vigente.

## Responsabile esterno del trattamento dei dati personali

Dati di contatto del Responsabile esterno del trattamento dei dati:

- **Società Tecnolink S.r.l**
- Sede Legale: Via P. Bagetti, 10 – 10143 Torino
- Codice fiscale/P.Iva: 0750410016
- Numero di telefono: 011 19878715
- Posta certificata: [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu)
- Persona di riferimento: Antonio Cappiello
- Indirizzo email: [cappiello@anticorruzioneintelligente.it](mailto: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

## 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 cinque.

## 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	<a href="#"><u>Microsoft Azure.</u></a>
Tipologia di servizio cloud	Public Cloud
Certificazioni del cloud service provider	<a href="#"><u>Consulta la documentazione di conformità di Microsoft Azure.</u></a>
Localizzazione dei data center utilizzati	<a href="#"><u>West Europe (Netherlands)</u></a>
Livelli di sicurezza adottati dal service provider	Operazioni eseguite da Microsoft per <a href="#"><u>proteggere l'infrastruttura di Azure.</u></a>

Ridondanza dei dati del service provider	Archiviazione con ridondanza di zona (Zone <u>Redundancy Storage, ZRS</u> ): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region).
<b>3° LIVELLO – INFRASTRUTTURA I.T.</b>	
Firewall	PfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.
Back-up	<p>Procedura di back-up delle Virtual Machine:</p> <ul style="list-style-type: none"> <li>● 1. Frequenza: ogni 4 ore.</li> <li>● 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.</li> <li>● 3. Area Primaria: West Europe (Netherlands).</li> <li>● 4. Area Secondaria : North Europe (Ireland).</li> <li>● 5. Retention Backup: 15 giorni.</li> </ul>
disaster recovery	<p>Procedura di Disaster Recovery delle Virtual Machine:</p> <ol style="list-style-type: none"> <li>1. Modalità: Cross Region Restore.</li> <li>2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria).</li> <li>3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).</li> </ol>
	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	<p>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.</p> <p><a href="#"><u>Visualizza la scheda di qualificazione del Marketplace ACN Cloud</u></a></p> <p><a href="#"><u>Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance</u></a></p> <p><a href="#"><u>Visualizza la scheda del produttore su Cloud Security Alliance</u></a></p>
Sistema di autenticazione	<p>Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente</p> <p>Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi:</p> <p>SPID (Sistema Pubblico di Identità Digitale)</p>
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	<ol style="list-style-type: none"><li>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.</li><li>2. Documenti. Criptazione e decrittazione mediante chiave privata.</li></ol>
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.

# Descrizione tecnica e funzionale della piattaforma Whistleblowing Intelligente



SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila ad uno dei gestori.

[Maggiori informazioni su SPID](#)  
[Non hai SPID?](#)



A tua garanzia e a garanzia di tutti i tuoi colleghi, puoi effettuare la segnalazione beneficiando delle tutele previste dalla legge, solo se ti identifichi attraverso lo SPID. In questo modo il Responsabile della prevenzione della corruzione sarà certo dell'identità del segnalante e tu non corri il rischio che qualcuno usi abusivamente le tue generalità per sottoporre una segnalazione di condotte illecite. Le tue generalità saranno acquisite automaticamente dal sistema SPID: Nome, Cognome, Data e luogo di nascita, Codice Fiscale e indirizzo di posta elettronica. Attenzione, potrai modificare solo l'indirizzo di posta elettronica, tutti gli altri valori non potranno essere modificati.

Cattura rettangolare

<b>DESCRIZIONE GENERALE DELLA SOLUZIONE</b>	<b>3</b>
<b>CARATTERISTICHE DELL'INFRASTRUTTURA E SICUREZZA APPLICATIVA</b>	<b>6</b>
<b>LIVELLI DI ACCESSO</b>	<b>11</b>
<b>DESCRIZIONE DEI CASI D'USO DEL SISTEMA</b>	<b>11</b>
Autenticarsi	11
Cambiare la password	11
Impostare il funzionamento del sistema	13
Pubblicare i link di accesso per i Segnalanti	13
Accedere alla piattaforma di segnalazione	14
Leggere l'atto organizzativo, le note esplicative e l'informativa sul trattamento dei dati personali	14
Accedere al modulo di segnalazione attraverso il canale specifico (dipendenti/equiparati)	14
Accedere al modulo di segnalazione attraverso il canale generico	15
Creare una segnalazione nel canale specifico (dipendenti/equiparati)	15
Creare una segnalazione nel canale generico	21
Dopo aver inviato la segnalazione	21
Acquisizione della segnalazione da parte del Responsabile	22
Esame dei requisiti essenziali della segnalazione	23
Affidare ad un collaboratore l'esame preliminare	25
Esaminare una segnalazione	25
Richiedere chiarimenti/ integrazioni	26
Integrare la segnalazione e/o rispondere alle richieste di chiarimenti/integrazioni	26
Accedere ai dati relativi all'identità del segnalante	27
Registrare le attività istruttorie e di verifica	27
Scrivere la relazione conclusiva	28
Chiudere la segnalazione	29
Monitorare il processo della singola segnalazione	29
Continuare il dialogo RPC- Segnalante anche quando la segnalazione è chiusa	30
Esprimere il consenso (o negarlo) a rivelare l'identità di segnalante in caso di procedimento disciplinare	30
Creare la reportistica	31
Lavorare con la Dashboard	32
Cambiare il Responsabile della prevenzione della corruzione	35
<b>SERVIZIO DI MANUTENZIONE EVOLUTIVA E NORMATIVA</b>	<b>36</b>

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
 Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
 C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

# DESCRIZIONE GENERALE DELLA SOLUZIONE

Sistema per la gestione delle segnalazioni di condotte illecite e di malamministrazione denominato “Whistleblowing Intelligente”, offerto in modalità Software as a Service (SaaS), conforme alle Linee Guida adottate dall’ ANAC con Delibera n. 469 del 9 giugno 2021 e al decreto legislativo del 10 marzo 2023, n.24 *Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.*

Il servizio è presente nel Marketplace dell’Agenzia per la Cybersicurezza Nazionale, verificabile al seguente link <https://catalogocloud.acn.gov.it/service/657>

“Whistleblowing Intelligente” è sul mercato dal 2016, è stato utilizzato da oltre 150 clienti (ASL, Enti Locali, Camere di Commercio, Aziende pubbliche e Consorzi di bonifica) ed è sottoposto a continua manutenzione evolutiva.

Il sistema permette di utilizzare due canali distinti di ingresso delle segnalazioni, uno per i dipendenti e soggetti equiparati con obbligo di identificazione e, l’altro, senza obbligo di identificazione.

Gli utenti possono accedere alla piattaforma utilizzando sia Personal Computer sia Tablet e sia Smartphone. La connessione avviene con protocollo protetto.

Il sistema permette ai segnalanti di allegare file di ogni tipo (documenti, audio, video).

Particolare cura è stata messa sulla problematica della semplicità d’uso, sia lato segnalante sia lato personale coinvolto nell’esame delle segnalazioni.

Il soggetto responsabile ha a disposizione questo semplice navigatore:



Il segnalante, invece, parte da questa semplice ed essenziale pagina WEB:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

# COMUNE SANT'AGNELLO

Whistleblowing Intelligente



## Collabora anche tu a rendere più efficiente ed integra la tua organizzazione!

Segnala in tutta tranquillità casi di spreco, corruzione, cattiva gestione pubblica.

SI TRATTA DI UN SOFTWARE SICURO E CRIPTATO.  
LA TUA IDENTITÀ RIMARRÀ SEGRETA.

Cattiva segnalazione

Tutti i campi contengono una guida di compilazione per facilitare l'uso del sistema.

E' possibile personalizzare i contenuti delle informazioni (Nome Ente; Stemma o Logo ente; Informativa trattamento dati personali; atto organizzativo) e le policy di amministrazione come i numero giorni minimo per la presa in carico della segnalazione; numero giorni massimo per la conclusione dell'esame della segnalazione.

Il sistema permette di generare report testuali e rappresentazioni grafiche delle principali caratteristiche delle segnalazioni: canale di ingresso; tipologia di illecito segnalato; tempi medi di chiusura.

Il software è stato sviluppato ed è mantenuto tenendo conto di tutti gli aspetti relativi alla sicurezza e alla protezione dei dati personali, in osservanza all'art. 25 del GDPR n. 2016/679 e a quanto indicato in materia di sicurezza del trattamento dei dati dalle Linee Guida adottate dall' ANAC con Delibera n. 469 del 9 giugno 2021 le quali a pagina 2 (il periodo termina a pag.3) così recitano:

*“In questo ambito, i trattamenti di dati personali effettuati dai soggetti obbligati possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett. c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. b) del Regolamento in relazione all'art. 54-bis,) o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (art. 6, § 1, lett. e) e art. 9, § 2, lett. g) e 10 del Regolamento).”*

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Si ricorda che il Segnalante non ha nessun obbligo a segnalare le condotte illecite previste dalla legge sul whistleblowing e, quindi, non è chiamato a risponderne per non averlo fatto.

L'invio della segnalazione, pertanto, esprime la manifestazione di volontà libera, specifica, informata e inequivocabile da parte del segnalante in relazione al trattamento dei dati personali, tanto più che, stabilisce l'ANAC nelle già richiamate Linee Guida, come riportato precedentemente, la base giuridica del trattamento non trova fondamento sul consenso del segnalante, bensì negli obblighi di legge a cui è sottoposto il titolare del trattamento qualora riceva una segnalazione.

**TECNOLINK S.r.l.**

*Sede legale* Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

# CARATTERISTICHE DELL'INFRASTRUTTURA E SICUREZZA APPLICATIVA

## 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.](#)**

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Localizzazione dei data center utilizzati	<u>West Europe (Netherlands)</u>
Livelli di sicurezza adottati dal service provider	Operazioni eseguite da Microsoft per <u>proteggere l'infrastruttura di Azure.</u>
Ridondanza dei dati del service provider	Archiviazione con ridondanza di zona ( <u>Zone Redundancy Storage, ZRS</u> ): 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	<p>Procedura di back-up delle Virtual Machine:</p> <ul style="list-style-type: none"> <li>● 1. Frequenza: ogni 4 ore.</li> <li>● 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.</li> <li>● 3. Area Primaria: West Europe (Netherlands).</li> </ul>

#### TECNOLINK S.r.l.

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
 Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
 C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

	<ul style="list-style-type: none"> <li>● 4. Area Secondaria : North Europe (Ireland).</li> <li>● 5. Retention Backup: 15 giorni.</li> </ul>
<b>disaster recovery</b>	<p><b>Procedura di Disaster Recovery delle Virtual Machine:</b></p> <ol style="list-style-type: none"> <li>1. Modalità: Cross Region Restore.</li> <li>2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria).</li> <li>3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).</li> </ol>
	<p>RTO (Recovery Time Objective, il tempo necessario per il ripristino del sistema): 2 giorni lavorativi (tempo minimo)</p>
	<p>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)</p>

#### 4° LIVELLO – COMPONENTI SOFTWARE

<b>Sistema operativo</b>	<b>Antivirus Microsoft Forefront</b>
--------------------------	--------------------------------------

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
 Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
 C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

**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.

**TECNOLINK S.r.l.**

*Sede legale* Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## 5° LIVELLO – CODICE APPLICATIVO

<b>Sicurezza informatica del produttore</b>	<p>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.</p> <p><u><a href="#">Visualizza la scheda di qualificazione del Marketplace ACN Cloud</a></u></p> <p><u><a href="#">Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance</a></u></p> <p><u><a href="#">Visualizza la scheda del produttore su Cloud Security Alliance</a></u></p>
<b>Sistema di autenticazione</b>	<p>Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente</p> <p>Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi:</p> <p>SPID (Sistema Pubblico di Identità Digitale)</p>
<b>IP filtering</b>	<p>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.</p>

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## 6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE

<b>Criptaggio database e documenti</b>	<p>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.</p> <p>2. Documenti. Criptazione e decrittazione mediante chiave privata.</p>
<b>Protocollo HTTPS</b>	<p>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.</p>

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

# LIVELLI DI ACCESSO

Sono previsti i seguenti livelli di accesso:

- **Responsabile:** può vedere e fare tutto, tranne cancellare le segnalazioni ricevute
- **Collaboratore:** può vedere e agire solo sulle segnalazioni che gli vengono assegnate dal Responsabile
- **Segnalante:** può compilare e sottomettere un modulo di segnalazione e in aggiunta, vedere e integrare le informazioni riferite ad una singola segnalazione. Il sistema non può riconoscere il segnalante anche nel caso in cui egli ha fornito le sue generalità

## DESCRIZIONE DEI CASI D'USO DEL SISTEMA

### Autenticarsi

L'autenticazione per accedere alla piattaforma è richiesta unicamente all'utente Responsabile ed eventualmente ai suoi collaboratori aggiunti in fase di configurazione.

L'autenticazione potrà avvenire con username e password o, in alternativa, attraverso lo SPID. Ai segnalanti non è richiesta l'autenticazione.

### Cambiare la password

Gli utenti hanno a disposizione la funzione "Cambio Password", come mostrato nella figura seguente



The image shows a screenshot of a web application interface. At the top, there is a navigation bar with several menu items: "Segnalazioni", "Dashboard", "Pannello Ente", "Accessi", and "Cambio password". The "Cambio password" item is highlighted with a blue background. Below the navigation bar, there is a form for changing the password. The form consists of three input fields: "Vecchia password:", "Nuova password:", and "Conferma password:". To the right of the "Conferma password:" field, there is a blue button with a white right-pointing arrow.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Impostare il funzionamento del sistema

Il Responsabile è l'unico utente con i permessi per accedere alle funzioni di configurazione facendo clic sul "Pannello Ente" dal menù principale.

Nel Pannello di Ente il Responsabile potrà:

- denominare il proprio ente
- inserire lo stemma o il logo dell'ente
- inserire/modificare l'indirizzo di posta elettronica su cui vuole ricevere gli alert dalla piattaforma
- linkare l'atto organizzativo interno con il quale si disciplina l'istituto del Whistleblowing
- linkare l'informativa sul trattamento dei dati personali
- stabilire il numero di giorni massimo per l'avvio dell'istruttoria della segnalazione dal momento in cui la segnalazione viene acquisita dal sistema
- stabilire il numero di giorni massimo per la chiusura del procedimento dal momento in cui la segnalazione viene acquisita dal sistema
- aggiungere un collaboratore (crea l'utente con nome utente e password ed automaticamente una e-mail viene inviata al collaboratore con le credenziali di accesso)
- rimuovere un collaboratore (automaticamente viene inviato una e-mail di notifica all'utente rimosso)

The screenshot shows the 'Pannello Ente' configuration page in the Whistleblowing Intelligente system. The page is titled 'Whistleblowing Intelligente - Pannello configurazione' and includes a sidebar labeled 'PANNELLO ENTE'. The main content area contains several configuration fields:

- Denominazione Ente (\*): Comune di Prova
- Località: Prova
- Tipologia Ente (\*): Pubblica Amministrazione Territoriale
- Stemma dell'ente: logo-2.png (with 'Choose File' and 'Update Logo' buttons)
- Responsabile: Whistleblowing NO Test utente (with 'Modifica Email' button)
- Attiva il centro di ascolto e di supporto al Whistleblower dell'associazione Libera: SI
- Disciplinare di utilizzo: https://docs.google.com/document/d/18aM649fzsi7OirGok-kZ
- Numero giorni massimo per l'avvio dell'istruttoria (\*): 15
- Numero giorni massimo per la chiusura del procedimento (\*): 60
- Codice di verifica: 12345
- Link Trattamento Dati Personali: https://docs.google.com/document/d/1qzDDpsBGeGEb\_FIU/
- Link accesso dipendenti e soggetti equiparati (identificazione solo tramite SPID): https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=TESTWSNO&dependente=1
- Link accesso senza obbligo di identificazione (a discrezione del RPCT): https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=TESTWSNO&dependente=0

At the bottom of the form, there are buttons for 'Salva', 'Aggiungi Collaboratore', 'Rimuovi Collaboratore', and 'Registro Responsabili'.

## Publicare i link di accesso per i Segnalanti

Il sistema genera automaticamente 2 link di accesso per i segnalanti:

1. per i dipendenti e soggetti equiparati con obbligo di dichiarare le proprie generalità (canale specifico)

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

2. per soggetti che non desiderano dichiarare la propria identità (canale generico)

Il Responsabile rende disponibile il primo link ed, eventualmente (sulla base di una sua autonoma valutazione) il secondo link, affinché siano pubblicati sul sito istituzionale dell'Ente nella pagina indicata da ANAC.

## Accedere alla piattaforma di segnalazione

Per accedere alla piattaforma di Whistleblowing, il segnalante clicca su un link posto nel sito istituzionale dell'ente in una pagina pubblica e, indipendentemente dal canale di accesso prescelto, egli accede ad una pagina iniziale in cui vedrà il nome e lo stemma/logo dell'ente e un chiaro riferimento al Whistleblowing.

## Leggere l'atto organizzativo, le note esplicative e l'informativa sul trattamento dei dati personali

Nella pagina di accesso alla piattaforma, il segnalante potrà consultare sia l'atto organizzativo con il quale l'ente regola l'istituto del whistleblowing sia una pagina di spiegazioni sull'uso del sistema e ai concetti fondamentali del Whistleblowing.

Nel modulo di segnalazione il segnalante trova il link all'informativa sul trattamento dei dati personali predisposto dall'Ente.

## Accedere al modulo di segnalazione attraverso il canale specifico (dipendenti/equiparati)

Dalla pagina di accesso alla piattaforma è possibile cliccare sul pulsante "NUOVA SEGNALAZIONE".

Per l'accesso al modulo di segnalazione, il sistema richiede di acquisire i dati riferiti all'identità del segnalante attraverso lo SPID (nome, cognome, data e luogo di nascita, codice fiscale). In questo modo si ha l'assoluta certezza dell'identità di colui che compie la segnalazione. Con lo SPID, il segnalante si identifica ma non si autentica nella piattaforma e neanche viene stabilita una relazione tra l'identità del segnalante e l'oggetto segnalazione.

## Accedere al modulo di segnalazione attraverso il canale generico

Se il segnalante ha fatto l'accesso al sistema di segnalazione attraverso il link del canale generico, per accedere al modulo di segnalazione non è richiesto l'uso dello SPID.

**TECNOLINK S.r.l.**

*Sede legale* Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

In questo caso, il modulo di segnalazione propone i campi con il quale il segnalante può manifestare le sue generalità (nome, cognome, data e luogo di nascita, codice fiscale), ma non è richiesto l'obbligo di compilazione.

## Creare una segnalazione nel canale specifico (dipendenti/equiparati)

Dopo essersi identificato attraverso lo SPID, il segnalante accede al modulo come presentato nella figura seguente:

### NUOVA SEGNALAZIONE DIPENDENTE

[Clicca qui per leggere l'informativa sul trattamento dei dati personali](#)

#### ATTENZIONE

Per presentare la segnalazione/comunicazione e per effettuare le successive integrazioni deve essere utilizzato unicamente questa piattaforma. Non vanno presentate duplicazioni della stessa segnalazione.

#### Stai compilando questo modulo perchè:

- sei un dipendente di questo ente o soggetto equiparato (dipendente di un ente di diritto privato sottoposto a controllo pubblico; lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore di questa amministrazione pubblica.)
- sei venuto a conoscenza di condotte illecite in ragione del tuo rapporto di lavoro
- sei mosso dall'intento di tutelare l'integrità di questo ente
- sei consapevole delle conseguenze a cui vai incontro in caso di segnalazioni false, rilasciate in mala fede o con intento denigratorio

**E' necessario spuntare le caselle di controllo per poter inviare la segnalazione. Se non metti il segno di spunta su tutti quadratini non sarà visibile il pulsante d'invio.**



Ti ricordiamo le tutele previste dalla legge nei confronti del Whistleblower: "Il pubblico dipendente che ... segnala al responsabile della prevenzione della corruzione e della trasparenza... ovvero all'Autorità nazionale anticorruzione (ANAC), o denuncia all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione. L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC ... " (dall'art.54 bis d. lgs 30/03/2001)

[clicca qui per approfondire](#)

---

**TECNOLINK S.r.l.**

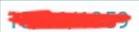
Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Dati relativi al segnalante

I dati relativi alla tua identità e il contenuto stesso della segnalazione saranno criptati e gestiti con il massimo livello di sicurezza. Il Responsabile della Prevenzione della Corruzione ed, eventualmente, un suo collaboratore dichiarato nel disciplinare di regolamentazione dell'Istituto del Whistleblowing in uso nel tuo ente, sono gli unici soggetti che possono decriptare, nei casi previsti dalla legge, le informazioni contenute nel modulo di segnalazione.

Hai ancora qualche dubbio? [Leggi qui](#)

 <span style="color: red;">Dati oscurati nella figura per riservatezza</span>




Qualifica/Ruolo *
Datore di lavoro *

**ATTENZIONE:** Puoi cambiare l'indirizzo e-mail dove ricevere le notifiche sul trattamento della segnalazione. Ti suggeriamo di utilizzare un indirizzo di posta elettronica privato o di crearne uno dedicato con nome di fantasia/fittizio: in questo modo resterai aggiornato in tempo reale e manterrai un grado elevato di sicurezza dei tuoi dati

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

elevato di sicurezza dei tuoi dati.

## Dati e informazioni relative al fatto

Quali fatti possono essere segnalati? 

Durata della condotta illecita \* :

Come sei venuto a conoscenza del fatto? \* :

Allega file multimediale

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Descrizione dei file allegati :

## Soggetti coinvolti nel fatto

Descrizione del fatto \* :

Soggetti dipendenti coinvolti

Soggetti privati coinvolti

Aziende coinvolte

Ulteriori informazioni riguardo i soggetti coinvolti :

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Altre informazioni da segnalare

Altri soggetti che possono fornire informazioni

Indica a quali altri soggetti hai già inviato la segnalazione

- ANAC
- Corte dei Conti
- Autorità Giudiziaria
- Altra autorità

Allega eventuale esposto

Scegli file...

**TECNOLINK S.r.l.**

*Sede legale* Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Indica se hai parlato con qualcuno dell'accaduto \*

Nessuno

Colleghi

Famiglia

Sindacato

Amici

Il mio superiore

Avvocato

Polizia

Carabinieri

Guardia di Finanza

Ispettorato per la Funzione Pubblica

Altro

Dichiarazione. I fatti segnalati sono collegati direttamente o indirettamente a miei interessi \* :

La segnalazione, nel rispetto della tutela della riservatezza della tua identità, può essere trasmessa ad altre Autorità, per i profili di rispettiva competenza.

#### ATTENZIONE

E' necessario spuntare tutte le caselle di controllo che trovi all'inizio di questo modulo per poter inviare la segnalazione.

Annulla

Se le dichiarazioni presentate ad inizio modulo non sono flaggate, il sistema non presenta il pulsante invio, come nel caso della figura.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Il sistema non consente di modificare i campi relativi all'identità del segnalante i quali, lo ricordiamo, sono acquisiti automaticamente da SPID. Unica eccezione è l'indirizzo di posta elettronica: l'utente può cancellare o modificare l'indirizzo e,ai preso in automatico dallo SPID

## Creare una segnalazione nel canale generico

Il modulo di segnalazione del canale generico è uguale a quello del canale specifico, tranne per il fatto di non presentare la parte riprodotta nella figura seguente e per non compilare automaticamente le informazioni relative all'identità del segnalante. Tali informazioni possono anche non essere fornite e ciò non compromette la possibilità di inviare la segnalazione.

### NUOVA SEGNALAZIONE DIPENDENTE

[Clicca qui per leggere l'informativa sul trattamento dei dati personali](#)

#### ATTENZIONE

Per presentare la segnalazione/comunicazione e per effettuare le successive integrazioni deve essere utilizzato unicamente questa piattaforma. Non vanno presentate duplicazioni della stessa segnalazione.

#### Stai compilando questo modulo perchè:

- sei un dipendente di questo ente o soggetto equiparato (dipendente di un ente di diritto privato sottoposto a controllo pubblico; lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore di questa amministrazione pubblica.)
- sei venuto a conoscenza di condotte illecite in ragione del tuo rapporto di lavoro
- sei mosso dall'intento di tutelare l'integrità di questo ente
- sei consapevole delle conseguenze a cui vai incontro in caso di segnalazioni false, rilasciate in mala fede o con intento denigratorio

**E' necessario spuntare le caselle di controllo per poter inviare la segnalazione. Se non metti il segno di spunta su tutti i quadratini non sarà visibile il pulsante d'invio.**

## Dopo aver inviato la segnalazione

Indipendentemente dal canale utilizzato, dopo aver inviato la segnalazione, al segnalante viene presentata a video la seguente pagina:

#### TECNOLINK S.r.l.

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## GRAZIE!

La tua segnalazione ci aiuterà a rendere la nostra organizzazione ancora più trasparente, integra ed efficiente.

Puoi monitorare l'iter del trattamento di questa segnalazione accedendo al [link](#) sottostante o inserendo il codice della segnalazione nella pagina iniziale del sistema di Whistleblowing Intelligente.

Codice segnalazione: **f1b5936b85fcbd6617b03f0fd2a637f9**

**Nota Bene:** nel caso si renda necessario decriptare e risalire ai tuoi dati identificativi verrai avvertito mediante messaggio privato e sull'attuale indirizzo email che hai indicato in fase di registrazione.

È importante monitorare lo stato della segnalazione. Il responsabile della prevenzione della corruzione potrebbe richiedere attraverso la piattaforma ulteriori informazioni. Se non rispondi il procedimento si ferma. Copiati il codice della segnalazione se non hai inserito una casella di posta elettronica a cui il sistema può inviare le notifiche.

Se il segnalante ha lasciato un indirizzo di posta elettronica, riceve anche un alert come mostrato nella figura seguente

## Grazie per il tuo contributo!

Denominazione ente: **Comune di Alba Adriatica**  
Ente utilizzato come esempio

Data della segnalazione: **19/03/2023 18:35:32**

Il codice di verifica della segnalazione è il seguente: **0fe9a4475fb78ea610c44e9f16c3d12a**

[Verifica ora »](#)

## Acquisizione della segnalazione da parte del Responsabile

Quando viene inserita una segnalazione, il Responsabile riceve un avviso dalla piattaforma all'indirizzo di posta elettronica indicato nel pannello di configurazione.

Di seguito è possibile vederne un esempio:

### TECNOLINK S.r.l.

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Nuova segnalazione  Posta in arrivo 

noreply@anticorruzioneintelligente.it

a me ▼

**E' presente una nuova segnalazione!**

Denominazione ente: **Comune di Alba Adriatica**

Data della segnalazione: **19/03/2023 18:35:32**

ID segnalazione: **537**

**[Verifica ora »](#)**

Nessun altro utente riceve questo avviso, anche nel caso in cui il Responsabile abbia provveduto in fase di configurazione a nominare uno o più collaboratori.

Cliccando sul link "Verifica ora", il responsabile sarà indirizzato sulla pagina di login e, dopo essersi autenticato, accede al pannello delle segnalazioni ricevute, una vista ordinata a partire dall'ultima segnalazione inviata con i dati identificativi della segnalazione, tra cui:

- data di creazione
- numero progressivo (assegnato automaticamente dal sistema)
- stato
- canale di invio

Finché il Responsabile non apre la segnalazione, questa non risulterà assegnata e lo stato sarà uguale a "Nuova".

A 5 giorni dalla scadenza dei tempi per eseguire l'esame preliminare, così come determinato in fase di configurazione, il Responsabile riceverà ogni giorno, fino a quando non entra nella segnalazione, un alert in posta elettronica.

## Esame dei requisiti essenziali della segnalazione

Dal momento in cui il Responsabile entra nella segnalazione, la segnalazione viene posta automaticamente nello stato "Esame preliminare".

Il Responsabile vede il contenuto della segnalazione ma i dati relativi al segnalante, se sono stati inseriti, risultano oscurati e si vedranno unicamente degli asterischi se, invece non sono

**[TECNOLINK S.r.l.](#)**

*Sede legale* Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

stati stati inseriti, i relativi campi risulteranno vuoti (caso possibile per segnalazioni inviate tramite il canale in cui non è richiesta l'identificazione tramite SPID)

Nessuna informazione della segnalazione potrà essere modificata e nessuna segnalazione potrà essere eliminata.

Nella pagina dove è visualizzata la segnalazione, è indicata un'area dedicata al Responsabile della prevenzione della corruzione articolata in diverse sub aree, la prima delle quali è denominata "Analisi Preliminare".

In questa sub area, il RPC è guidato nell'attività di verifica dei requisiti essenziali della segnalazione, come mostrato nella figura seguente:

### Requisiti essenziali ×

**ATTENZIONE**  
Se non scegli nessuna opzione, cliccando Salva la segnalazione non verrà considerata come segnalazione di Whistleblowing. Clicca Annulla se vuoi fare la valutazione in un altro momento.

Il segnalante riveste la qualifica di 'dipendente pubblico' o equiparato

La segnalazione ha ad oggetto condotte illecite

Il segnalante è venuto a conoscenza di tali 'condotte illecite' 'in ragione del proprio rapporto di lavoro'

La segnalazione è stata effettuata 'nell'interesse all'integrità della pubblica amministrazione'

Dopo aver valutato i requisiti essenziali della segnalazione, il Responsabile può decidere di continuare con l'esame preliminare o assegnare ad un collaboratore tale attività, nel caso abbia aggiunto collaboratori nella fase di impostazione.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Affidare ad un collaboratore l'esame preliminare

Attraverso l'apposito pulsante, il Responsabile può assegnare l'esame della segnalazione ad un collaboratore tra quelli registrati in fase di impostazione, come mostrato nella figura di esempio riportata qui di seguito:



**Assegna segnalazione**

Assegna a:

✓ Scegli...  
Celeste Maria

Annulla Salva

## Esaminare una segnalazione

Se il Responsabile ha assegnato la segnalazione ad un collaboratore, egli riceverà un alert in posta elettronica; dopo essersi autenticato, il collaboratore vedrà la lista delle segnalazioni a lui assegnate a partire dall'ultima assegnata.

L'assegnatario della segnalazione (Responsabile o Collaboratore), entrando nella segnalazione potrà operare nell'area dedicata al Responsabile della Prevenzione della Corruzione ed essere guidato nel compiere l'esame preliminare attraverso la seguente lista di controllo:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Esito esame preliminare

### ATTENZIONE

Se non scegli nessuna opzione, cliccando su Salva la segnalazione verrà considerata idonea e pronta per l'istruttoria. Clicca Annulla se vuoi completare l'esame preliminare in un altro momento

- Manifesta mancanza di interesse all'integrità della pubblica amministrazione
- Manifesta incompetenza dell'ente sulle questioni segnalate
- Manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti
- 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

Annulla

Salva

## Richiedere chiarimenti/ integrazioni

Colui che ha in esame la segnalazione, può chiedere al segnalante chiarimenti e integrazioni entrare nell'area "Comunicazioni": una chat asincrona che permette la comunicazione tra assegnatario della segnalazione e segnalante.

Il sistema si occupa di inviare un alert nella casella di posta elettronica del segnalante se indicata nel modulo di segnalazione.

Al momento in cui l'assegnatario invia un messaggio al segnalante, il sistema cambia lo stato della segnalazione in "In attesa di risposta" e sospende il conteggio del tempo in riferimento ai termini dell'esame preliminare.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Integrare la segnalazione e/o rispondere alle richieste di chiarimenti/integrazioni

Il segnalante può integrare la segnalazione precedentemente inviata e/o rispondere ad eventuali richieste da parte di colui che esamina la segnalazione.

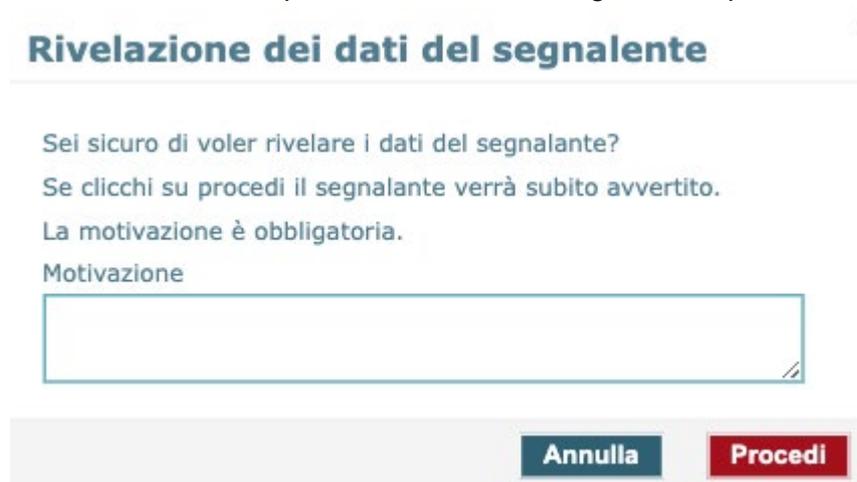
Per accedere alla segnalazione, il segnalante può o cliccare sul link che riceve se ha indicato nel modulo di segnalazione un indirizzo di posta elettronica, oppure rientrare nella pagina di accesso alla piattaforma di whistleblowing e digitare il Codice Univoco di Segnalazione che il sistema gli ha fornito al momento dell'invio della segnalazione stessa.

Nel caso di alert in posta elettronica, il messaggio non conterrà nessun riferimento al contenuto della segnalazione.

Quando il segnalante risponde ad un messaggio di colui che sta esaminando la segnalazione, il sistema ripristina automaticamente lo stato in cui era la segnalazione prima del messaggio da parte del Responsabile/Collaboratore e riprende il conteggio dei termini.

## Accedere ai dati relativi all'identità del segnalante

Solo il RPC può accedere ai dati relativi all'identità del segnalante cliccando sul pulsante "Rivela Identità". Si apre una finestra di dialogo come riportato nella figura seguente



The screenshot shows a dialog box with the following content:

- Rivelazione dei dati del segnalante**
- Sei sicuro di voler rivelare i dati del segnalante?
- Se clicchi su **procedi** il segnalante verrà subito avvertito.
- La motivazione è obbligatoria.
- Motivazione
- A text input field for the motivation.
- Buttons: **Annulla** (blue) and **Procedi** (red).

Il segnalante sarà immediatamente avvertito con un messaggio in posta elettronica (se ha lasciato il suo indirizzo) oppure potrà leggere il messaggio nella chat asincrona al primo accesso alla segnalazione dopo che il Responsabile ha messo in chiaro i suoi dati identificativi.

Per meglio proteggere l'identità del segnalante, il Responsabile ha la possibilità di cliccare sul pulsante "Oscura Identità" in modo da non renderne visibile i dati. Anche in quest'ultimo caso il segnalante sarà avvertito via mail e comunque troverà il messaggio nella chat asincrona riferita alla segnalazione.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Registrare le attività istruttorie e di verifica

L'esaminatore della segnalazione ha a disposizione un'area in cui annotare le attività istruttorie e di verifica svolte in relazione a quella specifica segnalazione, come mostrato nella figura seguente.

### Attività istruttoria e di verifica

Contenuto segnalazione già noto all'ente:	<input type="text" value="Sceali..."/>
Gravità del fatto segnalato:	<input type="text" value="Sceali..."/>
Priorità di trattamento:	<input type="text" value="Sceali..."/>
Diario:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">Annota qui data e attività eseguita</div>

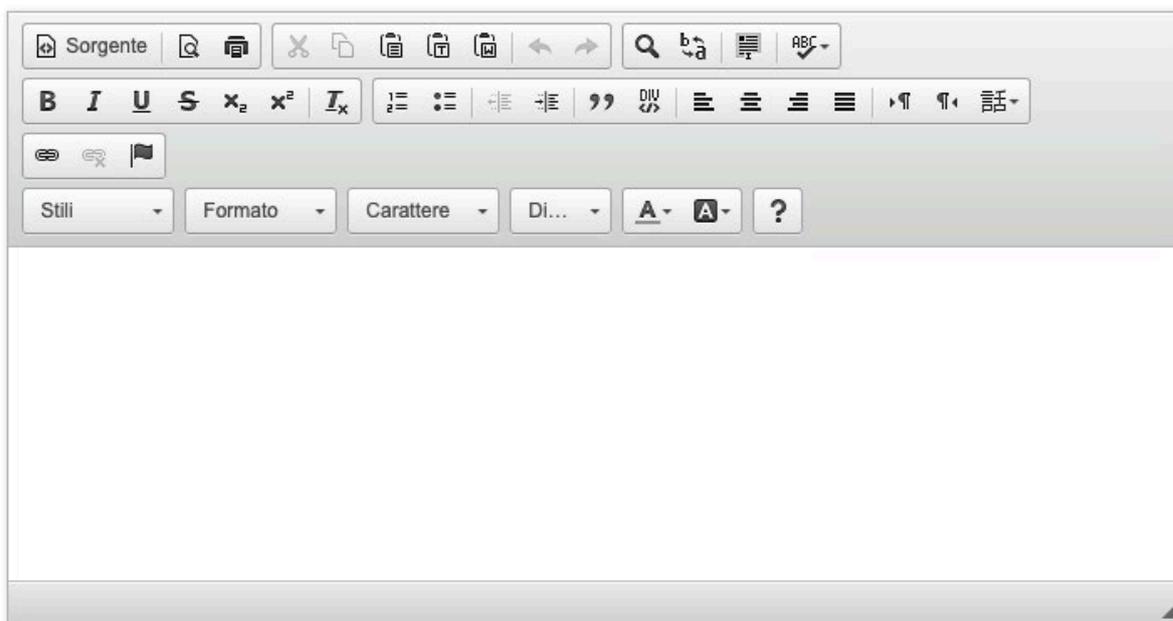
## Scrivere la relazione conclusiva

Al fine di evitare upload e download di file, con il rischio di compromettere la segretezza dei contenuti della segnalazione e dell'identità del segnalante, così come specificato da ANAC nelle linee guida del giugno 2021, all'interno della piattaforma e in relazione alla singola segnalazione, l'esaminatore ha a disposizione un editor di testo completo per scrivere la relazione delle risultanze istruttorie., come di seguito mostrato

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Risultanza Istruttorie:



## Chiudere la segnalazione

Quando l'esaminatore ritiene di aver concluso la verifica della segnalazione, può chiuderla cliccando sull'apposito pulsante. Il sistema mostrerà una finestra di dialogo come di seguito illustrato:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## Chiusura segnalazione x

Chiuso per:

Archiviato per infondatezza

UPD

ANAC

Corte dei conti

Autorità giudiziaria

Altro

Note di chiusura:

Non sono stati riscontrati elementi di conferma dei fatti  
elementi di

Annulla

Salva

Cliccando su salva, il sistema invierà un messaggio al segnalante riportando il tipo di chiusura della segnalazione e le motivazioni sintetiche, sempre che il segnalante abbia inserito un indirizzo di posta elettronica nel modulo di segnalazione. In caso contrario, il segnalante vedrà la sua segnalazione in stato "Chiuso" al primo accesso alla segnalazione e potrà leggere le motivazioni.

## Monitorare il processo della singola segnalazione

Il RPC ha la possibilità, per ogni segnalazione ricevuta, di ricostruire la cronologia delle azioni svolte, così come mostrato nella figura che segue:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Log del documento claims/incidente.php?idIncidente=534								
wb.anticorruzioneintelligente.it/workflow/showLog.php?docId=528								
» Log del documento								
Log delle azioni relative al documento "claims/incidente.php?idIncidente=534"								
Data e ora	Nome file	Dimensione	Processo	Stato iniziale	Stato destinazione	Utente	Azione	Motivazione
09/03/2023 16:16:53	claims/incidente.php?idIncidente=534	0 B	Anticorruzione		Nuovo	Importazione Automatica	<b>IMMESSO</b>	
09/03/2023 16:18:53	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	Nuovo	Esame preliminare	Test utente whistleblowing NO	<b>STATO CAMBIATO</b>	
09/03/2023 16:23:38	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	Esame preliminare	Nuovo	Test utente whistleblowing NO	<b>STATO CAMBIATO</b>	
09/03/2023 16:23:45	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	Nuovo	Esame preliminare	Test utente whistleblowing NO	<b>STATO CAMBIATO</b>	
09/03/2023 16:24:26	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	Esame preliminare	In attesa di risposta	Test utente whistleblowing NO	<b>STATO CAMBIATO</b>	
09/03/2023 16:34:21	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	In attesa di risposta	In attesa di risposta	Test utente whistleblowing NO	<b>DATI ANAGRAFICI RIVELATI</b>	
09/03/2023 16:35:47	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	In attesa di risposta	Chiuso	Test utente whistleblowing NO	<b>STATO CAMBIATO</b>	
09/03/2023 16:36:22	claims/incidente.php?idIncidente=534	0 B	Anticorruzione	Chiuso	Chiuso	Test utente whistleblowing NO	<b>DATI ANAGRAFICI OSCURATI</b>	
» Chiudi								

## Continuare il dialogo RPC- Segnalante anche quando la segnalazione è chiusa

Sia il segnalante sia il RPC hanno la possibilità di utilizzare la chat in relazione ad una specifica segnalazione anche quando la segnalazione è già in stato "Chiuso".

Per inviare e/o leggere messaggi in chat valgono le stesse regole di quando la segnalazione non è in stato "Chiuso".

## Esprimere il consenso (o negarlo) a rivelare l'identità di segnalante in caso di procedimento disciplinare

Nel corso di un procedimento disciplinare originato da una segnalazione, si potrebbe rendere necessario, per il proseguimento del procedimento, rivelare il nome del segnalante.

Il segnalante pertanto, deve esprimere in modo inequivocabile il suo consenso.

Il sistema presenta al segnalante ogni volta che egli entra nella segnalazione, un avviso come di seguito riportato:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

## STATO DELLA SEGNALAZIONE: **ESAME PRELIMINARE**

### ATTENZIONE

Se la tua segnalazione ha dato origine ad un procedimento disciplinare, potrebbe determinarsi la necessità di rivelare la tua identità anche alla persona segnalata, pena l'interruzione del procedimento stesso. Il RPCT può rivelare la tua identità solo dietro tuo esplicito consenso. Clicca sul pulsante se vuoi consentire al RPCT di rivelare la tua identità nel corso del procedimento disciplinare

ACCONSENTO

**CONSENSO NON ACCORDATO.** Ti ricordiamo che puoi rivedere la tua scelta premendo nuovamente sul pulsante "Acconsento" oppure ancora "Scelta ancora non fatta" a seconda delle diverse opzioni a disposizione del segnalante

Cliccando sul pulsante "ACCONSENTO", il sistema mostra questa finestra di dialogo:

### Gestione consenso

#### ATTENZIONE

Questo pulsante è visibile solo al Segnalante. Se acconsenti, la tua identità potrà essere resa nota nell'ambito del procedimento disciplinare nei confronti delle persone segnalate. In caso contrario, l'Ente potrebbe essere nelle condizioni di non poter avviare o portare a termine il procedimento disciplinare. L'eventuale scelta 'non Acconsento' può essere modificata in un secondo momento.

Annulla

Non acconsento

Acconsento

Cliccando sul tasto non acconsento, il segnalante ha, comunque, la possibilità di cambiare idea in futuro e cliccare sul tasto "Acconsento". Quando, invece, fornisce il suo consenso cliccando sull'apposito tasto, non avrà più la possibilità di ritirare il consenso già espresso. Il sistema rende visibile al segnalante e all'esaminatore della segnalazione se il consenso è stato fornito o negato, registrando data e ora di quando tale scelta è stata effettuata.

## Creare la reportistica

Il RPC ha la possibilità di filtrare le segnalazioni ricevute utilizzando uno o più dei seguenti criteri:

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)

Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)

C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

Ricerca segnalazione

<b>Id segnalazione da:</b>	<input type="text"/>	<b>Id segnalazione a:</b>	<input type="text"/>
<b>Data creazione da:</b>	<input type="text"/>	<b>Data creazione a:</b>	<input type="text"/>
<b>Stato segnalazione:</b>	Istruttoria	<b>Assegnato a:</b>	-- Scegli --
<b>Progressivo da:</b>	<input type="text"/>	<b>Progressivo a:</b>	<input type="text"/>
<b>Dipendente/Esterno:</b>	Esterno	<b>Ente in cui si è verificato il fatto:</b>	<input type="text"/>
<b>Periodo/Data:</b>	<input type="text"/>	<b>Luogo fisico in cui si è svolto:</b>	<input type="text"/>
<b>Descrizione del fatto:</b>	<input type="text"/>	<b>Tipo autenticazione da:</b>	<input type="text"/>
<b>Tipo autenticazione a:</b>	<input type="text"/>	<b>Priorità di trattamento:</b>	-- Scegli --
<b>Diario:</b>	<input type="text"/>		

» Cerca » Esporta in Excel » Segnalazioni assegnate a me

Nell'esempio riportato nella figura precedente, si è voluto filtrare l'elenco delle segnalazioni utilizzando il criterio dello stato della segnalazione (Istruttoria) e il canale di accesso (soggetto esterno = canale generico). Di seguito viene riportato esempio di cosa restituisce il sistema:

» Cerca » Esporta in Excel » Segnalazioni assegnate a me

Id segnalazione	Data creazione	Stato segnalazione	Assegnato a	Progressivo	Dipendente/Esterno	Ente in cui si è verificato il fatto	Periodo/Data	Luogo fisico in cui si è svolto	Descrizione del fatto	Tipo autenticazione	Priorità di trattamento	Diario Op.
504	17/03/2022	Istruttoria	Test utente whistleblowing NO	136	Esterno	tetst	test	test	rhtejkrshhkjwkhkhkj			<input type="text"/>
481	12/10/2021	Istruttoria	Test utente whistleblowing NO	129	Esterno	test	test	test	hdfkjhgkjdsfghkjshkjdsfgh			<input type="text"/>
476	07/10/2021	Istruttoria	Test utente whistleblowing NO	127	Esterno	erwtwert	rewt	fghfd	sdfgg			<input type="text"/>
475	07/10/2021	Istruttoria	Test utente whistleblowing NO	126	Esterno	dsfadf	sadfsaf	sdf	sdfs			<input type="text"/>
470	06/10/2021	Istruttoria	Test utente whistleblowing NO	121	Esterno	retew	ertwt	ertw	ewrtwetr			<input type="text"/>
469	06/10/2021	Istruttoria	Test utente whistleblowing NO	120	Esterno	retwt	ewrtwet	ertwt	ewrqrgwerwr		Alta	<input type="text"/>

E' così possibile ottenere l'elenco delle segnalazioni suddivise per tipologia, stato di avanzamento nel processo, ecc. L'elenco filtrato delle segnalazioni può essere esportato in excel per gli usi consentiti.

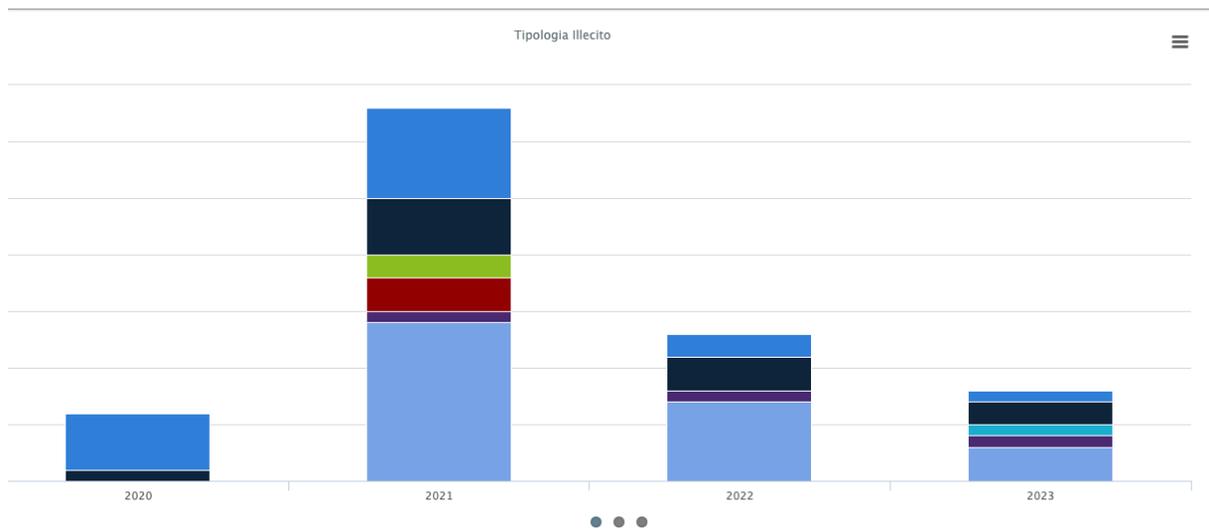
## Lavorare con la Dashboard

Il sistema mette a disposizione tre pannelli di controllo e altri sono facilmente creabili. E' possibile filtrare le segnalazioni sulla base di un intervallo di tempo e osservarne la distribuzione rispetto a:

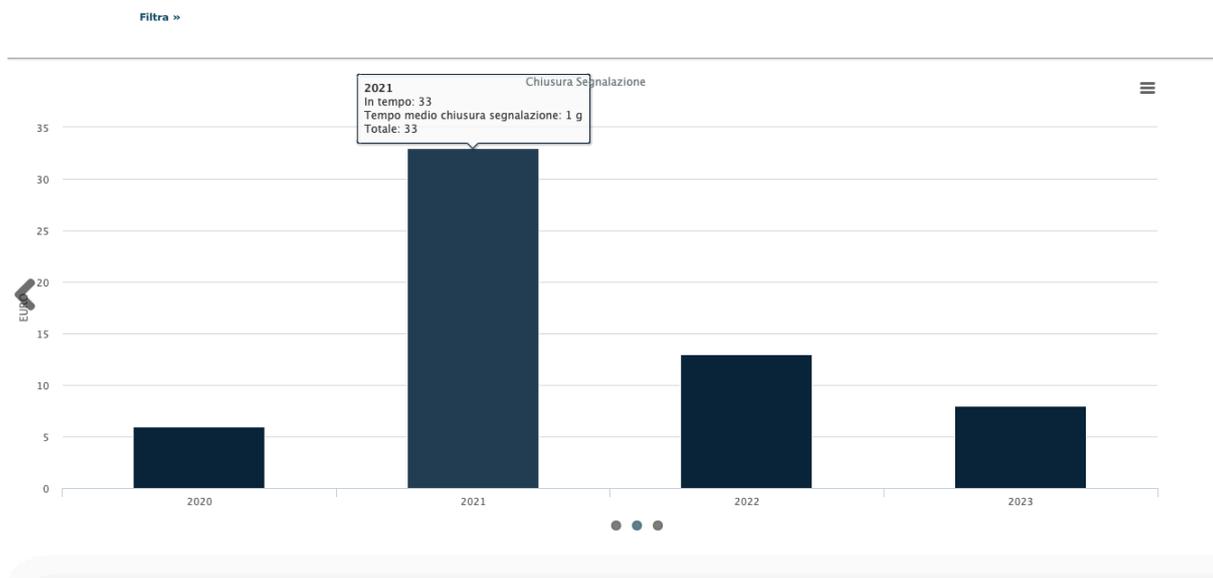
- Tipologia di illecito

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
 Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
 C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato



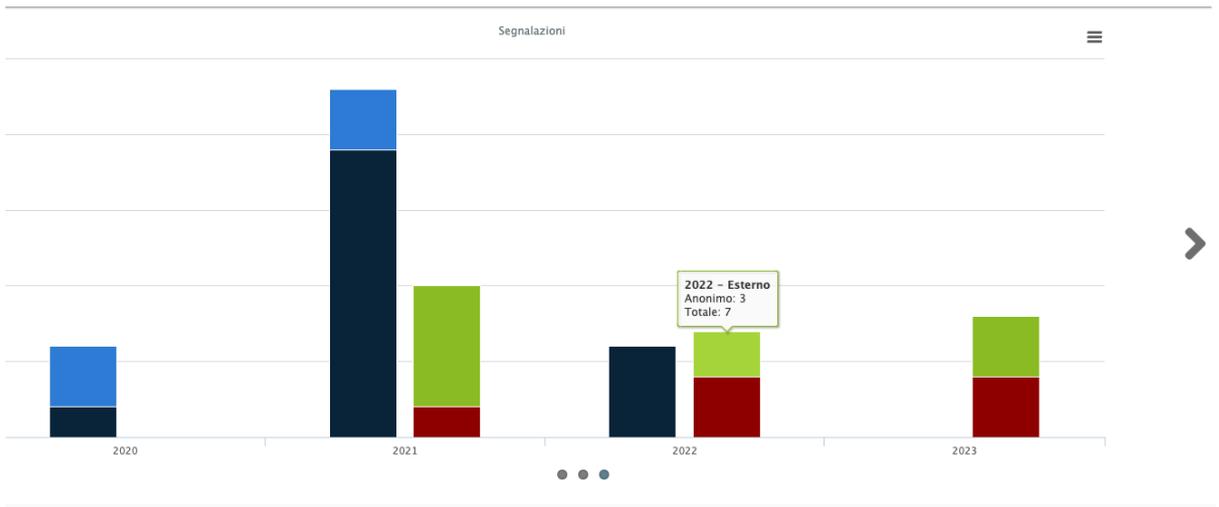
- tempo di chiusura delle segnalazioni



- Per canale di ricezione

**TECNOLINK S.r.l.**

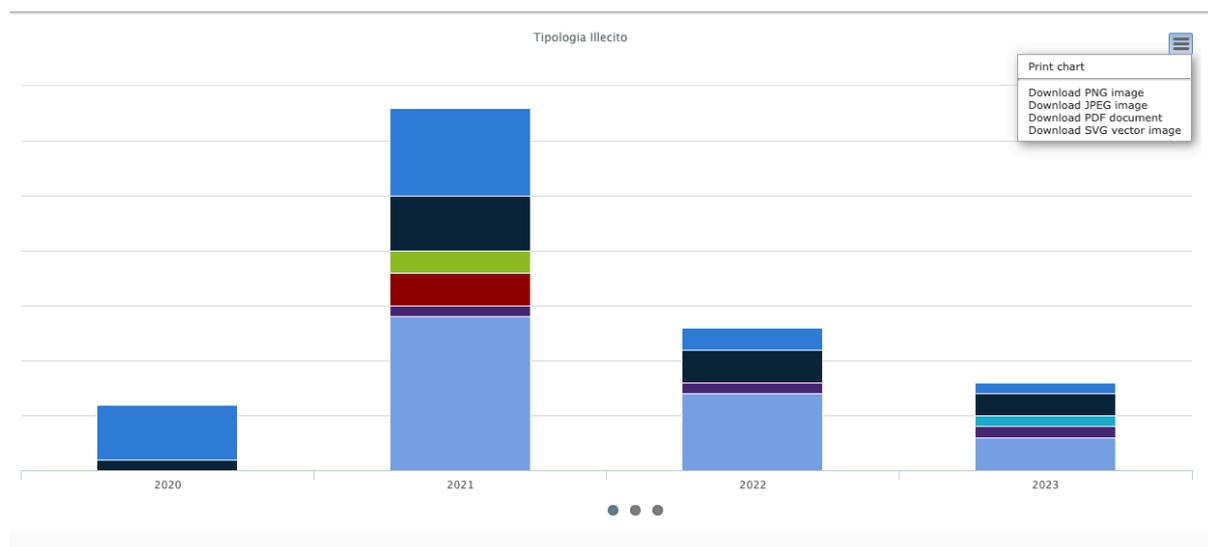
Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato



**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato

L'utente ha la possibilità di stampare l'istogramma o di scaricarlo in diversi formati, come mostrato nella figura seguente:



## Cambiare il Responsabile della prevenzione della corruzione

Il sistema fornisce la procedura per sostituire nel Sistema Responsabile; è così possibile generare automaticamente un vero e proprio registro dei Responsabili che si sono succeduti nella carica e i relativi periodi di attività, come mostrato nella prossima figura:

### Registro Responsabili

Cognome	Nome	Inizio Incarico	Fine Incarico
Test utente	whistleblowing NO	27/05/2020	
resp.aggiunto	antonio	26/05/2020	27/05/2020
Test utente	whistleblowing NO	04/09/2019	26/05/2020

Chiudi

## SERVIZIO DI MANUTENZIONE EVOLUTIVA E NORMATIVA

Nel corso della durata contrattuale, un team di esperti con elevate competenze tecnologiche e di dominio applicativo, curerà il costante aggiornamento del sistema in riferimento all'evoluzione normativa nazionale e internazionale oltre che allo stato dell'arte del contesto tecnologico di riferimento.

**TECNOLINK S.r.l.**

Sede legale Via P. Bagetti, 10 - 10143 Torino (TO)  
 Tel. +39 011 19878715 PEC [tecnolink@mypec.eu](mailto:tecnolink@mypec.eu) Sito internet [www.e-tecnolink.it](http://www.e-tecnolink.it)  
 C.F. e P.IVA 07504810016 REA TO - 900169 Cap. Sociale €10.400,00 int. versato