AREA AMMINISTRATIVA

Settore Affari Generali

Servizio Segreteria

DECRETO SINDACALE N. 17 del 06.11.2026

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI OCCASIONATO DA SEGNALAZIONI AI SENSI DELLA NORMATIVA IN MATERIA DI "WHISTLEBLOWING"

Oggetto: Misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n. 2016/679 – Atto di designazione del Responsabile per la Prevenzione della Corruzione e Trasparenza (RPCT), in relazione al trattamento dei dati personali, e conseguente attribuzione al soggetto designato di specifici compiti e funzioni, con delega all'esercizio ed allo svolgimento degli stessi secondo analitiche istruzioni impartite.

IL TITOLARE DEL TRATTAMENTO

VISTO il Decreto Legislativo 10 marzo 2023, n. 24, di 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 (di seguito, per brevità, semplicemente "Decreto");

CONSIDERATO CHE, a norma dell'articolo 1 del Decreto:
- "*I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano, ai sensi del presente articolo, propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto*" (comma 1);
- "*La gestione del canale di segnalazione è affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato*" (comma 2);
- "*I soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna*" (comma 5);

CONSIDERATO CHE, a norma dell'articolo 12 del Decreto:
- "*L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196*" (comma 2);
- "*I soggetti del settore pubblico e del settore privato, l'ANAC, nonché le autorità amministrative cui l'ANAC trasmette le segnalazioni esterne di loro competenza, tutelano l'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante*" (comma 7);

CONSIDERATO CHE, a norma dell'articolo 13 del Decreto:
- "*Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51*" (comma 1);
- "*I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4, in qualità di titolari del trattamento, nel rispetto dei princìpi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati*" (comma 4);
- "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*" (comma 6);

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo RGPD);

RILEVATO CHE, ai fini dell'osservanza delle disposizioni contenute nel RGPD, vanno innanzitutto individuati gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali;

RILEVATO CHE negli enti locali, per specifica disposizione legislativa (articolo 1, comma 7 della Legge 6 novembre 2012, n. 190) il Responsabile per la Prevenzione della Corruzione e Trasparenza (RPCT) è individuato, di norma, nel Segretario, salvo diversa e motivata determinazione.

RILEVATO CHE nelle Unioni di comuni, per specifica disposizione legislativa (articolo 1, comma 7 della Legge 6 novembre 2012, n. 190), può essere nominato un unico RPCT, le cui funzioni sono attribuite dal Presidente della Giunta al segretario comunale dell'unione o di uno dei comuni aderenti o a un dirigente apicale, salvo espresse e motivate eccezioni, in coerenza con quanto previsto articolo 1, comma 7 della Legge 6 novembre 2012, n. 190.

CONSIDERATO CHE, conformemente alle disposizioni del RGPD (articolo 29), e della normativa interna di adeguamento (articolo 2-quaterdecies del Decreto Legislativo 30 giugno 2003, n. 196)), il Titolare del trattamento può designare, sotto la propria responsabilità, ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati;

DATO ATTO che si rende necessario procedere alla designazione delle persone fisiche aventi specifici compiti e funzioni connessi al trattamento dei dati personali ed alla delega dell'esercizio e dello svolgimento di tali specifici compiti e funzioni alle persone fisiche designate;

RITENUTO di attribuire al RPCT, gli specifici compiti e funzioni spettanti al Titolare ed analiticamente elencati in calce al presente atto, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo;

CONSIDERATA la struttura organizzativa e l'organigramma funzionale degli Uffici e dei servizi di questo Ente;

VISTO l'atto organizzativo adottato dal Titolare con deliberazione di Giunta n. 98 del 15.10.2024, per l'assolvimento degli obblighi previsti dal Decreto;

DATO ATTO che presso l'Ente è nominato quale Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT):

NOME E COGNOME
CRISTINA BLOISE

STABILISCE

DI DESIGNARE, con decorrenza dalla data di ricezione del presente provvedimento, il summenzionato soggetto che opera sotto la diretta autorità del Titolare, quale persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali e relativi ai trattamenti conseguenti alla ricezione delle segnalazioni pervenute in applicazione della normativa in materia di whistleblowing, dando atto che i compiti e funzioni attribuite devono essere svolti:

- presso la sede del Titolare e le sue articolazioni territoriali;
- nell'ambito e conformemente alle istruzioni contenute nel presente atto di designazione.

DI ATTRIBUIRE, con decorrenza dalla data di ricezione del presente provvedimento, al summenzionato, i compiti e le funzioni analiticamente elencate in calce al presente provvedimento, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti il trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma conferisce soltanto il potere/dovere di svolgere i compiti le funzioni attribuite dal Titolare;

DI DELEGARE, per effetto di quanto sopra indicato e con decorrenza dalla data di ricezione del presente provvedimento al summenzionato l'esercizio e lo svolgimento di tutti i compiti e di tutte le funzioni attribuite dal Titolare, ed analiticamente elencate in calce al presente provvedimento, con facoltà di successiva integrazione e/o modificazione;

DI DARE ATTO che il summenzionato, assume, con decorrenza dalla data di ricezione del presente atto di designazione, attribuzione e delega, il ruolo di soggetto autorizzato e designato per il trattamento dei dati personali con delega a svolgere i compiti e le funzioni attribuiti dal Titolare medesimo:

DI DARE ATTO, altresì, che:

- tale ruolo ha validità per l'intera durata dell'incarico di Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT);
- tale ruolo viene a cessare al modificarsi dell'incarico di Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT);
- tale ruolo viene a cessare in caso di revoca espressa;
- al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto del presente provvedimento, salvo che ciò sia imposto o consentito da una norma di legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

DI DISPORRE la comunicazione personale, con rilascio di apposita dichiarazione di ricevimento del presente provvedimento.

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI AL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE E TRASPARENZA (RPCT) E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI DERIVANTI DA SEGNALAZIONI AI SENSI DELLA NORMATIVA IN MATERIA DI "WHISTLEBLOWING" SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

• identificare contitolari, responsabili e sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni ed i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
• ove necessario, identificare e designare, per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti lo svolgimento delle attività di competenza, le persone fisiche che operano sotto la diretta autorità del Titolare ed attribuire alle medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni e controllando costantemente che le persone fisiche designate, delegate e autorizzate al trattamento dei dati effettuino le operazioni di trattamento:
- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»;
- in attuazione del principio di «limitazione della conservazione»;
- in attuazione del principio di «integrità e riservatezza»;
- in attuazione del principio di «liceità, correttezza e trasparenza».
• effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti in relazione all'espletamento dei propri compiti e funzioni di RPCT, in relazione alle segnalazioni previste dal Decreto;
• effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
• effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati;
• effettuare, prima di procedere al trattamento, quando questo può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;

• prima di procedere al trattamento, consultare l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
• mettere in atto le misure tecniche ed organizzative adeguate e funzionali a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
• mettere in atto le misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
a) tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
b) dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica
• proporre e suggerire al Titolare misure tecniche ed organizzative ritenute necessarie a garantire la protezione dei dati dal trattamento, in relazione alle funzioni di competenza;
• contribuire alla tenuta del registro delle attività di trattamento in relazione ai trattamenti di competenza;
• cooperare, su richiesta, con il RPD/DPO e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
• in caso di violazione dei dati personali, collaborare con il Titolare, il RPD/DPO nel processo di notifica della violazione all'Autorità di controllo competente senza ingiustificato ritardo e, comunque, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
• in caso di violazione dei dati personali, comunicare la violazione all'Interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
• assicurarsi che il RPD/DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
• sostenere il RPD/DPO nell'esecuzione dei compiti assegnati, fornendogli le risorse necessarie per assolvere tali compiti, per accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica;

• documentare e tracciare, per iscritto, ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;
• documentare tutte le attività e gli adempimenti delegati e, in ogni caso, tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;
• controllare e monitorare la conformità dell'analisi, della valutazione dei rischi e della valutazione di impatto nonché controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;
• tracciare documentalmente le attività di controllo e monitoraggio mediante periodici report/resoconti/referti da sottoporre al Titolare ed al RPD/DPO;
• conformare il trattamento ai pareri ed indicazioni del RPD/DPO e dell'Autorità di controllo nonché alle linee guida ed ai provvedimenti dell'Autorità di controllo;
• attuare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto;
• promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
• effettuare ogni ulteriore attività, anche se non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa di riferimento.

SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI, in generale:

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, il RPCT deve attenersi alle seguenti ulteriori istruzioni:

- in attuazione del principio di «liceità, correttezza e trasparenza»,
    - le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini della gestione delle segnalazioni previste dal Decreto, nell'osservanza delle tecniche e metodologie in atto;
    - autorizzazione a comunicare od eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui il RPCT è preposto;
- in attuazione del principio di «limitazione della finalità» il trattamento dev'essere conforme alle finalità previste dal Decreto e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, ed obbligo di verificare la

pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;

- in attuazione del principio di «limitazione della conservazione»
  - conservare i dati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e, comunque, nel rispetto dei termini di conservazione previsti dal Decreto;
  - obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nella struttura di competenza, dati personali non necessari o divenuti ormai superflui;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare,
  - riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
  - non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
  - evitare di inviare, per fax, documenti in chiaro contenenti dati personali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice). In alternativa, si suggerisce di avvisare preventivamente il destinatario della comunicazione fax in modo che possa curarne la diretta ricezione;
  - evitare di utilizzare la posta elettronica non certificata e, in ogni caso, trasmettere documento in formato crittografato e protetti da password, utilizzando altro canale di comunicazione per l'invio della chiave di decrittazione;
- In attuazione del principio di «trasparenza»:
  - accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
  - fornire all'Interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 ed all'articolo 34 del GDPR, relative al trattamento utilizzando la modulistica all'uopo predisposta dal Titolare. Se richiesto dall'Interessato, le informazioni medesime possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato;
  - conservare, nel rispetto del principio di accountability, tutte le versioni delle informative in uno specifico archivio interno cartaceo e telematico e tenere traccia di tutte le modifiche al testo (connesse alle modifiche organizzative, tecniche e normative) al fine di consentire al Titolare una maggiore tutela in sede amministrativa e/o

giudiziaria nel caso di reclami o procedimenti giudiziari per risarcimento di danni conseguenti a trattamenti illeciti di dati;

- agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del RGPD, nel rispetto delle limitazioni disposte dal Decreto;

SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI, in particolare:

Modalità di segnalazione

I canali di segnalazione interna sono stabiliti dal Titolare con apposito atto organizzativo. E' tuttavia stabilito l'utilizzo, quale canale preferenziale di segnalazione, di una piattaforma informatica dedicata.
La piattaforma rilascia alla persona l'attestazione di avvenuta segnalazione e un codice numerico che permette di accedere alla segnalazione, verificare la risposta del RPCT e dialogare rispondendo a richieste di chiarimenti o approfondimenti.
Le segnalazioni Whistleblowing eventualmente pervenute in busta chiusa devono essere gestite con la dovuta cautela.
Il RPCT deve assicurarsi che la busta chiusa ricevuta non presenti segni di violazione del suo contenuto.
Gli atti o i documenti contenuti nella busta non devono mai essere lasciati incustoditi o privi di controllo: occorre pertanto dotarsi di adeguati strumenti di sicurezza, come cassetti con serratura o altri accorgimenti aventi funzione equivalente, idonei a proteggere i documenti da accessi non autorizzati.
Il RPCT deve ricorrere agli strumenti di sicurezza predisposti per la tutela di atti e documenti contenenti dati personali prima di assentarsi dal posto di lavoro, anche per assenze di breve durata.
Il RPCT deve prestare particolare cura e attenzione quando i documenti in suo possesso contengono dati particolari o giudiziari o, comunque, consentano l'identificazione delle persone fisiche tutelate dal Decreto.
L'accesso ai documenti ed alle informazioni relativi a segnalazioni (c.d. whistleblowing) è consentito solo al RPCT e al personale da questi espressamente autorizzato.

Istruzioni specifiche in merito al regime delle Tutele previste per il whistleblowing:

Fatto in ogni caso espresso richiamo e rinvio a quanto previsto dal Decreto:
- l'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
- la protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- la segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;

- la protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

In caso di avviso di procedimento disciplinare l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità e di comunicazione scritta delle ragioni di tale rivelazione.

La tutela dell'identità della persona coinvolta e della persona menzionata nella segnalazione va garantita fino alla conclusione dei procedimenti avviati in ragione della segnalazione e nel rispetto delle medesime garanzie previste in favore della persona segnalante.

La persona segnalata può essere sentita anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti. Tale soggetto non ha il diritto di essere sempre informato della segnalazione che lo riguarda ma solo nell'ambito del procedimento eventualmente avviato nei suoi confronti a seguito della conclusione della gestione della segnalazione e nel caso in cui tale procedimento sia fondato in tutto o in parte sulla segnalazione.

Pietra Ligure lì 06.11.2026

Il Titolare del Trattamento
Il Sindaco
Luigi DE VINCENZI

Luigi De
Vincenzi
06.11.2026
10:17:13
GMT+01:00

Dichiarazione di ricevimento dell'atto di designazione, autorizzazione e delega soprascritto e di impegno all'assunzione ed all'esercizio dei compiti, delle funzioni e delle responsabilità attribuite e delegate

il sottoscritto Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT),

Dichiara

1. di aver ricevuto il sovrascritto atto di designazione, attribuzione e delega di funzioni e responsabilità per il trattamento dei dati personali nell'ambito delle proprie funzioni;
2. di aver attentamente letto e compreso il contenuto di tale atto, e di impegnarsi ad attuare la delega;
3. di dare atto che l'obbligo di riservatezza correlato al ruolo assunto va osservato anche per il tempo successivo alla cessazione dell'incarico medesimo.

Pietra Ligure lì 06.11.2026

Il Responsabile
della Prevenzione della Corruzione
e Trasparenza (RPCT)
Dott.ssa Cristina Bloise

CRISTINA
BLOISE
06.11.2026
11:22:07
GMT+01:00