



Città di Piove di Sacco

(Provincia di Padova)

Settore I - Affari generali - Contratti - Centrale unica di committenza - CED - Personale
Piazza Matteotti, 4 – 35028 Piove di Sacco (PD) – Tel. 049-9709111 Fax: 049.-9702193

<http://www.comune.piovedisacco.pd.it> e-mail: personale@comune.piove.pd.it

pec: polisportello@pec.comune.piove.pd.it

Codice fiscale: 80009770282 Part. IVA 00696250281

Procedura per le segnalazioni di illeciti e irregolarità (WHISTLEBLOWING)

Definizione

Con l'espressione WHISTLEBLOWER si fa riferimento al soggetto che segnala agli organi legittimati ad intervenire violazioni di normative nazionali o europee commesse ai danni dell'interesse pubblico (o di un ente privato) di cui sia venuto a conoscenza nel contesto lavorativo.

La segnalazione (cd. whistleblowing), in tale ottica, è un atto di manifestazione di senso civico, attraverso cui il whistleblower contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per l'amministrazione di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Il whistleblowing è la procedura volta ad incentivare le segnalazioni e a tutelare, proprio in ragione della sua funzione sociale, il whistleblower.

In particolare, i dipendenti pubblici che segnalano un illecito non possono essere sottoposti a provvedimenti disciplinari e sono protetti contro le azioni ritorsive. Nel settore privato, le imprese hanno l'obbligo di prevedere le medesime tutele nei propri modelli organizzativi.

1. FONTE NORMATIVA E NATURA DELL'ISTITUTO

Il Decreto Legislativo 10 marzo 2023 n.24 recepisce in Italia la 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 sostituisce la precedente normativa in materia (Legge 30 novembre 2027 n.179 e art. 54 bis del Decreto legislativo 30 marzo 2001, n.165).

I riferimenti normativi, sempre aggiornati, sono consultabili al link <https://www.segnalazioni.net/normativa-e-compliance-sul-whistleblowing/>.

2. SCOPO E FINALITA' DELLA PROCEDURA

Scopo del presente documento è quello di rimuovere i fattori che possono ostacolare o disincentivare il ricorso all'istituto, quali i dubbi e le incertezze circa la procedura da seguire e i timori di ritorsioni o discriminazioni.

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

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

Pertanto, garantire la protezione – sia in termini di tutela della riservatezza che di tutela da ritorsioni - dei soggetti che si espongono con segnalazioni o denunce contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione o ente di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Tale protezione viene, ora, ulteriormente rafforzata ed estesa a soggetti diversi da chi segnala, come il facilitatore o le persone menzionate nella segnalazione, a conferma dell'intenzione del legislatore europeo e italiano di creare condizioni per rendere l'istituto in questione un importante presidio per la legalità e il buon andamento delle amministrazioni/enti.

3. SOGGETTI CHE GODONO DI PROTEZIONE IN CASO DI SEGNALAZIONE (SEGNALANTE E ALTRI SOGGETTI)

I soggetti ai quali l'ordinamento garantisce adeguata protezione e tutela in caso di segnalazione, denuncia o divulgazione pubblica sono i seguenti:

1. Dipendenti delle Pubbliche Amministrazioni;
2. Dipendenti delle Autorità amministrative indipendenti;
3. Dipendenti degli enti pubblici economici
4. Dipendenti di enti di diritto privato sottoposti a controllo pubblico;
5. Dipendenti delle società in house;
6. Dipendenti degli organismi di diritto pubblico;
7. Dipendenti dei concessionari di pubblico servizio;
8. Dipendenti del settore privato;
9. Lavoratori autonomi o collaboratori che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
10. Volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del settore pubblico o del settore privato
11. Liberi professionisti e consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato
12. Gli Azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.

La tutela è riconosciuta, oltre che ai soggetti segnalanti, anche a quei soggetti che potrebbero essere destinatari di ritorsioni in ragione del ruolo assunto nell'ambito del processo di segnalazione e precisamente:

1. Facilitatore, persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata
2. Persone del medesimo contesto lavorativo del segnalante, e persone che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado
3. Colleghi di lavoro del segnalante
4. Enti di proprietà del segnalante,
5. Enti presso i quali il segnalante lavora
6. Enti che operano nel medesimo contesto lavorativo del segnalante.

4. OGGETTO DELLA SEGNALAZIONE (AMBITO OGGETTIVO)

Sono oggetto di segnalazione le informazioni sulle violazioni di normative nazionali e dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'ente pubblico (o privato) commesse nell'ambito dell'organizzazione dell'ente con cui il segnalante intrattiene un rapporto qualificato di collaborazione (tra quelli elencati al precedente punto 3).

Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse che il whistleblower, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti. Tali elementi possono essere anche irregolarità e anomalie (indici sintomatici) che il segnalante ritiene possano dar luogo ad una violazione.

Le informazioni sulle violazioni devono essere apprese nel contesto lavorativo del segnalante, non solo con riguardo a chi ha un rapporto di lavoro "in senso stretto" con l'organizzazione dell'ente per cui lavora ma anche a anche coloro che hanno instaurato con tale ente altri tipi di rapporti giuridici, come consulenti, collaboratori, volontari, tirocinanti, persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, e ciò anche quando si tratta di situazioni precontrattuali, periodi di prova o situazioni successive allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Infine, possono essere segnalati i fatti appresi in virtù dell'ufficio rivestito ma anche notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, sia pure in modo casuale.

FATTISPECIE DELLE VIOLAZIONI SEGNALABILI:

- Violazioni del diritto nazionale
- Illeciti civili
- Illeciti amministrativi
- Condotte illecite rilevanti ai sensi del D.Lgs. n. 231/2001 (enti privati)
- Illeciti penali
- Illeciti contabili
- Irregolarità che possono costituire "elementi concreti" (indici sintomatici) tali da far ritenere al segnalante che potrebbe essere commessa una violazione
- Violazioni del diritto dell'UE
- Violazioni che ledono gli interessi finanziari dell'Unione Europea
- 10. Violazioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali
- Violazioni che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori sopra indicati.

Sono escluse dall'applicazione della disciplina e delle speciali tutele del whistleblowing:

1. 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 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.

2. Le segnalazioni di violazioni già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali

3. Le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale

4. CONTENUTO DELLE SEGNALAZIONI

Il whistleblower deve fornire tutti gli elementi utili a consentire agli uffici competenti di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione.

In particolare è necessario risultino chiare:

- se conosciute, le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;

- la descrizione il più possibile chiara e completa del fatto;

- se conosciute, le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati (ad esempio la qualifica o il settore in cui svolge l'attività);

- le generalità del soggetto che effettua la segnalazione con indicazione della posizione o funzione svolta all'interno dell'ente o dell'attività svolta nell'ambito di rapporto di collaborazione con l'ente.

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

Ove quanto segnalato non sia adeguatamente circostanziato, chi gestisce le segnalazioni può chiedere elementi integrativi al segnalante.

Le segnalazioni anonime, vale a dire prive di elementi che consentano di identificare il loro autore, anche se recapitate tramite le modalità previste dal presente documento, non verranno prese in considerazione nell'ambito delle procedure volte a tutelare il dipendente pubblico che segnala illeciti, ma verranno trattate alla stregua delle altre segnalazioni anonime e prese in considerazione per ulteriori verifiche solo se relative a fatti di particolare gravità e con un contenuto che risulti adeguatamente dettagliato e circostanziato. Resta fermo il requisito della veridicità dei fatti o situazioni segnalati, a tutela del denunciato.

Tuttavia, qualora la persona venga successivamente identificata e abbia subito ritorsioni si applicano le misure di protezione per le ritorsioni previste per il whistleblowing.

5. I CANALI E LE MODALITÀ DI PRESENTAZIONE DELLE SEGNALAZIONI

a) I CANALI INTERNI – LA PIATTAFORMA DEL COMUNE

La gestione della segnalazione è affidata al Responsabile della Prevenzione della Corruzione e della Trasparenza del Comune di Piove di Sacco (RPCT), il quale rilascia alla persona segnalante un avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione, mantiene le interlocuzioni con la persona segnalante, dà un corretto seguito alle segnalazioni ricevute e infine fornisce un riscontro alla persona segnalante.

Il Comune di Piove di Sacco mette a disposizione al whistleblower **un applicativo software** accessibile al link: <https:///>.

L'applicativo software consente anche di effettuare segnalazioni orali e garantisce assoluta riservatezza e crittografia dei dati del segnalante e della segnalazione, in quanto ac-

cessibili esclusivamente dal soggetto ricevente. Per queste ragioni **l'utilizzo della piattaforma è indicato dal Comune di Piove di Sacco come forma preferenziale rispetto alle altre tipologie di segnalazioni.**

Se dovessero tuttavia pervenire segnalazioni al di fuori della piattaforma <https://.net/>, le stesse verranno recepite e trattate secondo i principi stabiliti in materia di whistleblowing.

Verranno dunque assunte le seguenti modalità:

- Modalità di trattamento mediante segnalazione **via e-mail e via PEC**.
Le segnalazioni inoltrate dagli interessati via e-mail o via PEC vengono acquisite e lette in prima battuta dagli operatori dell'ufficio Protocollo i quali, opportunamente istruiti in tal senso, dovranno prevedere una protocollazione c.d. "riservata". Detto protocollo sarà visualizzabile esclusivamente dal Segretario comunale in qualità di RPCT.

- Modalità di trattamento mediante segnalazione pervenuta **in formato cartaceo**
In caso di segnalazioni scritte, il documento verrà protocollato in forma riservata (solo il destinatario della missiva ha accesso al documento), imbustato e trasmesso al Segretario comunale in qualità di RPCT con la dicitura "riservato/personale". Il documento verrà custodito dal RPCT in armadio chiuso a chiave nel proprio ufficio. Il segnalante ai fini di una maggiore sicurezza della propria identità personale potrà inviare tramite raccomandata AR tre buste: la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "riservata al RPCT". La terza busta, senza aprirla, verrà dall'addetto protocollata in modo riservato e trasmessa al RPCT.

- Modalità di trattamento mediante segnalazione **orale al di fuori della piattaforma**
In caso di segnalazione orale, l'ufficio Segreteria metterà in contatto il soggetto segnalante con il RPCT.
Tramite la segnalazione orale, la tutela della identità personale del segnalante può risultare in concreto più debole a causa della sua stessa natura. La segnalazione scritta mediante piattaforma è suggerita in via prioritaria.

Ogni singola segnalazione pervenuta al di fuori della piattaforma sarà inserita in essa dal Segretario comunale in qualità di RPCT. Sarà cura dello stesso fornire al soggetto segnalante una password al fine di consentire a questi di monitorare la propria segnalazione all'interno della piattaforma.

Le segnalazioni anonime effettuate fuori piattaforma verranno registrate e trattate solo se in presenza di elementi contenutistici tali da consentirne la trattazione.

Per ogni modalità di segnalazione descritta è garantita la riservatezza dell'identità del segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

SEGNALAZIONE TRAMITE LA PIATTAFORMA WHISTLEBLOWING

La piattaforma whistleblowing è accessibile al link: <https://piovedisacco.segnalazioni.net>

Il processo di segnalazione si svolge secondo le seguenti fasi:

- la segnalazione viene effettuata attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, verrà presa in carico se è soltanto se adeguatamente circostanziata;
- la segnalazione viene ricevuta dal Segretario comunale in qualità di RPCT e da lui gestita in modo da garantire la segretezza del segnalante;
- al momento dell'invio della segnalazione, il segnalante riceve una password che deve conservare per poter accedere nuovamente alla piattaforma, verificare la risposta dell'RPCT e dialogare rispondendo a eventuali richieste di chiarimenti o appro-

- fondimenti;
- la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smart-phone) sia dall'interno dell'ente che dal suo esterno. La tutela dell'anonimato è garantita in ogni circostanza.

Per ulteriori informazioni è possibile visionare le FAQ presenti al link <https://piovedisacco.segnalazioni.net> oppure al link <https://www.digitalpa.it/suite-software/whistleblowing/caratteristiche.html>.

b) IL CANALE ESTERNO PRESSO ANAC

Ferma restando la preferenza per il canale interno è prevista la possibilità di effettuare una segnalazione direttamente attraverso ANAC,

Le condizioni per ricorrere al canale esterno presso ANAC sono le seguenti:

- 1) Se il canale interno obbligatorio non è attivo, oppure è attivo ma non è conforme a quanto previsto dal legislatore in merito ai soggetti e alle modalità di presentazione delle segnalazioni
- 2) La persona ha già fatto la segnalazione interna ma non ha avuto seguito
- 3) La persona segnalante ha fondati motivi di ritenere che se effettuasse una segnalazione interna alla stessa non sarebbe dato efficace seguito o questa potrebbe determinare rischio di ritorsione
- 4) La persona segnalante ha fondato motivo di ritenere ma la violazione possa costituire un pericolo imminente o palese per il pubblico interesse

c) LA DIVULGAZIONE PUBBLICA

E' stata introdotta un'ulteriore modalità di segnalazione, consistente nella 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.

Le condizioni per poter effettuare una divulgazione pubblica sono le seguenti:

- 1) ad una segnalazione interna a cui l'amministrazione/ente non abbia dato riscontro nei termini previsti abbia fatto seguito una segnalazione esterna ad ANAC la quale, a sua volta, non ha fornito riscontro al segnalante entro termini ragionevoli;
- 2) la persona ha già effettuato direttamente una segnalazione esterna ad ANAC la quale, tuttavia, non ha dato riscontro al segnalante in merito alle misure previste o adottate per dare seguito alla segnalazione entro termini ragionevoli;
- 3) la persona effettua direttamente una divulgazione pubblica in quanto ha fondato motivo, di ritenere, ragionevolmente, sulla base di circostanze concrete e quindi, non su semplici illazioni, che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse;
- 4) la persona effettua direttamente una divulgazione pubblica poiché ha fondati motivi di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni oppure possa non avere efficace seguito.

d) La denuncia all'Autorità giudiziaria

Qualora il whistleblower rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dalla normativa (vedi precedenti punti a e b), ciò non lo esonera dall'obbligo di denunciare alla competente Autorità giudiziaria i fatti penalmente rilevanti e le ipotesi di danno erariale (Procura della Repubblica ovvero Sezione regionale Corte dei Conti territorialmente competente), in virtù di quanto previsto dal combinato disposto dell'art.331 c.p.p. e degli artt. 361 e 362 c.p.

Si rammenta in ogni caso che l'ambito oggettivo degli artt. 361 e 362 c.p., disponendo l'obbligo di denunciare soltanto reati (procedibili d'ufficio), è più ristretto di quello delle segnalazioni effettuabili dal whistleblower, che può segnalare anche illeciti di altra natura. Resta fermo che, laddove il dipendente pubblico denunci un reato all'Autorità giudiziaria ai sensi degli artt. 361 o 362 c.p. e poi venga discriminato per via della segnalazione, potrà beneficiare delle tutele previste dalla normativa vigente per le ritorsioni subite.
Le stesse regole sulla tutela della riservatezza e del contenuto delle segnalazioni vanno rispettate dagli uffici delle Autorità giudiziarie cui è sporta la denuncia.

6. LA TUTELA DELLA RISERVATEZZA DEL SEGNALANTE

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 a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p.

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.

I sistemi per garantire la tutela della identità del segnalante sono:

- a) preferenza per la gestione informatizzata delle segnalazioni, con il ricorso a strumenti di crittografia **mediante la piattaforma dedicata attivata dal Comune**;
- b) **sottrazione della segnalazione e della documentazione ad essa allegata all'accesso agli atti amministrativi** previsto dagli artt. 22 e ss. della L.241/1990 e all'accesso civico generalizzato ex art. 5 del d.lgs. n. 33/2013;
- c) **rispetto dei principi in materia di protezione dei dati personali.**

La riservatezza, oltre che all'identità del segnalante, viene garantita anche a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante.

La riservatezza viene garantita anche nel caso di segnalazioni - interne o esterne - effettuate in forma orale.

Si tutela la riservatezza del segnalante anche quando la segnalazione perviene a personale diverso da quello autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo

In due casi espressamente previsti dalla normativa vigente, per rivelare l'identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione:

- nel procedimento disciplinare laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare;
- nei procedimenti instaurati in seguito a segnalazioni interne o esterne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

7. TUTELA DELLA RISERVATEZZA DELL'IDENTITÀ DELLE PERSONE SEGNALATE (O COINVOLTE) E DI ALTRI SOGGETTI

La tutela dell'identità della persona coinvolta e della persona menzionata nella segnalazione va garantita da parte degli enti destinatari delle segnalazioni fino alla conclusione dei procedimenti avviati in ragione della segnalazione e nel rispetto delle medesime garanzie previste in favore della persona segnalante. La persona segnalata può essere sentita o viene sentita, dietro sua richiesta, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

La persona segnalata non ha il diritto di essere sempre informata della segnalazione che la riguarda ma solo nell'ambito del procedimento eventualmente avviato nei suoi confronti a seguito della conclusione della gestione della segnalazione e nel caso in cui tale procedimento sia fondato in tutto o in parte sulla segnalazione.

8. IL TRATTAMENTO DEI DATI PERSONALI

La tutela dei dati personali è assicurata non solo alla persona segnalante o denunciante ma anche agli altri soggetti cui si applica la tutela della riservatezza, quali il facilitatore, la persona coinvolta e la persona menzionata nella segnalazione in quanto "interessati" dal trattamento dei dati.

Le qualifiche dei soggetti che trattano i dati personali

Titolari del trattamento

- Il Comune di Piove di Sacco che ha istituito il canale interno

(ANAC per il canale esterno - Altre autorità competenti a cui sono trasmesse le segnalazioni)

Responsabile del trattamento

- Fornitore esterno

Persone autorizzate

- Persone espressamente designate dal RPCT che gestiscono e trattano le segnalazioni .

Principi da rispettare per il trattamento dei dati personali

- Trattare i dati in modo lecito, corretto e trasparente.
- Raccogliere i dati al solo fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce.
- Garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono trattati.
- Assicurare che i dati siano esatti e aggiornati.
- Conservare i dati per il tempo necessario al trattamento della specifica segnalazione. Non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
- Assicurare il trattamento in maniera da garantire la sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione e dal danno accidentali .
- Rispettare il principio della privacy by design e della privacy by default .

- Effettuare la valutazione d'impatto sulla protezione dei dati.
- Rendere ex ante ai possibili interessati un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi (ad esempio sul sito web, sulla piattaforma, oppure informative brevi in occasione dell'uso di altre modalità scritte o orali).
- Assicurare l'aggiornamento del registro delle attività di trattamento.
- Garantire il divieto di tracciamento dei canali di segnalazione .
- Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante.

9. LA TUTELA DA RITORSIONI

A tutela del whistleblower opera il divieto di ritorsione.

Si definisce ritorsione "qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere a causa della segnalazione, che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto".

Si tratta di una definizione ampia del concetto di ritorsione che può consistere sia in atti o provvedimenti che in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano un pregiudizio ai soggetti tutelati. La ritorsione può essere anche "solo tentata o minacciata".

Esempi (con carattere non esaustivo) di ritorsione:

- 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;
- 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;
- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
- richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La protezione prevista in caso di ritorsioni non trova applicazione in caso di accertamento con sentenza, anche non definitiva di primo grado nei confronti del segnalante, della responsabilità penale per i reati di calunnia o diffamazione o comunque per i medesimi reati commessi con la denuncia, ovvero della responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o colpa grave.

Nei casi di accertamento delle dette responsabilità, al soggetto segnalante e denunciante

è inoltre applicata una sanzione disciplinare.

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 dalla normativa 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 ovvero della sua responsabilità civile per lo stesso titolo.

Le presunte ritorsioni, anche solo tentate o minacciate, devono essere comunicate esclusivamente ad ANAC.

10. RESPONSABILITA' DEL WHISTLEBLOWER

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare del whistleblower nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 del codice civile, come anticipato nel presente punto 9.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente policy, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

11. SICUREZZA DEL SEGNALANTE NELLE SEGNALAZIONI MEDIANTE LA PIATTAFORMA TELEMATICA ATTIVATA DAL COMUNE

- Crittografia asimmetrica sui contenuti testuali e sui file allegati: la crittografia non richiede azioni specifiche da parte degli utenti. Il sistema crittografico, garantisce che i messaggi ed i relativi allegati possano essere letti esclusivamente dal mittente e destinatario attraverso l'abbinamento della "chiave crittografica pubblica e privata".

- Possibilità di accesso tramite smart card.

- Accesso regolamentato a norma privacy: l'accesso alle segnalazioni è consentito esclusivamente tramite credenziali (per gli utenti registrati) o tramite l'inserimento dei codici associati alla segnalazione (per gli utenti non registrati).

Sicurezza applicativa

Separazione della segnalazione dall'identità del segnalante. La riservatezza del segnalante è ulteriormente garantita dall'applicazione, che prevede una netta separazione del processo di iscrizione dal processo di segnalazione, per una corretta separazione dei dati; nella segnalazione inviata, infatti, non viene indicato il nominativo del segnalante. Resta ferma la possibilità per il responsabile di attivare la procedura tramite la quale il sistema associa l'identità del segnalante alla segnalazione, motivando la richiesta, quando ciò è ritenuto necessario e nei casi previsti dalla normativa. Tale azione viene automaticamente notificata al segnalante e registrata nel sistema.

Server dedicati DigitalPA: massima protezione dei dati e dei livelli di sicurezza, garantiti sia dalla certificazione DigitalPA ISO 27001/2014 che dalla infrastruttura della server farm certificata ISO 27001/2014.

Firewall hardware e Software integrato: ogni piattaforma dispone di un firewall integrato con strettissime regole, che limitano gli accessi e le azioni agli esclusivi compiti dedicati al software; i firewall si integrano e potenziano ulteriormente la sicurezza.

Certificato SSL: il software di whistleblowing è accessibile esclusivamente tramite accesso

HTTPS (Secure Sockets Layer).

IP e Certificato SSL dedicati per ciascun cliente.

Validazioni input utente: la piattaforma è basata su un approccio di validazione input dell'utente. Attraverso regole estremamente rigide l'utente viene verificato sia a livello client che a livello server.

Prevenzione CSRF: tutte le richieste gestite dalla piattaforma sono protette da token CSRF.