



PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta
Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente
Gestione associata di servizi e assistenza ai Comuni**

DECRETO DEL PRESIDENTE

Decreto nr. 74 del 04/09/2026

Oggetto: PROCEDURA DI SEGNALAZIONE DI VIOLAZIONI DI DISPOSIZIONI
NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE
PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE PUBBLICA - DISCIPLINA DELLA
TUTELA DELLA PERSONA CHE SEGNALE VIOLAZIONI (D.LGS N. 24 DEL 10 MARZO
2023) C.D. WHISTLEBLOWING -AGGIORNAMENTO ATTO ORGANIZZATIVO.

Hash:

DEL_DECP_74_2026.pdf.p7m

8834B091BE28390293EBAA24FEAABBA795EFE21A92750FE12FFA431D9042F973A537C727
35508FFF1E8B50C2BDC855F7FF764AF5A791A184EAC2012ACAE1249C

All. 3) DPIA whistleblowing- PROVINCIA DI PISA_signed.pdf.p7m

32178C3807F550BC4EFE70F1E3EED724EB796C1E99A2E82439E1E3536668F1165ED423086E
5C601D582160D9099CB5A8CB5F824F1B3882E8446311311569BFD2

Allegato 2) informativa privacy.pdf.p7m

E73C053DAAD1844B9BB3E6D61877535CC44AFD38BEA955B93C172E8C4F85C4614E0053B
BE3C97F61C4195CDC7BB391F4F7F2D817A945E729DF79D664286ACF5A

Allegato 1) Procedura WHISTLEBLOWING.pdf.p7m

3C96897D0EEE83E4E91260719D674A08CB0A795A26860F96689B343FF1E14BCC28313BD90
8D428C0D4ECB8F7B38A2E7E4458C125F7556A0A06D6DF7FAF68450B



PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta
Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente
Gestione associata di servizi e assistenza ai Comuni**

SEGRETERIA GENERALE

DECRETO PRESIDENZIALE

Proposta nr. 2302 del 2026

Decreto nr. 74/2026

Oggetto: PROCEDURA DI SEGNALAZIONE DI VIOLAZIONI DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE PUBBLICA - DISCIPLINA DELLA TUTELA DELLA PERSONA CHE SEGNALE VIOLAZIONI (D.LGS N. 24 DEL 10 MARZO 2023) C.D. WHISTLEBLOWING -AGGIORNAMENTO ATTO ORGANIZZATIVO.

IL PRESIDENTE

Nell'esercizio dei poteri assunti ai sensi e per gli effetti del Decreto Legislativo n. 267/2000 Testo Unico degli Enti Locali e della legge n. 56/2014;

Con l'assistenza del Segretario generale ai sensi e per gli effetti dell'art. 97, comma 2, del TU n. 267/2000, in ordine alla conformità dell'azione amministrativa alle leggi, allo Statuto e ai regolamenti;

Visto lo Statuto della Provincia, adottato con delibera n. 1 del 16 marzo 2015 dall'Assemblea dei Sindaci;

Visti, altresì:

- il **D.Lgs. 24 del 10.03.2023** “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.” il quale ha abrogato gli artt. 54-bis, D.Lgs. 165/2001 e 3, l. 179/2017 e raccolto in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico, sia di quello privato;
- la **Delibera ANAC del 12 luglio 2023, n. 311** recante “Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”, con cui l'Autorità ha fornito indicazioni sulla presentazione ad ANAC e relativa gestione delle segnalazioni esterne, così come previsto dall'art. 10 del d.lgs. n. 24/2023;
- la **Delibera n. 478 del 26 novembre 2025**, con cui Anac ha approvato le “[Linee Guida](#) in materia di whistleblowing sui canali interni di segnalazione”, dando indicazioni sulle modalità di gestione dei **canali interni** di segnalazione;
- la **Delibera n. 479, del 26 novembre 2025**, con cui Anac ha poi apportato modifiche ed [integrazioni](#) alle Linee guida sulla presentazione e gestione delle segnalazioni esterne, così da

assicurare la coerenza dei contenuti con le indicazioni presenti superando alcune criticità segnalate dai soggetti tenuti ad applicare il d.lgs. n. 24/2023;

Considerato che con il **Decreto Presidenziale n. 60 dell'11.05.2022** il Presidente della Provincia di Pisa ha aderito al **progetto “Whistleblowing PA” promosso da “Transparency International Italia”** e conseguentemente ha approvato la “Procedura di segnalazione di illeciti o di irregolarità. Disciplina della tutela del dipendente pubblico che segnala illeciti (cd. whistleblower)”;

Rilevato che la disciplina a livello nazionale è stata interamente riformata ad opera del D.Lgs 10 marzo 2023, n. 24;

Ritenuto, necessario, alla luce delle modifiche introdotte dal **D.Lgs. 24 del 10.03.2023 e dalle nuove Linee guida Anac**, sostituire la procedura di segnalazione suddetta con la nuova e aggiornata **“PROCEDURA DI SEGNALAZIONE DI VIOLAZIONE DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITA' DELL'AMMINISTRAZIONE. DISCIPLINA DELLA TUTELA DEL WHISTLEBLOWER”** di cui all'**allegato 1)**, parte integrante e sostanziale del presente atto;

Considerato che, come prescritto all'art.4 comma 1 del D.Lgs 24/2023, è stata data **informazione** alle Organizzazioni Sindacali, trasmettendo la procedura alle stesse con nota n. prot. 34705 del 3.07.2026

Dato atto:

- che la suddetta procedura si applicherà ai dipendenti della Provincia di Pisa, ed a tutti i soggetti di cui all'art.3 del d.lgs. 24 del 10 marzo 2023 che intendano segnalare violazioni di cui siano venuti a conoscenza nell'ambito del proprio contesto lavorativo;
- che la nuova procedura recepisce le novità introdotte dal D.lgs. 24 del 10 Marzo 2023, in particolare quelle relative a:
 - 1) i soggetti segnalanti;
 - 2) l'ambito della violazione;
 - 3) introduzione della segnalazione interna in forma orale;
 - 4) il canale esterno di segnalazione;
 - 5) il divieto di ritorsione ed altre misure di protezione del segnalante;

Preso atto:

- del **Decreto presidenziale n° 30 del 13 marzo 2025** con cui è stato approvato il PIANO INTEGRATO DI ATTIVITA' E ORGANIZZAZIONE 2025-2027 ANNUALITA' 2025, che assorbe al suo interno il PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA per il medesimo triennio;

- del **Decreto presidenziale n° 40 del 10 aprile 2026** con cui è stato approvato il PIANO INTEGRATO DI ATTIVITA' E ORGANIZZAZIONE 2026-2028 ANNUALITA' 2026, che assorbe al suo interno il PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA per il medesimo triennio;

- della **Determinazione n. 967 del 23 giugno 2026** avente ad oggetto “Registro unico dei trattamenti - attività – categorie dell'Amministrazione provinciale di Pisa ai sensi del regolamento UE 679/2016 (GDPR- general data protection regulation). Aggiornamento.”

Considerato, inoltre, che:

- il Regolamento (UE) 2016/679 ha introdotto rilevanti obblighi a carico dei titolari del trattamento, la cui inosservanza espone gli stessi a severe sanzioni, finalizzati a garantire che il trattamento di dati personali si svolga nel pieno rispetto dei diritti dell'interessato, persona fisica;
- l'art. 29 del GDPR dispone che chiunque agisca sotto l'autorità del titolare ed abbia accesso a dati personali "non può trattare tali dati se non è istruito in tal senso";
- l'art. 2 quaterdecies del D. Lgs. 196/2003 dispone che il titolare può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, "che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità";
- l'art 12 del D.Lgs. n. 24/2023 dispone che le segnalazioni possano essere ricevute solamente da soggetti espressamente autorizzati al trattamento dei dati personali ai sensi degli art. 29 e 32, paragrafo 4 del GDPR e dell'art. 2 quaterdecies del Codice della Privacy;
- che le Linee Guida Anac approvate con Delibera n°311 del 12 luglio 2023 come modificata e integrata con Delibera n. 479 del 26 novembre 2025, precisano che *"nei soggetti del settore pubblico tenuti a nominare un Responsabile della prevenzione della corruzione e della trasparenza (RPCT) la gestione del canale interno è affidata a quest'ultimo"*;
- che con D.P. 97/2025 è stato individuato il Responsabile della prevenzione della corruzione e della trasparenza della Provincia di Pisa nella figura del Segretario generale, dott. D'Aco Danilo, **a cui, pertanto, alla luce di quanto detto al punto precedente è affidata la gestione del canale interno di segnalazione;**
- che con D.P. 98/2025 è stato individuato il coordinatore di tutte le procedure e le attività amministrative relative al "trattamento dei dati personali" sempre nella persona del Dott. Danilo D'Aco;
- che le stesse Linee Guida Anac prevedono che *"Visti i numerosi e delicati compiti affidati dalla legge al gestore nonché l'ampiezza delle responsabilità a suo carico in caso di inadempimento, l'Autorità ritiene fondamentale che questi possa avvalersi, laddove le dimensioni organizzative lo consentano, di un gruppo di lavoro dedicato per svolgere l'attività di verifica e di analisi delle segnalazioni"* e che *"Ferma restando la discrezionalità degli enti, la scelta dei soggetti chiamati a supportare il gestore potrebbe ricadere, a titolo esemplificativo, nel settore pubblico, sul personale dell'ufficio di supporto al RPCT o sui suoi referenti"*;

Dato perciò atto che:

- con successivi atti interni si procederà ad espressa autorizzazione al trattamento dei dati personali ai sensi degli art. 29 e 32, paragrafo 4 del GDPR da parte dei soggetti chiamati a supportare l'RPCT o a sostituirlo in caso di prolungata assenza o conflitto di interessi;
- in ottemperanza a quanto previsto dall'art. 35 Regolamento (UE) 2016/679, e dall'art. 13, comma 6 del d.lgs. 24/2023, l'ente ha provveduto a effettuare la valutazione di impatto del trattamento sulla protezione dei dati personali e a redigere apposito documento (allegato 3), previa consultazione con il DPO, il quale ha rilasciato, in data 23 Aprile 2026, parere favorevole.

Visto il parere favorevole di regolarità tecnica espresso dal Segretario generale ai sensi dell'art. 49, comma 1 del D.Lgs 267/2000 ed omissis il parere di regolarità contabile espresso dal Dirigente del Settore Programmazione Finanziaria, in quanto non dovuto poiché l'atto non ha riflessi finanziari né diretti né indiretti, ai sensi dell'art.49, comma 1 del medesimo D.Lgs 267/2000.

Ritenuto di dichiarare immediatamente eseguibile il presente atto, ai sensi e per gli effetti dell'art. 134, comma 4, D.lgs. 267/2000, vista la necessità di dar corso quanto prima agli adempimenti conseguenti al presente decreto;

DECRETA

Per le motivazioni esposte in premessa, che qui si intendono integralmente richiamate:

1. Di approvare, la **“PROCEDURA DI SEGNALAZIONE DI VIOLAZIONE DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL’UNIONE EUROPEA CHE LEDONO L’INTERESSE PUBBLICO O L’INTEGRITA’ DELL’AMMINISTRAZIONE. DISCIPLINA DELLA TUTELA DEL WHISTLEBLOWER”** di cui all'**allegato 1)** del presente decreto di cui forma parte integrante e sostanziale, che, per gli effetti, **sostituisce la precedente disciplina adottata con decreto presidenziale n. 60/2022.**
2. Di approvare l'**informativa sul trattamento** dei dati personali sulla procedura inerente le segnalazioni di condotte illecite presso l'amministrazione (whistleblowing), di cui all'**allegato 2)**.
3. Di approvare, ai sensi e per gli effetti del combinato disposto dell'art. 35 del GDPR e dell'art. 13, comma 6 del d.lgs. 24/2023 la **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** relativa al trattamento di dati personali “whistleblowing”, nel testo di cui **all'Allegato 3)** al presente atto.
4. Di dare atto che è stata data **informazione** alle Organizzazioni Sindacali, trasmettendo la procedura alla stesse in data 03.07.2026. Con nota prot. n. 34705 ex art 4 del D.Lgs 24/2023.
5. Di demandare al Settore competente la pubblicazione della procedura nelle apposite pagine della sezione “Amministrazione Trasparente” del sito web istituzionale della Provincia di Pisa.
6. Di trasmettere il presente atto ai Dirigenti, al Segretario Generale, alla RSU e alle Organizzazioni Sindacali.
7. Di dare atto che, ai sensi di quanto precisato dalle Linee Guida Anac approvate con Delibera n°311 del 12 luglio 2023 come modificata e integrata con Delibera n. 479 del 26 novembre 2025, l'**incarico di gestore delle segnalazioni di cui al D.Lgs 24 del 10 marzo 2023 è in capo al Responsabile della Prevenzione della Corruzione e Trasparenza nella persona del Dott. Danilo D’Aco.**
8. Di demandare al Dott. Danilo D’Aco, quale gestore della procedura di segnalazione, nonché coordinatore di tutte le procedure e le attività amministrative relative al “trattamento dei dati personali”, **gli atti organizzativi di competenza** discendenti dall’adozione della nuova procedura di segnalazione, compresa **l’adozione di atti interni di autorizzazione al trattamento dei dati personali** ai sensi degli art. 29 e 32, paragrafo 4 del GDPR, **al personale di supporto e di quello chiamato a sostituirlo in caso di prolungata assenza o conflitto di interessi.**

9. Di provvedere a dare ampia diffusione al personale della Provincia di Pisa della suddetta procedura e dell'applicativo informatico per l'inoltro delle segnalazioni.

Approvato e sottoscritto con firma digitale:

Il Presidente

Massimiliano Angori



PROVINCIA DI PISA

PROCEDURA DI SEGNALEZIONE DI VIOLAZIONE DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITA' DELL'AMMINISTRAZIONE –(DISCIPLINA DELLA TUTELA DEL WHISTLEBLOWER)

In attuazione della Direttiva (UE) 2019/1937, è stato emanato il d.lgs. n. 24 del 10 marzo 2023 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 d.lgs. n. 24/2023 oltre a determinare l'abrogazione dell'art. 54 bis del d.lgs. 165/2001, assorbendone la relativa disciplina, ha introdotto una serie di novità, tra cui l'ampliamento dei soggetti beneficiari delle protezioni, la disciplina dei canali di segnalazione e delle condizioni per accedervi, la specificazione degli obblighi di riservatezza, l'ampliamento della casistica delle ritorsioni e l'introduzione delle misure di sostegno in favore delle persone segnalanti.

Con delibera ANAC del 12 luglio 2023, n. 311 recante “Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”, l'Autorità ha fornito indicazioni sulla presentazione ad ANAC e relativa gestione delle segnalazioni esterne, così come previsto dall'art. 10 del d.lgs. n. 24/2023.

Con delibera n. 478, approvata dal Consiglio del 26 novembre 2025, Anac ha approvato le Linee Guida in materia di whistleblowing sui canali interni di segnalazione, dando indicazioni sulle modalità di gestione dei canali interni di segnalazione.

L'obiettivo è garantire un'applicazione uniforme ed efficace della normativa sul whistleblowing e indirizzare ulteriormente i soggetti tenuti a dare attuazione alla stessa.

Infine con Delibera n. 479, approvata dal Consiglio del 26 novembre 2025, Anac ha poi apportato modifiche ed integrazioni alle Linee guida sulla presentazione e gestione delle segnalazioni esterne, così da assicurare la coerenza dei contenuti con le indicazioni presenti superando alcune criticità segnalate dai soggetti tenuti ad applicare il d.lgs. n. 24/2023.

Le principali novità contenute nella nuova disciplina sono:

- la specificazione dell'ambito soggettivo con riferimento agli enti di diritto pubblico, a quelli di diritto privato e l'estensione del novero di questi ultimi;
- l'ampliamento del novero delle persone fisiche che possono essere protette per le segnalazioni, denunce o divulgazioni pubbliche;

- l'espansione dell'ambito oggettivo, cioè di ciò che è considerato violazione rilevante ai fini della protezione, nonché distinzione tra ciò che è oggetto di protezione e ciò che non lo è;
- la disciplina di tre canali di segnalazione e delle condizioni per accedervi: interno (negli enti con persona o ufficio dedicato oppure tramite un soggetto esterno con competenze specifiche), esterno (gestito da ANAC) nonché il canale della divulgazione pubblica;
- l'indicazione di diverse modalità di presentazione delle segnalazioni, in forma scritta o orale;
- la disciplina dettagliata degli obblighi di riservatezza e del trattamento dei dati personali ricevuti, gestiti e comunicati da terzi o a terzi;
- i chiarimenti su che cosa si intende per ritorsione e ampliamento della relativa casistica;
- la disciplina sulla protezione delle persone segnalanti o che comunicano misure ritorsive offerta sia da ANAC che dall'autorità giudiziaria e maggiori indicazioni sulla responsabilità del segnalante e sulle scriminanti;
- l'introduzione di apposite misure di sostegno per le persone segnalanti e il coinvolgimento, a tal fine, di enti del Terzo settore che abbiano competenze adeguate e che prestino la loro attività a titolo gratuito;
- la revisione della disciplina delle sanzioni applicabili da ANAC e l'introduzione da parte dei soggetti privati di sanzioni nel sistema disciplinare adottato ai sensi del d.lgs. n. 231/2001.

Con il presente atto organizzativo si intende recepire nell'ordinamento interno all'Ente le novità normative sopra descritte adeguando la procedura di segnalazione e adottando le idonee precauzioni per tutelare il soggetto segnalante (c.d. whistleblower), garantendone l'anonimato e contrastando ogni possibile ritorsione nei confronti dello stesso, individuando e rimuovendo i possibili fattori che potrebbero impedire il ricorso all'istituto della segnalazione di illeciti nel pubblico interesse, in osservanza di quanto previsto dalla normativa vigente.

Nella nuova definizione proposta dal decreto legislativo 24/2023 il segnalante (c.d. whistleblower) è la persona fisica che effettua la segnalazione, la denuncia o la divulgazione pubblica di informazioni su violazioni acquisite nell'ambito del proprio contesto lavorativo.

Pur rischiando personalmente atti di ritorsione a causa della segnalazione, egli svolge un ruolo di interesse pubblico, dando conoscenza, se possibile tempestiva, di problemi o pericoli all'ente di appartenenza o alla comunità.

A seguito dell'abrogazione dell'art. 54 bis del D.lgs. 165/2001, ad opera del decreto legislativo n. 24/2023, l'individuazione dei soggetti legittimati a effettuare le segnalazioni è affidata all'art. 3 del decreto in parola.

Il suddetto articolo ha notevolmente ampliato il novero dei soggetti cui, all'interno del settore pubblico, è riconosciuta protezione, anche da ritorsioni, in caso di segnalazione, interna o esterna, divulgazione pubblica e denuncia all'autorità giudiziaria, inserendo per la prima volta una tutela anche a favore di figure diverse da chi segnala, denuncia o effettua divulgazioni pubbliche, non previste dalla previgente normativa (es. facilitatore, persone del medesimo contesto lavorativo legate da uno stabile legame affettivo o di parentela).

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, come sottolineato dall'Anac nelle premesse delle linee guida sopra dette, *“garantire la protezione – sia in termini di tutela della riservatezza che di tutela da ritorsioni -dei soggetti che si espongono con segnalazioni, denunce o, con il nuovo istituto della divulgazione pubblica, 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.”*

In tale ottica l'obiettivo prioritario del presente documento è quello di aggiornare, in linea con le nuove prescrizioni di cui al decreto legislativo 24/2023, la procedura di segnalazione precedentemente approvata con decreto presidenziale n.60 del 2022, allo scopo di fornire al segnalante oggettive indicazioni operative circa:

- a) i soggetti destinatari della segnalazione;
- b) l'oggetto e i contenuti della segnalazione;
- c) Le possibili modalità di segnalazione;
- d) le forme di tutela che, devono essere offerte, allo stesso segnalante e ai soggetti ulteriormente indicati dal decreto legislativo 24/2023, per evitare possibili ripercussioni sulla loro vita lavorativa.

PROCEDURE DI SEGNALEZIONE

Art. 1)

Soggetti legittimati alla segnalazione

I soggetti che possono beneficiare della tutela prevista dalla normativa sono, ai sensi dell'art. 3 del D.Lgs. 24/2023, coloro che effettuano segnalazioni interne o esterne, divulgazioni pubbliche o denunce all'autorità giudiziaria o contabile di violazioni rilevanti per il decreto citato e di cui siano venuti a conoscenza **nell'ambito del proprio contesto lavorativo.**

Nello specifico la tutela si applica a:

- dipendenti della Provincia di Pisa, sia a tempo determinato che indeterminato, con qualsiasi profilo e qualifica professionale;
- dipendenti della Provincia di Pisa anche se in servizio presso altre amministrazioni pubbliche in posizione di comando, distacco o situazioni analoghe;
- dipendenti di altre amministrazioni pubbliche in posizione di comando, distacco o situazioni analoghe presso la Provincia di Pisa;
- dipendenti di enti pubblici economici e degli enti di diritto privato nei cui confronti la Provincia di Pisa esercita il controllo ex art. 2359 c.c.;
- dipendenti delle società in house, nonché i lavoratori e i collaboratori di imprese fornitrici di beni o servizi o che realizzano opere a favore della Provincia di Pisa, nel caso di segnalazioni di illeciti o irregolarità riguardanti l'Amministrazione Provinciale;
- dipendenti degli organismi di diritto pubblico della Provincia di Pisa;
- dipendenti dei concessionari di pubblico servizio della Provincia di Pisa;
- lavoratori autonomi, liberi professionisti e consulenti che svolgono la propria attività lavorativa presso la Provincia di Pisa;
- volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Provincia di Pisa;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso la Provincia di Pisa (ad esempio componenti dell'Organismo di valutazione, del Collegio dei Revisori,...).

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.

In virtù dell'elenco previsto all'art. 3 del D.LGS 24/2023, l'accezione da attribuire al "contesto lavorativo" è più ampia rispetto alla disciplina previgente, comprendendo al suo interno non solo i rapporti di lavoro in senso stretto (e quindi i dipendenti dell'ente), ma anche altri tipi di rapporti giuridici riconducibili rapporti di consulenza, volontariato, collaborazione, tirocinio etc).

Ulteriori destinatari della tutela del segnalante

Sono destinatari della medesima tutela del segnalante anche i seguenti, ulteriori soggetti:

- persone dello stesso contesto lavorativo che assistono il segnalante nel processo di segnalazione ("facilitatori"), la cui identità deve essere mantenuta riservata;

- persone del medesimo contesto lavorativo del segnalante, a lui legate da uno stabile legame affettivo o di parentela entro il quarto grado;
- persone del medesimo contesto lavorativo del segnalante, che hanno con lui un rapporto abituale e corrente;
- enti di proprietà della persona segnalante o per i quali la stessa persona lavora;
- enti che operano nel medesimo contesto lavorativo del segnalante;
- persone che hanno effettuato una segnalazione anonima, che sono state successivamente identificate, e che hanno subito ritorsioni.

Art. 2

Destinatario delle segnalazioni

La Provincia di Pisa individua nel Responsabile della Prevenzione della Corruzione e della Trasparenza, il soggetto destinatario delle segnalazioni.

Il RPCT può essere coadiuvato da soggetti del suo gruppo di supporto specificamente nominati in atto interno.

Le informazioni sulle violazioni di cui i segnalanti sono venuti a conoscenza nell'ambito del contesto lavorativo vanno trasmesse al Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT) esclusivamente attraverso l'apposita procedura informatica di cui all'art. 8 del presente documento o in forma orale previa richiesta, tramite piattaforma informatica di cui all'art. 8, di incontro con il RPCT. in corso di attivazione.

Qualora la segnalazione interna effettuata ai sensi del decreto legislativo n. 24/2023, sia presentata, per errore, ad un soggetto diverso dal RPCT, tale soggetto deve provvedere a trasmettere la stessa in termini riservati al RPCT entro sette giorni dal suo ricevimento (ad esempio, in busta chiusa riservata da consegnare nelle mani del RPCT), dando contestuale notizia della avvenuta trasmissione alla persona segnalante (sempre in termini riservati).

Art. 3

Conflitto di interessi e prolungata assenza del Responsabile della prevenzione della corruzione e trasparenza

Nel caso in cui il Responsabile della prevenzione della corruzione versi in una delle condizioni di conflitto di interessi tipiche e atipiche di cui all'art. 51 c.p.c. o agli artt. 6 e 7 del d.P.R. n. 62/2013 oppure nel caso in cui il RPCT coincida con la persona segnalante, con la persona coinvolta o interessata dalla segnalazione, lo stesso viene sostituito nel suo ruolo di gestione del canale interno di segnalazione dal Dirigente del Settore Programmazione Finanziaria e Risorse.

Quest'ultimo sostituisce il RPCT anche in caso di assenza prolungata (superiore a trenta giorni).

In caso di assenze brevi superiori a sette giorni ma inferiori a trenta non è prevista la sostituzione ma il segnalante sarà avvisato, sempre tramite la pagina del sito che l'elaborazione della segnalazione potrà subire ritardi e che verrà elaborata al rientro dell'RPCT,

Art. 4

Contenuto della segnalazione

I comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori:
 - appalti pubblici;
 - servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo;
 - sicurezza e conformità dei prodotti;
 - sicurezza dei trasporti;
 - tutela dell'ambiente;
 - radioprotezione e sicurezza nucleare;
 - sicurezza degli alimenti e dei mangimi e salute e benessere degli animali;
 - salute pubblica;
 - protezione dei consumatori;
 - tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione;
- i comportamenti impropri da parte del funzionario pubblico che, al fine di curare un interesse proprio o di terzi, assuma o concorra all'adozione di una decisione che devia dalla cura imparziale dell'interesse pubblico non sono più considerate di per sé violazioni segnalabili, bensì possono essere considerate come elementi concreti di una violazione che potrebbe concretizzarsi.

Non sono considerate segnalazioni di whistleblowing quelle aventi ad oggetto una contestazione, rivendicazione o richiesta legata ad un interesse di carattere personale del segnalante.

Il "segnalante" non dovrà utilizzare, quindi, l'istituto in argomento per scopi meramente personali o per effettuare rivendicazioni di lavoro contro superiori gerarchici o l'Amministrazione, per le quali occorre riferirsi alla disciplina e alle procedure di competenza di altri organismi o uffici.

Possono essere oggetto di segnalazione, divulgazione pubblica o denuncia anche quegli elementi che riguardano condotte volte ad occultare le violazioni. Si pensi, ad esempio, all'occultamento o alla distruzione di prove circa la commissione della violazione.

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 le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio).

Irrilevanza dei motivi personali del segnalante o del denunciante.

I motivi che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della trattazione della segnalazione e della protezione da misure ritorsive. Resta comunque fermo che non sono considerate segnalazioni di whistleblowing quelle aventi ad oggetto una contestazione, rivendicazione o richiesta legata ad un interesse di carattere personale del segnalante.

Elementi e caratteristiche della segnalazione

È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni negli enti e amministrazioni del settore pubblico e privato nonché da parte di ANAC.

Il contenuto essenziale della segnalazione è costituito da:

- tempo e luogo in cui si è verificato il fatto della segnalazione
- la descrizione del fatto
- generalità e altri elementi utili a identificare il soggetto cui attribuire i fatti segnalati.

Possono essere allegati anche documenti che a supporto della fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti che potrebbero essere a conoscenza dei fatti.

Il Responsabile della prevenzione della corruzione e trasparenza è coadiuvato dal Dirigente del Settore Programmazione Finanziaria e Risorse e dal personale della Segreteria generale che viene coinvolto a discrezione del Responsabile, tenuto conto della tipologia della segnalazione.

Art. 5

Segnalazioni anonime

Le segnalazioni anonime non rientrano nell'ambito di applicazione delle presenti disposizioni ed esse vengono di norma archiviate.

Solo qualora le segnalazioni anonime pervenute siano circostanziate e rivestano il carattere della attualità esse possono, a insindacabile giudizio dell'RPCT, essere oggetto di specifici approfondimenti secondo le ordinarie procedure di vigilanza.

Di tali segnalazioni e dei relativi esiti si potrà tenere conto in sede di aggiornamento della Sottosezione “Rischi corruttivi e trasparenza” del PIAO.

Tuttavia, la nuova normativa prevede che il segnalante anonimo, successivamente identificato e al ricorrere dei relativi presupposti, possa godere delle tutele previste dalla normativa.

Al fine di attribuire ad esse data certa, anche le segnalazioni anonime vengono acquisite al protocollo riservato dell'Ente.

Art. 6

Inammissibilità della segnalazione

La segnalazione viene considerata inammissibile e viene archiviata senza ulteriori accertamenti, nei seguenti casi:

- manifesta mancanza di interesse all'integrità della pubblica amministrazione;

- manifesta incompetenza della Provincia di Pisa sulle questioni segnalate;
- manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- intervento della Provincia di Pisa non più attuale;
- finalità palesemente emulativa;
- accertato contenuto generico della segnalazione o tale da non consentire la comprensione dei fatti,
- ovvero segnalazione corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione in assenza della segnalazione di condotte illecite;
- mancanza dei dati che costituiscono elementi essenziali della segnalazione (come sopra descritti).

Si rappresenta in questa sede la rilevanza di un comportamento collaborativo del segnalante, al quale si richiede, anche nel proprio interesse, di tenere costantemente aggiornata la Provincia di Pisa in ordine all'evoluzione della propria segnalazione, soprattutto quando questa non sia più connotata dal carattere di attualità.

Si precisa che la segnalazione di cui al decreto legislativo n. 24/2023 citato, indirizzata al RPCT o ad ANAC, non sostituisce, per i soggetti tenuti e laddove ne ricorrano i presupposti, la denuncia alla competente Autorità giudiziaria ordinaria o contabile.

Art.7

Modalità di segnalazione

7.1 Canali interni di segnalazione

Il destinatario della segnalazione interna è il Responsabile della prevenzione della Corruzione e trasparenza (RPCT) e la stessa può essere effettuata tramite i seguenti canali interni che la Provincia di Pisa mette a disposizione sulla base di quanto stabilito dall'art 4 D.Lgs. 24/2023:

- in forma scritta in modalità informatica con accesso alla piattaforma direttamente dal link “Whistleblowing” pubblicato sul sito istituzionale della Provincia di Pisa “Amministrazione Trasparente/Altri contenuti/Prevenzione della Corruzione”;
- in forma orale attraverso la richiesta tramite la piattaforma di incontro con il Responsabile della Prevenzione della Corruzione e Trasparenza;

7.2 Canale esterno di segnalazione

Il segnalante può usufruire anche di un canale esterno che consiste nell'effettuare una segnalazione ad ANAC ai sensi dell'art. 7 d.lgs. 24/2023 e al ricorrere dei requisiti richiesti dall'art. 6 d.lgs. 24/2023, come sotto meglio specificati.

Le condizioni richieste dal menzionato art. 6 per il ricorso alla segnalazione esterna ad ANAC da parte del segnalante, in particolare, sono le seguenti:

- il canale di segnalazione interna non è attivo o, anche se attivato, non è conforme alla normativa;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

7.3 Divulgazione pubblica

Il segnalante può divulgare pubblicamente la segnalazione ai sensi dell'art. 15 d.lgs. 24/2023 al ricorrere delle seguenti condizioni:

- la persona segnalante ha già effettuato una segnalazione interna ed esterna ad ANAC, oppure ha effettuato direttamente una segnalazione esterna ad ANAC e delle stesse non è stato dato riscontro;
- la persona segnalante ha fondati motivi di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito;
- la persona segnalante ha fondato motivo di ritenere, sulla base di circostanze concrete, che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Art. 8

Segnalazione interna in forma scritta tramite modalità informatica

Il “segnalante” potrà inviare una segnalazione attraverso la procedura informatica denominata “**piattaforma Whistleblowing PA**” il cui indirizzo web è pubblicato sul sito istituzionale dell'ente all'interno della sezione Amministrazione trasparente, nella sottosezione dedicata alla “Prevenzione della corruzione” e sul portale interno dell'ente “Intranet” oppure seguendo direttamente la modulistica ANAC.

Le caratteristiche della modalità di segnalazione su Piattaforma sono le seguenti:

- la segnalazione viene fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata;
- la segnalazione viene ricevuta dal Responsabile per la Prevenzione della Corruzione (RPCT) e da lui gestita mantenendo il dovere di confidenzialità nei confronti del segnalante;
- la segnalazione ricevuta sarà protocollata in modalità riservata e custodita ai sensi di legge, in modo da garantire la massima sicurezza e riservatezza;
- al segnalante è trasmesso avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione.

- nel momento dell'invio della segnalazione, il segnalante riceve un codice numerico di 16 cifre che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta dell'RPCT e dialogare rispondendo a richieste di chiarimenti o approfondimenti;
- la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno dell'ente che dal suo esterno. La tutela dell'anonimato è garantita in ogni circostanza.
- la piattaforma permette il dialogo, anche in forma anonima, tra il segnalante e l'RPCT per richieste di chiarimenti o approfondimenti, senza quindi la necessità di fornire contatti personali;

Le segnalazioni inoltrate potranno essere gestite esclusivamente dal “Responsabile per la Prevenzione della Corruzione (RPCT)” e dal “Dirigente del Settore Programmazione Finanziaria e Risorse” che accederanno alla piattaforma con credenziali riservate e personali nel rispetto delle misure minime di sicurezza in materia di tutela dei dati personali della Provincia di Pisa.

La conservazione dei dati avverrà a norma di legge e per il tempo necessario e, qualora i dati fossero costituiti da documenti cartacei, si provvederà alla custodia e conservazione in apposito armadio chiuso a chiave situato presso gli uffici del “Responsabile della Prevenzione della Corruzione (RPCT)” o del “Dirigente del Settore Programmazione Finanziaria e Risorse” e accessibile solo alle persone appositamente autorizzate. Al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte, l'accesso ai dati sarà consentito esclusivamente, oltre che al “Responsabile della Prevenzione della Corruzione (RPCT)” e al “Dirigente del Settore Programmazione Finanziaria e Risorse”, al personale della Segreteria generale e agli amministratori di sistema.

Art. 9

Segnalazione interna in forma orale tramite richiesta di incontro diretto

Il segnalante può utilizzare la procedura informatica della Piattaforma anche per richiedere un appuntamento con il RPCT e fare la segnalazione durante il colloquio in forma orale, in cui verrà redatto apposito verbale controfirmato.

In caso sia stato richiesto un colloquio con il RPCT, l'avviso di ricevimento contiene la proposta di appuntamento, che in ogni caso dovrà essere fissato entro 20 giorni, e la richiesta di consenso alla verbalizzazione del colloquio stesso. Il verbale redatto a seguito del colloquio viene sottoposto dal RPCT entro 20 giorni alla persona segnalante che può verificare, rettificare e confermare il verbale mediante la propria sottoscrizione.

Art. 10

Attività di accertamento delle segnalazioni

Il “Responsabile della Prevenzione della Corruzione (RPCT)”, all'atto del ricevimento della segnalazione, provvederà, avvalendosi del “Dirigente del Settore Programmazione Finanziaria e Risorse” ed eventualmente del personale della Segreteria generale, a un esame preliminare della stessa, mirato a verificare la presenza dei requisiti di ammissibilità e avvierà, con le opportune cautele, la procedura

interna per la verifica dei fatti rappresentati nella dichiarazione del segnalante, investendo le strutture competenti per il prosieguo delle attività.

In caso di sua assenza o impedimento procederà il “Dirigente del Settore Programmazione Finanziaria e Risorse”.

Durante l’istruttoria, che dovrà essere avviata entro 15 gg dalla data di ricezione della segnalazione, l’RPCT esegue una prima imparziale valutazione sulla sussistenza di quanto rappresentato nella segnalazione. A tale scopo può avviare un dialogo con il segnalante, chiedendo ulteriore documentazione a supporto della tesi del segnalante, chiarimenti circa il contenuto della segnalazione o eventuali integrazioni alla stessa. Il segnalante che riceva una richiesta di integrazione della comunicazione, procede inoltrando, se lo ritiene, gli elementi richiesti.

Il responsabile RPCT può anche procedere all’audizione personale del segnalante e di eventuali altri soggetti che possono riferire sugli episodi rappresentati nella segnalazione.

Art. 11

Riscontro al segnalante

Il termine per fornire riscontro alla segnalazione è di tre mesi dalla data dell’avviso di ricevimento o, in mancanza, dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Tuttavia, occorre precisare che il medesimo riscontro, da rendersi nel termine di tre mesi, può anche essere meramente interlocutorio, giacché possono essere comunicate le informazioni relative a tutte le attività sopra descritte che si intende intraprendere e lo stato di avanzamento dell’istruttoria. In tale ultimo caso, terminata l’istruttoria, gli esiti dovranno comunque essere comunicati alla persona segnalante.

All’esito dell’istruttoria, il RPCT fornisce riscontro alla segnalazione che può consistere in:

- comunicazione dell’archiviazione per carenza di prove a carico del segnalato che giustifichino la prosecuzione delle indagini;
- descrizione delle attività intraprese o da intraprendere all’esito dell’istruttoria svolta (per es. rinvio all’autorità competente per ulteriori indagini, avvio di un’inchiesta interna, adozione di provvedimenti per affrontare la questione sollevata, ecc...). Nel caso la segnalazione risulti fondata il Responsabile della prevenzione della corruzione e trasparenza, in relazione ai profili di illiceità, individua, tra i seguenti, il soggetto al quale inoltrare la segnalazione:
 - Dirigente del Settore cui è ascrivibile il fatto
 - Ufficio per i procedimenti disciplinari
 - Autorità giudiziaria
 - Corte dei Conti
 - ANAC.

Qualora, all'esito delle opportune verifiche, la segnalazione risulti fondata, in tutto o in parte, il Responsabile della Prevenzione della Corruzione e Trasparenza, in relazione alla natura della violazione, provvederà:

- 1) a comunicare l'esito dell'accertamento al Dirigente Responsabile del Settore di appartenenza dell'autore della violazione accertata affinché adotti i provvedimenti di competenza, incluso, sussistendone i presupposti, l'esercizio dell'azione disciplinare, purchè la competenza, per la gravità dei fatti, non spetti direttamente all'Ufficio Procedimenti Disciplinari (UPD), che in tal caso provvederà direttamente;
- 2) a presentare segnalazione all'Autorità Giudiziaria competente, se sussistono i presupposti di legge;
- 3) ad adottare o a proporre di adottare, se la competenza è di altri soggetti o organi, tutti i necessari provvedimenti amministrativi per il pieno ripristino della legalità.

PRECAUZIONI PER LA TUTELA DEL SEGNALANTE

Art. 12

Tutela della riservatezza

La segnalazione non possono essere utilizzata oltre quanto necessario per dare adeguato seguito alla stessa.

Ai sensi dell'art. 12 del D. Lgs n. 24/2023 l'identità del segnalante non può essere rivelata, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare

Allo stesso modo è tutelata l'identità delle persone coinvolte e menzionate nelle segnalazioni fino alla conclusione dei procedimenti avviati a seguito delle segnalazioni stesse.

Per identità si intende non solo il nominativo della persona, ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identità della persona stessa.

Pertanto, l'intera procedura e gestione della segnalazione ricevuta attraverso il canale interno di cui all'art. 4 avviene in modalità riservata, in modo da garantire la massima sicurezza, riservatezza e anonimato. Al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte, l'accesso ai dati sarà consentito esclusivamente al RPCT, ed eventualmente al gruppo di supporto, tutti soggetti competenti appositamente formati e debitamente autorizzati al trattamento dei dati personali ai sensi dell'art. 29 e 32 del Reg. (UE) 2016/679 e dell'art. 2-quaterdecies del d.lgs. 196/2003 e ss. mm. ii.

In caso di mancato rispetto della tutela della riservatezza del segnalante, il RPCT, i componenti del gruppo di supporto e l'amministratore di sistema rispondono disciplinarmente; il RPCT inoltre può incorrere nelle sanzioni previste dalle norme di legge vigenti.

Nel caso la segnalazione avvenga con modalità diverse di quanto previsto all'art. 4 del d.lgs 24/2023, o pervenga a persone diverse dal RPCT, le persone riceventi la segnalazione dovranno adottare tutte le misure necessarie per garantire la riservatezza del segnalante, delle persone coinvolte o menzionate nella segnalazione e della eventuale documentazione allegata. La conservazione dei dati avverrà a norma di

legge e per il tempo necessario all'accertamento della fondatezza della segnalazione e, se del caso, all'adozione dei provvedimenti conseguenti e/o all'esaurirsi di eventuali azioni avviate a seguito della segnalazione. Successivamente, tali dati saranno distrutti.

Qualora i dati fossero costituiti da documenti cartacei, si provvederà alla custodia e conservazione in apposito armadio chiuso a chiave situato presso gli uffici del RPCT, e accessibile solo alle persone appositamente autorizzate. In ogni caso, la conservazione dei dati non potrà superare il termine dei cinque anni dalla data in cui viene comunicato al segnalante l'esito finale della procedura di segnalazione. Nell'ambito del procedimento penale, l'identità del 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 del segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

Nell'ambito del procedimento disciplinare attivato dall'Amministrazione contro il presunto autore della condotta segnalata, l'identità del segnalante non può essere rivelata ove la contestazione dell'addebito disciplinare si fondi su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti ad essa. 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 del segnalante alla rivelazione della sua identità, e solo previo avviso al segnalante in forma scritta delle ragioni della rivelazione dei dati riservati.

Il consenso in forma espressa del segnalante e l'avviso al segnalante in forma scritta delle ragioni della rivelazione dei dati riservati sono condizioni necessarie anche nel caso in cui, nei procedimenti instaurati in seguito a segnalazioni, la rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

Nel caso in cui l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare, l'Ente non potrà procedere con il procedimento disciplinare se il segnalante non acconsente espressamente alla rivelazione della propria identità.

In tale caso, il RPCT provvederà quindi ad acquisire tale consenso presso il segnalante, utilizzando la piattaforma informatica dedicata o le altre modalità previste dal canale interno di segnalazione di cui all'art. 8, attraverso richiesta di sottoscrizione del suddetto consenso. Coloro che ricevono o sono coinvolti nella gestione della segnalazione, anche solo accidentalmente, sono tenuti a tutelare la riservatezza di tale informazione. La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare.

La segnalazione è sottratta all'esercizio del diritto di accesso agli atti amministrativi disciplinato dagli artt. 22 e seguenti della Legge n. 241/1990 e ss.mm.ii e dall'accesso civico generalizzato di cui agli artt. 5 e seguenti del D. Lgs. 33/2013.

Art. 13

Tutela da ritorsioni.

I soggetti che segnalano all'Autorità Giudiziaria, alla Corte dei Conti, all'Autorità Nazionale Anticorruzione (ANAC), o al "Responsabile" violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, di cui siano venute a conoscenza nel contesto lavorativo, non possono subire alcuna ritorsione.

Per ritorsione si intende, ai sensi dell'art. 2 comma 1 lettera m) del decreto legislativo 24/2023, 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 quindi ad esse strettamente collegato 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.

Di seguito sono indicate talune fattispecie che, qualora siano riconducibili all'articolo 2, comma 1, lettera m), costituiscono ritorsioni:

- a) il licenziamento, la sospensione o misure equivalenti;
- b) la retrocessione di grado o la mancata promozione;
- c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- e) le note di merito negative o le referenze negative;
- f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- g) la coercizione, l'intimidazione, le molestie o l'ostracismo;
- h) la discriminazione o comunque il trattamento sfavorevole;
- i) la 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;
- l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- m) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- p) l'annullamento di una licenza o di un permesso;
- q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Le persone segnalanti e gli altri soggetti di cui all'art. 3 comma 5 possono comunicare ad Anac le ritorsioni, anche solo tentate o minacciate. (art 19 d.lgs 24/2023)

L'ANAC informa il Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.

In caso di accertamento positivo da parte di Anac di atti di ritorsione, gli stessi, a norma dell'art. 19 d.lgs 24/2023, debbono ritenersi nulli.

Nello specifico caso del licenziamento a carattere ritorsivo dei soggetti di cui all'art. 3 del D.Lgs., lo stesso si intende nullo e l'amministrazione è obbligata al reintegro nel posto di lavoro.

Art. 14

Limitazioni della responsabilità

Se al momento della rivelazione o diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per far scoprire la violazione, e se la segnalazione, la divulgazione pubblica o la denuncia sia stata effettuata nel rispetto delle condizioni previste dall'art 16 comma 1 lettere a) e b) del d.lgs. n. 24/2023 per beneficiare della tutela dalle ritorsioni, le persone che segnalano, denunciano o effettuano una divulgazione pubblica non incorrono in alcun tipo di responsabilità civile, penale, amministrativa o disciplinare.

Art. 15

Sanzioni

1. Fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie:

- a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'art. 12 del decreto 24 del 10 marzo 2023;
- b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quelle di cui agli articoli 4 e 5 del decreto 24 del 10 marzo 2023 , nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
- c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3 del decreto 24 del 10 marzo 2023, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.

Art. 16

Responsabilità disciplinare

Le violazioni della disciplina whistleblowing costituiscono fonte di responsabilità disciplinare per coloro che:

- hanno commesso ritorsioni, ostacolato o tentato di ostacolare la segnalazione o violato l'obbligo di riservatezza;
- non hanno istituito il canale di segnalazione, non hanno adottato le procedure per l'effettuazione e la gestione delle segnalazioni ovvero hanno adottato procedure non conformi alle previsioni del decreto;
- non hanno svolto le attività di verifica e analisi delle segnalazioni.

È sanzionabile disciplinarmente anche la persona segnalante nel caso in cui ne sia stata accertata, anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o di calunnia ovvero ne sia stata accertata la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

Art. 17

Onere della Prova

Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati ai sensi dell'art. 14 del presente documento, nei confronti delle persone segnalanti, si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all' autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere.

Art. 18

Canale esterno di segnalazione

L'Autorità Nazionale Anticorruzione (ANAC) attiva un canale di segnalazione esterna, che il segnalante può utilizzare nei seguenti casi, come previsto all'art. 6 del D. Lgs n. 24/2023:

- a) il canale di segnalazione interna non è attivo o, anche se attivato, non è conforme a quanto previsto dallo stesso Decreto;
- b) la persona segnalante ha già effettuato una segnalazione interna ai sensi dell'articolo 4 del D. Lgs n. 24/2023 e la stessa non ha avuto seguito;
- c) la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione; d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

La stessa Autorità mette a disposizione sul proprio sito web le indicazioni e le modalità da seguire per utilizzare tale canale.

Art. 19

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.

Art. 20

Comunicazione e formazione

La Provincia di Pisa promuove, a tutela dei segnalanti, un'efficace attività di comunicazione e formazione sui diritti e gli obblighi relativi alla segnalazione degli illeciti, a tutela del pubblico interesse, nell'ambito dei percorsi di formazione sull'etica pubblica e del Codice di comportamento dei pubblici dipendenti.

Art. 21

Trattamento dati personali

I dati personali del soggetto segnalante, del soggetto segnalato e degli altri soggetti eventualmente coinvolti, acquisiti in occasione della presentazione e della gestione delle segnalazioni ai sensi del presente atto, sono trattati in piena conformità a quanto stabilito dalla normativa vigente in materia di protezione dei dati personali e, più precisamente, dal Regolamento europeo 2016/679 (GDPR) e dal D.Lgs. n. 196/2003, come da ultimo modificato e integrato dal D.Lgs. n. 101/2018.

Le operazioni di trattamento consistono nell'acquisizione e registrazione, nella consultazione ed elaborazione da parte del RPCT e dei componenti dell'USRPCT, nella conservazione e nella cancellazione dei dati. Il trattamento viene effettuato dai suddetti soggetti allo scopo di garantire una corretta gestione delle segnalazioni ricevute e ai fini dell'adempimento degli obblighi di legge connessi alla disciplina del "whistleblowing".

I dati trattati sono soltanto quelli strettamente necessari alla gestione della segnalazione e non possono essere utilizzati oltre quanto necessario per dar seguito alla medesima.

I dati personali e le informazioni contenuti nelle segnalazioni possono essere comunicati agli uffici competenti per i relativi adempimenti, così come all'Autorità giudiziaria, a quella contabile e all'ANAC, in ottemperanza degli obblighi di legge.

È garantito agli interessati l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR.

Tuttavia, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati dall'Amministrazione, non può esercitare i diritti previsti dai sopra richiamati articoli del GDPR, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante.

Il Responsabile della protezione dei dati personali vigila sull'adozione da parte del titolare del trattamento di misure idonee a garantirne la protezione.

Art. 22

Disposizioni finali

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

Art. 23

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.



PROVINCIA DI PISA

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

La Provincia di Pisa, nell'ambito delle proprie finalità istituzionali e in adempimento agli obblighi previsti dall'art. 13 del Regolamento UE 2016/679 ("Regolamento"), Le fornisce **informazioni** in merito al trattamento dei dati personali da Lei conferiti al fine di segnalare condotte illecite presso l'amministrazione (**whistleblowing**).

1) TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è la Provincia di Pisa, con sede operativa in via Nenni 30, 56124 Pisa (PI), nella persona del Presidente della Provincia.

2) RESPONSABILE DELLA PROTEZIONE DEI DATI

La Provincia di Pisa ha nominato il "Responsabile della Protezione dei Dati", che può essere contattato scrivendo all'indirizzo di posta elettronica dpo@provincia.pisa.it.

3) CATEGORIE DI DATI PERSONALI, FINALITA' E BASE GIURIDICA DEL TRATTAMENTO

Il trattamento in questione comporta il conferimento – di persona al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), con invio di segnalazione tramite compilazione di un form su apposita procedura web – di dati anagrafici, codice fiscale, dati di contatto e, eventualmente, dati sulla qualifica professionale, nonché di dati e informazioni ulteriori connessi alla condotta illecita riportata. I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi dell'art. 54-bis "Tutela del dipendente pubblico che segnala illeciti" del D.Lgs. n. 165/2001. Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) di Ateneo. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non sia opponibile per legge (ad esempio, indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità del segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione. La base giuridica di tale trattamento è rappresentata dall'art. 6, c. 1, lett. c), del Regolamento (adempimento di un obbligo legale al quale è soggetto il titolare del trattamento). Il trattamento dei dati personali è improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti dell'interessato, nonché agli ulteriori principi previsti dall'art. 5 del Regolamento.

4) MODALITA' DI TRATTAMENTO

Il trattamento dei dati personali verrà effettuato esclusivamente dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), e dal personale di supporto debitamente autorizzato e istruito ai sensi degli art. espressamente autorizzati al trattamento dei dati personali ai sensi degli art. 29 e 32, paragrafo 4 del GDPR e dell'art. 2 quaterdecies del Codice della Privacy, con l'utilizzo di procedure anche informatizzate, dotate di strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d'integrità e riservatezza, anche accidentali.

5) TEMPI DI CONSERVAZIONE

I dati verranno conservati per 5 anni decorrenti dalla data di ricezione della segnalazione, nonché per tutto il periodo necessario allo svolgimento degli eventuali procedimenti scaturenti dalla gestione della segnalazione (disciplinare, penale, contabile). È fatta salva la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie

6) DESTINATARI E CATEGORIE DI DESTINATARI DEI DATI PERSONALI

I dati personali non saranno comunicati ad altri soggetti, ad esclusione dei casi sopra indicati, così come non saranno oggetto di diffusione.

7) CONFERIMENTO DEI DATI

Il conferimento dei dati personali è facoltativo. Il mancato conferimento potrebbe tuttavia pregiudicare l'istruttoria della segnalazione: le segnalazioni anonime, infatti, verranno prese in considerazione solo ove si presentino adeguatamente circostanziate e rese con dovizia di particolari, in modo da far emergere fatti e situazioni connessi a contesti determinati.

8) DIRITTI DEGLI INTERESSATI E MODALITA' DI ESERCIZIO

In qualità di interessato, ha diritto di ottenere dalla Provincia, nei casi previsti dal Regolamento, l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi o la limitazione del trattamento ovvero di opporsi al trattamento medesimo. La richiesta potrà essere presentata, senza alcuna formalità, contattando direttamente il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) all'indirizzo di posta elettronica personale disponibile alla pagina principale della sezione Amministrazione Trasparente. Gli interessati che ritengano che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento UE 2016/679 hanno, inoltre, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

In ogni caso, le disposizioni in materia di diritti dell'interessato sottostanno alle limitazioni di cui all'art. 2-undecies del d.lgs. 30 giugno 2003, n. 196 "limitazioni ai diritti dell'interessato" ai sensi del quale: "i

diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio"

In particolare, l'esercizio di tali diritti:

- potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del segnalante;
- in tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160 del Codice Privacy, nel qual caso il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale.
- La segnalazione e la relativa documentazione ad essa allegata è sottratta al diritto di accesso agli atti amministrativi, previsto dagli artt. 22 e ss. Della Legge 241/1990 e accesso civico generalizzato ex art. 5 del d.Lgs. 33/2013.

Per ogni ulteriore informazione e comunque per inviare la richiesta è possibile rivolgersi all'indirizzo di contatto del Titolare del trattamento.

Pisa 15.07.2026



PROVINCIA DI PISA

**DOCUMENTO DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI
RELATIVI AL TRATTAMENTO NELL'AMBITO DELLA PROCEDURA DI
WHISTLEBLOWING**

(DPIA - DATA PROTECTION IMPACT ASSESSMENT)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento “possa presentare un rischio elevato”.

Titolare del trattamento:

Provincia di Pisa

Legale rappresentante:

Presidente della Provincia Dott. Massimiliano Angori

Responsabile della protezione dei dati (RPD/DPO):

Avv. Marco Giuri

Sede

Piazza Vittorio Emanuele II , n. 14, Pisa

Data

INTRODUZIONE

MOTIVAZIONE DELLA VALUTAZIONE

Il presente documento viene elaborato sulla scorta dell'articolo 35 del Regolamento UE 679/2016.

La valutazione d'impatto si rende necessaria alla luce di un'attenta autoanalisi compiuta circa il trattamento dei dati personali.

La Provincia di Pisa, quale Ente Pubblico, ritiene necessario procedere ad una valutazione di impatto, stante il rischio elevato che il *trattamento di dati personali nell'ambito della procedura di whistleblowing* può avere sui diritti e le libertà delle persone fisiche, in ragione delle caratteristiche di pervasività e possibile intrusione nella sfera dei comportamenti personali, proprie dello stesso .

L'art. 35 del GDPR prevede infatti che “quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Inoltre, al par. 7 il legislatore europeo stabilisce: “la valutazione contiene almeno:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione”.

La valutazione di impatto si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini dall'utilizzo della piattaforma informatica gratuita individuata (Whistleblowing Solutions I.S. S.r.l.).

Il Titolare del trattamento provvederà: - all'adozione di politiche di controllo periodiche in riferimento ai dati oggetto del trattamento in questione e alle misure esistenti o pianificate (misure applicate ai dati, misure generali di sicurezza dei sistemi e misure organizzative); ad effettuare una

precisa e rigorosa manutenzione dei sistemi; alla costante formazione del personale designato/autorizzato al trattamento dei dati. La DPIA viene pubblicata sul sito web della Provincia di PISA, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione - Whistleblowing

CONTESTO

PANORAMICA DEL TRATTAMENTO

Il trattamento oggetto della presente DPIA è relativo alla acquisizione e gestione delle **segnalazioni di illeciti c.d. whistleblowing** ai sensi del **d.lgs. 24 del 10 marzo 2023** che recepisce la **Direttiva UE 1937/2019**.

Responsabilità connesse al trattamento

Provincia di Pisa: titolare del trattamento nella persona del Presidente *pro tempore*.

RPCT dell'Ente: gestore del trattamento è l' RPCT dell'Ente.

WHISTLEBLOWING SOLUTION SRL: responsabile del trattamento

SEE WEB: sub-responsabile del trattamento nominato da whistleblowing solutions srl per la gestione dell'infrastruttura informatica (IaaS).

Transparency International Italia: Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing.

Standard applicabili al trattamento

D. LGS N.24 del 2023

Direttiva UE n.1937/2019

LL. GG. ANAC approvate con Delibera n. 311 del 12 Luglio 2023

LL.GG. ANAC approvate con Delibera n. 478 del 26 Novembre 2025

Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing.

Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:

- ISO/IEC 27001:2022
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- ISO 9001:2015
- CSA STAR Level 1
- ACN

(vedi allegato 1)

DATI, PROCESSI E RISORSE DI SUPPORTO

Categorie di dati trattati

I dati trattati sono quelli inseriti nella segnalazione e nel caso, acquisiti nel corso della conseguente istruttoria. Tali dati possono essere sia dati comuni (identità del segnalante, del segnalato, i ruoli ricoperti dagli stessi), sia dati particolari e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento dei dati (descrizione funzionale)

Il trattamento dei dati oggetto della presente D.P.A. si articola nelle seguenti fasi:

Ricezione e Raccolta: Attivazione della piattaforma, invio della segnalazione, autenticazione e cifratura dei dati.

Gestione e Analisi: Accesso alla piattaforma limitato agli autorizzati, istruttoria, interlocuzione con il segnalante e indagini interne.

Chiusura e feedback: Comunicazione dell'esito della segnalazione al segnalante entro tre mesi dalla conferma di ricezione.

Conservazione e archiviazione: i dati non utili alla gestione non sono raccolti o, se raccolti accidentalmente, eliminati.

La documentazione è conservata per il tempo necessario (non oltre i 5 anni dall'esito finale). Nel caso di contenzioso o segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrebbe essere protratto anche oltre i termini sopraindicati, sino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

Risorse di supporto ai dati

La Provincia di Pisa si avvale, per la gestione delle segnalazioni, di una piattaforma informatica di segnalazione basata su software libero e open-source Global leaks di cui Whistleblowing Solutions è coautore e coordinatore di progetto.

L'infrastruttura IaaS e SaaS privata è basata sulle seguenti tecnologie:

- Dettaglio Hardware
- VMWARE (virtualizzazione)
- Debian Linux LTS (sistema operativo)
- VEEAM (backup)
- OPNSENSE (firewall)
- OPENVPN (vpn).

(Vedi allegato1-Documento di supporto del responsabile del trattamento).

La gestione delle segnalazioni non avviene tramite altri canali. Infatti, anche nell'ipotesi in cui il segnalante chieda un appuntamento a RPCT, quest'ultimo provvederà a inserire la segnalazione raccolta oralmente direttamente nella piattaforma. Tutte le attività istruttorie, avviate in seguito alla segnalazione, sono gestite nell'ambito della piattaforma, così come le comunicazioni con il segnalante, il segnalato ed eventuali ulteriori soggetti (informatori).

PRINCIPI FONDAMENTALI

PROPORZIONALITÀ E NECESSITÀ

Finalità trattamento

Il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento ed è relativo alle procedure c.d. whistleblowing sono trattati esclusivamente per ricevere e gestire le segnalazioni di violazioni presentate ai sensi del D. Lgs. 10 marzo 2023, n. 24, effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e procedere all'adozione di tutti i conseguenti provvedimenti. I dati non sono trattati per ulteriori finalità.

Basi legali che rendono lecito il trattamento

Il trattamento di dati comuni (dati identificativi e di contatto del segnalante, dell'autore delle violazioni o di altre persone a vario titolo coinvolte nelle vicende segnalate) costituisce l'adempimento di un obbligo legale e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR. Nel caso in cui vengano trattati dati appartenenti a categorie particolari, la base giuridica è rappresentata dall'art. 9.2, lett. b) e g) GDPR, in connessione con l'art. 2-sexies, comma 2, lett. dd), del D.Lgs. n.196/2003. Per i dati personali relativi a condanne penali e misure di sicurezza, la base giuridica è rappresentata dall'art. 2-octies, comma 3, lett. a), del D.Lgs. n. 196/2003. I dati personali sono trattati sulla base del consenso espresso del segnalante ai fini della conoscibilità della segnalazione ove la stessa sia necessaria alla difesa dell'incolpato, anche nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023).

Adeguatezza, pertinenza e proporzionalità dei dati in relazione alle finalità per cui sono trattati (minimizzazione dei dati)

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI).

Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia.

Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata.

L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia. Al fine di consentire la possibilità di segnalazioni orali e al contempo tutelare l'anonimato e la confidenzialità, il sistema applica avanzate tecniche di "vocoding" (atte a evitare di raccogliere il timbro vocale) e "pitch shifting" (atte a variare il tono della voce in modo casuale) capaci di offrire elevate caratteristiche di anonimizzazione al passo con la ricerca nello specifico contesto d'uso. Tali tecniche permettono ai riceventi di ascoltare la registrazione senza essere in condizione di

identificare la voce direttamente e rendendo altamente inefficaci tecniche moderne di de-anonimizzazione. Nonostante la registrazione venga protetta sotto questo profilo e venga mantenuta in forma alla pari di ogni allegato della segnalazione, per l'ascolto è indicato l'uso di cuffie per limitare l'esposizione del contenuto del messaggio.

Aggiornamento dati

L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.

Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento. Nel caso di segnalazioni palesemente infondate le stesse vengono immediatamente archiviate. Nel caso di informazioni non coerenti, nell'ambito dell'istruttoria RPCT e i soggetti autorizzati alla gestione della segnalazione possono aggiornare i dati, chiedere eventuali integrazioni o rettifiche che sono comunque inserite nel fascicolo della segnalazione. Inoltre, il segnalante può sempre interloquire con RPCT, tramite la piattaforma, al fine di chiedere la modifica / integrazione delle informazioni trasmesse.

Qual è il periodo di conservazione dei dati?

Le segnalazioni, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023. Nel caso di contenzioso o di segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrà essere protratto anche oltre i termini sopra indicati, fino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

Specificatamente alla piattaforma informatica, come si legge all'allegato 1, sono previste:

- Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati.

- Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte.

- Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Informativa privacy interessati

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità:

- Comunicazione a tutti i dipendenti sull'esistenza del canale di segnalazione interno;
- Pubblicazione sito web istituzionale – sezione dedicata al Whistleblowing.

Consenso degli interessati

Il trattamento dei dati personali acquisiti con la segnalazione e nell'ambito delle successive attività istruttorie non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR. Il consenso degli interessati costituisce la base giuridica unicamente per la comunicazione dell'identità del segnalante al segnalato, ove la stessa sia necessaria alla difesa dell'incolpato nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023). La piattaforma consente di raccogliere il consenso del segnalante per tale fine al momento dell'invio della segnalazione, tramite apposito form.

Esercizio diritti di accesso e di portabilità dei dati

Quanto al diritto di accesso, si segnala che tale diritto non appare immediatamente esercitabile poiché limitato ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (...) f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993,

n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58". L'interessato può comunque avanzare la richiesta ai dati di contatto indicati dal Titolare del trattamento nell'informativa fornita ai sensi degli artt. 13 e 14 oppure contattando direttamente il Data Protection Officer nominato dall'Ente. La Provincia di Pisa effettuerà tutte le valutazioni del caso, tenendo sempre in considerazione l'obbligo di garantire la riservatezza del segnalante.

Esercizio diritti di rettifica e di cancellazione (diritto all'oblio)

Il diritto alla cancellazione non è applicabile al caso di specie, ai sensi dell'art. 17, par. 3, GDPR a norma del quale: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: (...) b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse".

Esercizio diritti di limitazione e di opposizione

Il diritto alla limitazione non appare esercitabile, ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (...) f) alla riservatezza dell' identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58.

Non è previsto il riconoscimento del diritto di opposizione, sussistendo motivi legittimi cogenti per procedere al trattamento, in considerazione delle finalità di interesse pubblico perseguite, degli interessi connessi al buon andamento della PA, nonché della necessità e proporzionalità del trattamento medesimo.

Formalizzazione obblighi dei responsabili del trattamento

Whistleblowing PA Srl è stata formalmente nominata quale Responsabile del trattamento (All. 2). La Nomina risponde ai criteri di cui all'art. 28 GDPR.

Tutela dati in caso di trasferimento di dati al di fuori dell'Unione europea

Non è previsto alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

RISCHI

MISURE ESISTENTI O PIANIFICATE

Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLabs rating A+.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Protocollo crittografico: <https://docs.globaleaks.org/en/stable/security/EncryptionProtocol.html>

Tracciabilità

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

Archiviazione

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM.

Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

Vulnerabilità

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.

A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.

Audit di sicurezza: <https://docs.globaleaks.org/en/stable/security/PenetrationTests.html>

Backup

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

Manutenzione

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Sicurezza dell'hardware

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.

I datacenter del fornitore IaaS sono certificati ISO27001.

Lotta contro il malware

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware.

Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Sicurezza dei canali informatici

Tutte le connessioni sono protette tramite protocollo TLS 1.2+

Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

Sicurezza dei documenti cartacei

La sicurezza dei documenti cartacei è garantita attraverso le seguenti misure:

- attività di trattamento dei dati riservata al solo personale autorizzato;
- accesso agli archivi e/o ad altro luogo in cui sono custoditi dati su supporto cartaceo al solo personale autorizzato;
- sensibilizzazione e formazione di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali;
- il trattamento dei dati (specie di quelli sensibili o particolari) deve avvenire solo all'interno dei locali protetti dell'Ente ed accessibili solo agli autorizzati;
- dotazione di sistemi di videosorveglianza;
- chiusura delle porte di accesso dei locali;
- guardiania portierata;
- chiusura a chiave degli archivi;
- armadi e contenitori dotati di serrature.

Il trattamento dei dati (specie di quelli sensibili o particolari) deve avvenire solo all'interno dei locali protetti dell'Ente ed accessibili solo agli autorizzati.

ACCESSO ILLEGITTIMO AI DATI

Principali impatti sugli interessati se il rischio si dovesse concretizzare

- Condotte ritorsive (il licenziamento, la sospensione o misure equivalenti, la retrocessione di grado o la mancata promozione, il mutamento di funzioni, il cambiamento del luogo di lavoro, la

riduzione dello stipendio, la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria, la coercizione, l'intimidazione, le molestie o l'ostracismo, la discriminazione o comunque il trattamento sfavorevole, la 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, il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche la perdita di redditi, l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro, la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso, la richiesta di sottoposizione ad accertamenti psichiatrici o medici).

- Conseguenze di carattere reputazionale
- Difficoltà nelle relazioni lavorative e sociali
- Aumento stress lavorativo
- Estorsione (anche sotto forme di tentativo) .
-

Principali minacce che potrebbero concretizzare il rischio

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco criptolocker che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;
- Spamming, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati. Il rischio de quo è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server,

che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione;

- Furto di credenziali di autenticazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;
- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati), o verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

Fonti di rischio

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente).

Fonti non umane: (acqua, materiali pericolosi, virus informatici generici).

Misure fra quelle individuate contribuiscono a mitigare il rischio

- Crittografia
- Tracciabilità
- Archiviazione
- Vulnerabilità
- Backup
- Manutenzione
- Sicurezza dell'hardware
- Lotta contro il malware
- Sicurezza dei canali informatici
- Controllo degli accessi logici
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Sicurezza dei documenti cartacei

Gravità del rischio alla luce degli impatti potenziali e delle misure pianificate

Importante

Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

In particolare condotte ritorsive (il licenziamento, la sospensione o misure equivalenti, la retrocessione di grado o la mancata promozione, il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria, la coercizione, l'intimidazione, le molestie o l'ostracismo, la discriminazione o comunque il trattamento sfavorevole, la 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, il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro, la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso, la richiesta di sottoposizione ad accertamenti psichiatrici o medici).

Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Limitata

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte e come rappresentate nell'All. 1) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy. In particolare, le misure di sicurezza approntate proteggono la riservatezza dell'identità sia del whistleblower, sia della persona segnalata, sia di qualsiasi altra persona comunque menzionata nella segnalazione, nonché la riservatezza del contenuto della segnalazione e della relativa documentazione. Ciò è garantito anche tramite il ricorso a strumenti di crittografia.

MODIFICHE INDESIDERATE DEI DATI

Principali impatti sugli interessati se il rischio si dovesse concretizzare

Ingiusto coinvolgimento del segnalato in procedimenti disciplinari e/o giudiziari,, Condotte ritorsive di cui all' art. 12 d.lgs 24/2023

Principali minacce che potrebbero consentire la concretizzazione del rischio

- Negligente custodia delle credenziali di accesso alla Piattaforma;
- Utilizzo improprio / cessioni di credenziali per l'accesso alla Piattaforma;
- Intercettazioni delle trasmissioni o dei dati;
- Data Breach subito dai Responsabili del trattamento;
- Violazione della piattaforma da parte di attaccanti esterni.

Fonti di rischio

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente),

Fonti non umane: Possono essere un incidente o un sinistro verificatosi presso uno dei soggetti incaricati del trattamento (interruzioni di corrente, incendio, inondazione, ecc.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Crittografia
- Tracciabilità
- Vulnerabilità
- Controllo degli accessi logici
- Backup
- Manutenzione
- Archiviazione
- Sicurezza dell'hardware
- Lotta contro il malware
- Sicurezza dei canali informatici
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Sicurezza dei documenti cartacei

Gravità del rischio alla luce degli impatti potenziali e delle misure pianificate

Importante

La gravità del rischio è valutata importante in considerazione delle categorie dei soggetti interessati (soggetti segnalanti oggetto di possibili condotte ritorsive, ma anche soggetti segnalati passibili di procedimenti disciplinari o giudiziari a loro carico), nonché delle possibili conseguenze a carico degli stessi in caso di violazione dell'integrità dei dati.

Probabilità del rischio con riguardo a minacce, fonti di rischio e misure pianificate

Limitata

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy.

PERDITA DI DATI

Impatti principali sugli interessati se il rischio dovesse concretizzarsi

Mancata definizione dell'istruttoria e conseguenti possibili problematiche di natura giuslavoristica e contrattuale.

Principali minacce che potrebbero consentire la materializzazione del rischio

- Data Breach subito dai Responsabili del trattamento;
- Violazione della piattaforma da parte di attaccanti esterni;
- Furto di credenziali di autenticazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;
- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati);

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco criptolocker che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;
- Spamming, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati;
- Il rischio de quo è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server, che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione;
- Verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

Fonti di rischio

Fonti non umane: es. acqua, materiali pericolosi, virus informatici generici);

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente).

Quali misure contribuiscono a mitigare il rischio

Sicurezza dei canali informatici

Crittografia

Archiviazione

Tracciabilità

Vulnerabilità

Manutenzione

Backup

Lotta contro il malware

Sicurezza dell'hardware

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

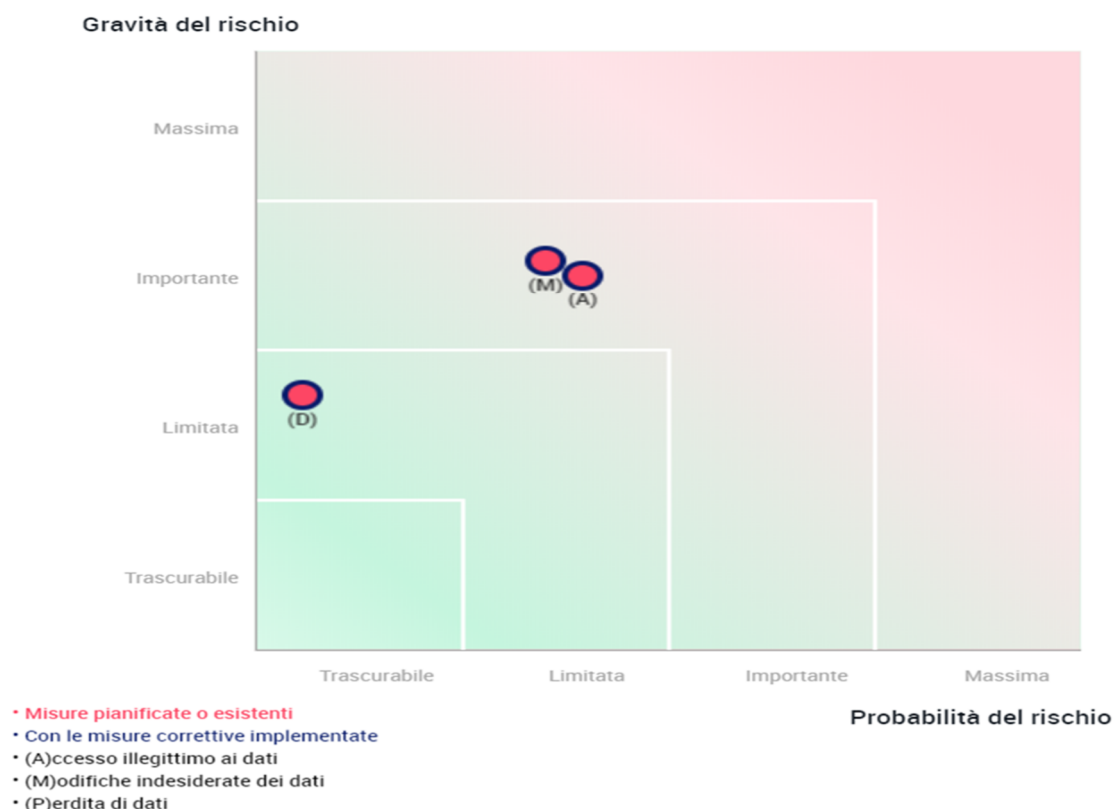
Controllo degli accessi logici

Gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate

Limitata, la perdita indesiderata dei dati potrebbe comportare ricadute nell'iter amministrativo dei processi dell'Ente, comportando possibili ricadute di natura contrattuale rispetto agli interessati. Tali difficoltà risultano comunque superabili anche se con spendita di tempo e di risorse dedicate alle necessarie rettifiche / integrazioni.

Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Trascurabile, le politiche di gestione della vulnerabilità, nonché i sistemi di backup adottati dal Responsabile del trattamento riducono la probabilità del rischio.



31/03/26

Ai sensi del paragrafo 2, art. 35 del GDPR si consulta il responsabile della protezione dei dati: questo viene sempre coinvolto nelle decisioni dell'Ente e viene richiesto il suo parere su singole questioni o quesiti che hanno a che fare con il trattamento dei dati personali.

Anche il presente documento verrà sottoposto al suo vaglio finale.

PARERE DEL DPO: POSITIVO rilasciato dall'Avvocato Marco Giuri in data 23 Aprile 2026.

CONCLUSIONI

Si ritiene che le contromisure adottate in vista di un rischio iniziale, determinato come alto, possano ragionevolmente abbassarlo ad un livello di sicura gestibilità da parte del Titolare.

In quest'ottica, si ritiene superflua, in accordo con il DPO, la consultazione preventiva dell'Autorità Garante, ai sensi e per gli effetti dell'art. 36 Regolamento UE 679/2016, in considerazione anche della disponibilità dell'Ente all'adozione di un graduale piano di adeguamento per assicurare la migliore sicurezza e protezione dei dati trattati da parte della Provincia.

Il Titolare del trattamento, in persona del Direttore Generale pro tempore, preso atto delle valutazioni sopra riportate in ordine all'analisi del potenziale impatto per i diritti e le libertà degli interessati, con l'adozione della presente DPIA, dispone che il documento sia reso pubblico sul sito internet istituzionale nell'apposita sezione WHISTLEBLOWING.

Il Direttore Generale/Segretario Generale
Dott. Danilo D'Aco



PROVINCIA DI PISA

**Istituzione dei Comuni per il governo dell'area vasta
Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente
Gestione associata di servizi e assistenza ai Comuni**

SEGRETERIA GENERALE

PARERE DI REGOLARITA' TECNICA

Sulla proposta di Decreto n. 2302/2026

ad oggetto: PROCEDURA DI SEGNALAZIONE DI VIOLAZIONI DI DISPOSIZIONI
NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE
PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE PUBBLICA - DISCIPLINA DELLA
TUTELA DELLA PERSONA CHE SEGNALE VIOLAZIONI (D.LGS N. 24 DEL 10 MARZO
2023) C.D. WHISTLEBLOWING -AGGIORNAMENTO ATTO ORGANIZZATIVO.

si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere
FAVOREVOLE in ordine alla regolarita' tecnica.

Pisa li, 15/07/2026

Sottoscritto dal Dirigente

(D'ACO DANILO)
con firma digitale