VALUTAZIONE DI IMPATTO PRIVACY
SUI DIRITTI E LE LIBERTÀ
DEGLI INTERESSATI DEL TRATTAMENTO:
Gestione segnalazioni Whistleblowing

Autore	**Legale rappresentante pro tempore**, con la collaborazione del Referente privacy dell'Ente
Revisore	**Referente privacy** Dott.ssa Bandaccari
Parere	**Responsabile Protezione Dati (RPD/DPO)** Avv. Paolo Musacchio per Cap&G Consulting srl
Validatore	**Legale rappresentante pro tempore**, con la collaborazione del Referente privacy dell'Ente
Data	11 luglio 2023

1. CONTESTO DEL TRATTAMENTO

Trattamento in considerazione

Il trattamento ha per oggetto eventuali segnalazioni (whistleblowing) di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato, effettuate da parte dei dipendenti del Comune e dei lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'Ente.
Il Consiglio dei ministri in data 10 marzo 2023 (in vigore dal 15 luglio) ha approvato in via definitiva il D. Lgs n. 24/2023 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".
In esso vi sono maggiori garanzie a tutela della riservatezza della identità del segnalante, della persona coinvolta o menzionata, del contenuto e della relativa documentazione. L'ANAC, sentito il Garante per la protezione dei dati personali, ha adottato linee guida relative alla procedura di presentazione e la gestione delle segnalazioni esterne.
Tali Linee Guida prevedono uso di modalità informatiche e strumenti di crittografia per garantire la riservatezza della persona segnalante, della persona coinvolta o menzionata nella segnalazione e della relativa documentazione. I dati personali dei segnalanti devono essere "minimizzati". Ciò significa che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.
Tra le finalità della normativa in materia vi è quella di offrire tutela, ed assicurare la riservatezza dell'identità del segnalante che faccia emergere condotte e fatti illeciti.
I dati presenti nelle segnalazioni pervengono, per iscritto, oralmente o attraverso la pagina "Whistleblowing" del sito web dell'Ente (che ha implementato l'apposito software di ANAC), e sono trattati, esclusivamente dal Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT) dell'Ente, che funge anche da custode dell'identità del segnalante.
Ai sensi dell'art. 4, c. 5, del d.lgs. n. 24/2023, 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.
Ai sensi dell'art. 5, c. 1. del d.lgs. n. 24/2023, nell'ambito della gestione del canale di segnalazione interna, la persona o l'ufficio interno ovvero il soggetto esterno, ai quali è affidata la gestione del canale di segnalazione interna svolgono le attività necessarie per dare riscontro alla segnalazione, mettendo a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne.
Il d.lgs. n. 24/2023 dedica le seguenti disposizioni alla riservatezza del segnalante:
<u>Art. 12 - Obbligo di riservatezza</u>
1. Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.
2. L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identita' 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.
3. Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale.
4. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identita' della persona segnalante non puo' essere rivelata fino alla chiusura della fase istruttoria.
5. Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.
6. È dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, nella ipotesi di cui al comma 5, secondo periodo, nonché nelle procedure di segnalazione interna ed esterna di cui al presente capo quando la rivelazione della identità della persona segnalante e delle informazioni di cui al comma 2 è indispensabile anche ai fini della difesa della persona coinvolta.
7. 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'identita' 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.
8. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.
9. Ferma la previsione dei commi da 1 a 8, nelle procedure di segnalazione interna ed esterna di cui al presente capo, la persona coinvolta puo' essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

Art. 13 - Trattamento dei dati personali

1. 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. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE) 2018/1725.
2. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.
3. I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.
4. 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 principi 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 liberta' degli interessati.
5. I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.
6. 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.

Responsabilità connesse al trattamento

L'Amministrazione Comunale è il Titolare del trattamento dei dati personali acquisiti mediante le segnalazioni.
Il Titolare:

- definisce le linee organizzative per l'applicazione della normativa di settore;
- effettua, quando previste, le notificazioni al Garante per la protezione dei dati personali, attraverso i vertici apicali dell'organizzazione amministrativa dell'Ente;
- detta le linee guida di carattere fisico, logistico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti;
- vigila sull'osservanza delle disposizioni impartite;
- cura gli adempimenti relativi alla protezione dei dati personali, quali l'aggiornamento del registro dei trattamenti, la valutazione di impatto privacy sui diritti e le libertà degli interessati (DPIA), l'attuazione delle misure di sicurezza adeguate al rischio del trattamento.

Al RPCT è affidata la responsabilità amministrativa del sistema di segnalazione.
Il Comune, nella sua qualità di titolare del trattamento dei dati personali adempie agli obblighi di svolgimento della valutazione di impatto privacy e della notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi e per gli effetti degli articoli 35 e 36, RGPD.
I dati possono essere trattati anche da parte dei soggetti esterni come ANAC, Titolare autonomo del trattamento nonché da parte del personale dell'Ente, eventualmente individuato e designato con apposita nomina a "soggetto autorizzato" al trattamento.
Non vi sono Responsabili del trattamento.

Standard applicabili al trattamento

Fonti Normative:
- Regolamento UE n. 2016/679 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 ("RGPD");
- D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- Direttiva UE 2019/1937;
- D.Lgs. 24 marzo 2023, n. 24;
- Linee Guida ANAC sul whistleblowing.

Categorie di dati trattati

I dati trattati sono i dati conferiti dal segnalante, che possono appartenere alla categoria dei dati comuni (identificativi, anagrafici), nonché a categorie particolari di dati personali (art. 9, GDPR) e alla categoria dei dati relativi a condanne penali o reati (art. 10, GDPR).

Ciclo di vita del trattamento dei dati

Le segnalazioni pervengono, per iscritto, oralmente o attraverso la pagina "Whistleblowing" del sito web dell'Ente (che ha implementato l'apposito software di ANAC), al Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT) dell'Ente, che funge anche da custode dell'identità del

segnalante. Tale figura si occupa della gestione del canale di segnalazione, della custodia di eventuali documenti su supporto cartaceo (cfr. art. 14, commi da 2 a 4 del d.Lgs. 24 marzo 2023, n. 24), nonché dell'istruttoria e del riscontro della segnalazione.
Risorse di supporto ai dati Apparecchiature e strumenti elettronici. Fascicoli su supporto cartaceo.
Eventuali destinatari dei dati (con specifico riferimento ad eventuali Titolari Autonomi) I dati personali trattati potranno essere comunicati ai seguenti soggetti: - Autorità Nazionale Anticorruzione (ANAC); - Corte dei Conti; - Autorità Giudiziaria e Polizia Giudiziaria. I dati personali non possono essere oggetto di comunicazione nell'ambito delle procedure di trasparenza cui il Titolare del trattamento è soggetto (quali ad esempio diritto di accesso documentale, diritto di accesso civico, ecc.). I dati non saranno oggetto di diffusione.

2. VALUTAZIONE PRINCIPI FONDAMENTALI

Scopi del trattamento. Il trattamento dei dati personali forniti dal segnalante risulta necessario per: a) acquisire le segnalazioni di presunte condotte illecite, delle quali sia venuto a conoscenza l'interessato in ragione del proprio rapporto di servizio con il Titolare, commesse dai soggetti che a vario titolo interagiscono con il medesimo; b) effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione; c) adottare eventuali e conseguenti provvedimenti.
Basi giuridiche. La base giuridica di liceità del trattamento dei dati personali "comuni" è rinvenibile, per tutte le finalità, nell'art. 6, par.1, lettera e), RGPD, poiché il trattamento è necessario per l'esecuzione di compiti di interesse pubblico o comunque connessi all'esercizio dei pubblici poteri del Titolare, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità del Titolare. Per il trattamento di dati "particolari", la base giuridica è invece rappresentata dall'assolvimento di obblighi e dall'esercizio di diritti specifici del Titolare del trattamento e dell'Interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), RGPD), nonché dall'esecuzione di un compito di interesse pubblico rilevante assegnato dalla legge al Titolare (art. 9, par. 2, lett. g), RGPD), ai sensi dell'art. 2-sexies lett. dd) del D.lgs. 196/2003 e s.m.i. Per il trattamento dei dati relativi a condanne penali e reati, infine, la base giuridica, ai sensi dell'art. 10, RGPD, è rappresentata dall'obbligo di legge cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), RGPD) e dall'esecuzione di compiti di interesse pubblico assegnati dalla legge al Titolare (art. 6, par. 1, lett. e), RGPD), in ragione dell'art. 2-octies, lett. a) del D.lgs. 196/2003 e s.m.i.
Adeguatezza, pertinenza e limitatezza dei dati raccolti. I dati personali oggetto di trattamento vengono: a) trattati in modo lecito e secondo correttezza per le finalità istituzionali; b) raccolti e registrati per le finalità consentite e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di attività non incompatibili con tali scopi; c) raccolti in modo pertinente, completo e non eccedente, rispetto alle finalità per le quali sono raccolti o successivamente trattati.
Esattezza e aggiornamento dei dati. I dati sono trattati nel rispetto dei principi di esattezza e aggiornamento.
Tempi di conservazione. Come imposto dall'art. 14, d. lgs. n. 24/2023, le segnalazioni, interne ed esterne, e la relativa

documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Esercizio dei diritti degli interessati

Con riferimento all'esercizio dei diritti degli interessati, disciplinati dagli artt. 15-22 del GDPR, si tenga conto che è prevista una loro limitazione, in correlazione con l'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196, di talché non potranno essere esercitati, per previsione di legge, i diritti da cui possano derivare pregiudizi effettivi e concreti:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
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, nonché agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

Rapporti con i responsabili del trattamento

Non vi sono responsabili del trattamento.

Garanzie riguardanti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali

Non sono previsti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali.

2.1 TABELLA VALUTAZIONE PRINCIPI FONDAMENTALI

Principi fondamentali		
Finalità		
Basi legali		
Adeguatezza, pertinenza, limitatezza dei dati		
Esattezza e aggiornamento dei dati		
Periodo di conservazione		
Informativa		
Raccolta del consenso		
Diritto di accesso e alla portabilità dei dati		
Diritto di rettifica e di cancellazione		
Diritto di limitazione e di opposizione		
Responsabilità del trattamento		
Trasferimenti di dati		

Descrizione della valutazione

I principi fondamentali appaiono soddisfatti, con l'eccezione di due criticità:

- INFORMATIVA: l'informativa sul trattamento non è disponibile nel sito web del Comune, pertanto, non appare soddisfatto appieno il principio di correttezza e trasparenza verso gli interessati;
- RESPONSABILITA' DEL TRATTAMENTO: è necessario designare i soggetti che trattano i dati presenti nelle segnalazioni di fatti illeciti quali soggetti delegati/autorizzati al trattamento dei dati personali.

Alla luce di tali valutazioni, si impongono:

- è necessario pubblicare l'informativa nel sito web del Comune, la cui elaborazione spetta al DPO dell'Ente;
- è necessario designare il RPCT (Segretario Comunale), soggetto responsabile dell'istruttoria whistleblowing, quale soggetto Delegato al trattamento dei dati personali.

3. VALUTAZIONE DELLE MISURE DI SICUREZZA DEL TRATTAMENTO

All'esito dei controlli effettuati nell'Ente, alcune misure di sicurezza sono state valutate come "migliorabili", come risulta dalla tabella seguente.

ID	MISURA	VALUTAZIONE	MOTIVAZIONE
MS1	**Politiche di tutela della privacy**	Migliorabile	Il Titolare del trattamento, nel rispetto del Regolamento (UE) 2016/67, ha nominato un Responsabile della Protezione dei dati (RPD) in maniera da guidare e verificare la protezione dei dati personali all'interno della struttura anche mediante l'attuazione di un modello organizzativo efficace e verificato (con procedure, istruzioni, registrazioni delle non conformità, ecc.). Il titolare ha predisposto: 1- Procedura per la gestione dei diritti degli interessati; controllo delle modalità con le quali vengono fornite le informazioni all'interessato (artt. 12, 13 e 14 RGPD), compreso come viene raccolto il consenso, ove necessario; comunicazione e informazioni trasparenti, efficaci (es. granulari e stratificate, comprensibili e snelle) e verificate agli interessati; pubblicizzazione di canali di comunicazione e/o punti di contatto per l'esercizio dei diritti degli interessati, richieste di chiarimento, ecc. 2- Nomina personale autorizzato (per iscritto) contenente vincolo di riservatezza e con allegate istruzioni per il trattamento e policy specifiche per il personale relative all'uso delle postazioni, Internet, posta elettronica, utilizzo supporti removibili e documentazione cartacea; al riutilizzo sicuro e dismissione di dispositivi elettronici e supporti, alla tutela della privacy. I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con le politiche di sicurezza. I dipendenti, lavoratori e persone autorizzate al trattamento comprendono le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. 3- Supervisione e vigilanza sulla protezione dei dati, con l'adozione di una propria procedura di gestione del data breach, al fine di essere nella condizione di adempiere agli artt. 33 e 34, Reg. UE 2016/679. 4- Controllo periodico del contenuto delle informative da fornire agli interessati. 5- Monitoraggio sui trasferimenti di dati verso paesi terzi o organizzazioni internazionali e, in caso affermativo, se i dati godono di una protezione equivalente (con i fondamenti di legittimi-

			tà su cui è basato il trasferimento, ai sensi del Capo V artt. 44 e ss. RGPD). Tuttavia, è necessaria l'immediata pubblicazione, nel sito web del Comune, dell'informativa sul trattamento dei dati personali relativi alle segnalazioni, avente il contenuto tassativamente previsto dall'art. 13, par. 1, Reg. UE 2016/679 (RGPD), la cui elaborazione spetta al DPO dell'Ente.
MS2	**Gestione del "rischio privacy" (specifico per gli Interessati)**	Migliorabile	La presente DPIA costituisce strumento di gestione del rischio "privacy". Sono, inoltre, censite le categorie di trattamento ed i dati trattati, mediante un Registro dei trattamenti adottato ai sensi dell'art. 30, Reg. UE 2016/679, per il quale, tuttavia, è necessario verificare la necessità di un suo aggiornamento proprio nella riga del trattamento relativa all'anticorruzione e whistlebowing.
MS3	**Politiche di cybersecurity e analisi delle vulnerabilità**	Accettabile	Il titolare ha adottato politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate e i dati trattati (documentare le procedure operative, inventari, aggiornamenti di software e hardware, analisi e correzione di vulnerabilità, ecc.).
MS4	**Gestione del personale (formazione, ruoli e responsabilità, gestione di eventi imprevisti)**	Migliorabile	Il titolare ha pianificato, per l'autunno 2023, misure di sensibilizzazione e formazione del personale sulla cultura della protezione dati e sui principi fondamentali di liceità correttezza e trasparenza, limitazione finalità, minimizzazione, limitazione della conservazione, adottate al momento della presa in carico di un dipendente, nonché formazione specifica al personale sulle vulnerabilità informatiche (furti identità, ransomware, phishing, pretexting, keylogging, ecc.). Esistono contromisure per le seguenti minacce: corruzione; carichi di lavoro eccessivi, stress o cambiamenti negative nelle condizioni lavorative; assegnazione di compiti al personale oltre le loro capacità; uso insufficiente di competenze, etc.; indisponibilità del personale (sciopero; infortunio sul lavoro; malattia professionale; infortuni o malattie; morte; indisposizione neurologica, psicologica o psichiatrica, etc.); modifiche a come la posta viene smistata; riorganizzazione dei sistemi di trasmissione documentazione cartacea; cambio di lingua ufficiale o lavorativa; riassegnazione ruoli; termine o cessazione per interruzione di contratti; cambi di mansione; subentro; interruzione di un flusso autorizzativo dovuto ad una riorganizzazione. Vengono disattivati tutti gli account connessi al personale cessato e verifica della restituzione di eventuali supporti mobili, documenti etc, contenenti dati personali. Tuttavia, è necessario designare il RPCT (Segretario Comunale), soggetto responsabile dell'istruttoria whistleblowing, quale soggetto Delegato al trattamento dei dati personali. Ai sensi del nuovo decreto sul Whistleblowing, tutti gli Enti coinvolti dalla norma sono tenuti alla creazione di canali di segnalazione interna, che garantiscano, anche tramite strumenti di crittografia, la riservatezza dell'identità del segnalante e del contenuto della segnalazione, e che siano, altresì, affidati a uffici o persone interne, o ancora a soggetti esterni, purchè auto-

			nomi e specificamente formati.
MS5	**Gestione relazione con le terze parti che accedono ai dati**	Accettabile	Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto e possibilmente i riferimenti alle clausole contrattuali che delimitano l'ambito delle rispettive responsabilità (art. 28 RGPD). Nel caso di specie, tuttavia, la piattaforma di segnalazione utilizzata è quella di ANAC, che opera quale autonomo titolare del trattamento.
MS6	**Vigilanza (audit di conformità)**	Accettabile	Potrebbe essere, tuttavia, necessario adottare una Procedura di audit.
MS7	**Prevenzione da danni fisici e fonti di rischio non umane**	Accettabile	Sono presenti: sistema antincendio, separazione impianti e compartimentazione antincendio, allarmi temperatura e sistemi di rilevazione e auto-spegnimento incendi, gas inerte e interruzione automatica alimentazione. Allarmi anti umidità e antiallagamento sotto pavimento flottante. Impianti di condizionamento e ventilazione. Filtri antipolvere e altri sistemi di pulizia. Derattizzazione ove necessaria.
MS8	**Antiintrusione e controllo degli accessi fisici**	Accettabile	I dati personali oggetto di trattamento sono custoditi nel software di ANAC nonché nei fascicoli su supporto cartaceo. Alle sale, ubicate all'interno di locali chiusi al pubblico, possono accedere esclusivamente il Titolare e i soggetti autorizzati al trattamento dei dati. Nei locali dell'Ente è presente sistema di controllo degli accessi fisici da parte di dipendenti / fornitori / manutentori/ visitatori / ospiti / utenti ai locali che ospitano il trattamento. Armadi chiusi a chiave o stanze chiuse a chiave, procedure di accesso a chiavi, ecc. Porta d'ingresso chiusa.
MS9	**Lotta contro il malware**	Accettabile	Su tutti i pc sono installati antivirus e firewall e viene svolto un controllo periodico degli aggiornamenti, anche del Sistema.
MS10	**Sicurezza dei siti web**	Accettabile	Il sito web risiede in UE e ha le misure di sicurezza previste dalla normativa vigente per gli Enti pubblici. L'Amministrazione garantisce la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione anche mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione. La tecnologia TOR rappresenta una delle possibili soluzioni per l'anonimizzazione dei dati del segnalante.
MS11	**Sicurezza di server, reti, Wi-Fi**	N/A	Il trattamento non è svolto mediante server e reti di proprietà del Titolare.
MS12	**Sicurezza di hardware, postazioni e dispositivi**	N/A	Il trattamento non è svolto mediante server e reti di proprietà del Titolare.
MS13	**Sicurezza dei software**	N/A	Il trattamento non è svolto mediante server e reti di proprietà del Titolare. Il software utilizzato è messo a disposizione da ANAC e invia le segnalazioni alla casella PEC del Sindaco.
			È garantita la conformità della misura, tuttavia, sarebbe opportuno procedere ai seguenti controlli: Prevenzione di malfunzionamenti e problemi tecnici dei sistemi.
			Esistenza di una politica di manutenzione fisica dei dispositivi,

MS14	**Manutenzione**	Accettabile	specificando l'eventuale ricorso all'outsourcing, compresa la manutenzione remota, ove autorizzata, con specifica attenzione ai metodi di gestione dei materiali difettosi. Manutenzione interna periodica di Sistemi e di reti (Backup configurazioni, verifica firmware, prestazioni hardware, capienza dischi, utilizzo risorse, ecc.). Contratti di manutenzione e assistenza hardware e software attivi. Possibilità di effettuare manutenzioni pianificate senza impatti negativi sulla gestione della funzionalità. Gli aggiornamenti cri-tici di sicurezza rilasciati dallo sviluppatore del sistema operati-vo devono essere installati regolarmente.
MS15	**Backup e Restore**	Accettabile	I backup sono effettuati con più di un sistema per contrastare malfunzionamenti in fase di ripristino. Le copie di sicurezza sono isolate dal sistema e mantenute sicure tramite misure di sicurezza fisiche. Le procedure di backup riguardano l'intero sistema, (OS, Applicazione, Dati). Viene effettuata una copia di sicurezza con cadenza settimanale delle informazioni strettamente necessarie per il completo ripristino del sistemaMisure idonee a ripristinare immediatamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico e politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.).
MS16	**Business continuity**	Accettabile	Il Titolare ha definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery. Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino.
MS17	**Disaster recovery**	Accettabile	Sono definiti requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in seguito a eventi disastrosi. Il "recupero dal disastro" è l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività. Il Disaster Recovery Plan (DRP) è il documento che esplicita tali misure, compreso all'interno del più ampio piano di continuità operativa (BCP).
MS18	**Controllo degli accessi logici, autenticazione, password**	Accettabile	Accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi. Autenticazione a più fattori. Blocco accesso a seguito di ripetuti tentativi di accesso falliti consecutivi. È garantita la qualità delle password tramite la validazione, (8 caratteri con minuscole, maiuscole, numeri e caratteri speciali). Integrazione con il Domain Controller. Le credenziali già utilizzate non possono essere riutilizzate a breve distanza di tempo. Le credenziali soprattutto quelle delle utenze amministrative vengono sostituite con frequenza semestrale. Sono utilizzati sistemi centralizzati di gestione delle password (Single Sign On)Gestione corretta dei messaggi di errore facendo si che questi non rivelino informazioni riservate sul si-

			stema. Timeout di sessione se l'utente non è attivo per un determinato periodo di tempo.
MS19	**Gestione dei profili di accesso**	Accettabile	È mantenuto un inventario delle utenze amministrative. I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa. La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli. La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati. Le utenze amministrative sono formalmente autorizzate. Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza. Disattivazione account e password predefiniti del fornitore. Generazione di un'allerta all'aumento dei privilegi di utenza amministrativa. Implementazione del principio del privilegio minimo. Vengono tracciati nei log tutti i tentativi di accesso falliti delle utenze amministrative.
MS20	**Tracciabilità (Logging) degli eventi**	Accettabile	Non vi è un sistema di log, situazione ottimale per il trattamento in analisi. Tuttavia, per gli altri trattamenti, è consigliabile tracciare l'attività degli utenti del sistema, con un sistema di controllo da accessi non autorizzati e di conservazione per un termine congruo rispetto alle finalità di tracciamento. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante. Il tracciamento può essere effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati. In ogni caso, la disciplina della gestione degli accessi e dei log applicativi rientra nella serie di atti organizzativi che l'amministrazione deve adottare per adempiere alle previsioni in materia di sicurezza informatica e protezione dei dati personali.
MS21	**Minimizzazione dei dati personali**	Accettabile	Con riferimento al principio di "minimizzazione dei dati" di cui all'art. 5, co. 1, lett. c) del GDPR, il rispetto di tale obbligo, nel trattamento del whistleblowing, non è più lasciato alla mera responsabilizzazione del titolare del trattamento, bensì stabilito in maniera cogente. Dal lato pratico e operativo il titolare del trattamento dovrà predisporre misure tecniche, organizzative e di formazione del personale, per impedire la raccolta ex ante di dati personali non utili alla specifica segnalazione, verificare tempestivamente la stessa, individuando appunto i dati personali non utili, e provvedere, se del caso, alla cancellazione ex post.
MS22	**Altre misure applicate ai dati**	Accettabile	È implementato un sistema di gestione delle chiavi crittografiche. Formazione relativa alla cifratura. Le chiavi private sono adeguatamente protette. Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura. Chiavi di cifratura personali. Nel trattamento del whistleblowing, è utilizzata la crittografia.
MS23	**Archiviazione sicura (nella consegna,**	Accettabile	Sono implementate politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eli-

	sistemazione, consultazione) e dismissione sicura		minazione, politiche di archiviazione, protezione della confidenzialità, ecc.). I dati che non sono più di utilizzo corrente, ma il cui periodo di conservazione non è ancora terminato, per esempio poiché sono conservati in previsione di eventuali contenziosi, dovrebbero essere archiviati. È in vigore una procedura per il rilascio delle credenziali e per la loro cancellazione.
MS24	**Archiviazione sicura dei documenti cartacei e dismissione sicura**	Accettabile	La misura è sufficientemente soddisfatta, tuttavia, è consigliabile procedere a: - elaborazione di Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento, che descrivono come i documenti sono stampati, archiviati, distrutti e condivisi; - adozione di una procedura per la dismissione sicura dei fascicoli cartacei a fine vita, al fine di evitare il recupero di informazioni da documentazione cartacea abbandonata o dismessa; - verifica della sicurezza degli appartamenti in cui sono conservati i fascicoli.

4. VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI IN CASO DI ACCESSO ILLEGITTIMO (R), MODIFICA INDESIDERATA (I) E PERDITA (D) DEI DATI PERSONALI

Il rischio inerente o potenziale (Ri) è il rischio calcolato prima dell'applicazione delle misure di sicurezza.

Rischio inerente = Probabilità (Minaccia) * Gravità (Impatto)
Ri = P * G

Il risultato corrisponde a una scala di valori: potremo avere un rischio inerente (Ri) trascurabile, limitato, importante, massimo.

Nelle tabelle successive, mutuate dal metodo proposto dall'autorità di controllo francese Commission nationale de l'informatique et des libertés ("CNIL"), sono rappresentati i controlli svolti per la "Valutazione dei rischi per i diritti e le libertà degli interessati in caso di accesso illegittimo (R), modifica indesiderata (I) e perdita dei dati (D)".

In particolare, è stata stimata la gravità dei rischi (gli impatti potenziali per i diritti e le libertà degli interessati) e la probabilità che si verifichino eventi che potrebbero determinare l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati, dalla prospettiva degli interessati.

Accesso illegittimo ai dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	Gli impatti sugli interessati si pongono al livello massimo, poiché i medesimi potrebbero avere potrebbero avere: - Conseguenze fisiche significative (es. aggravamento dello stato di salute) - Conseguenze materiali significative (es. furto di identità, perdite monetarie non indennizzate, perdita del posto di lavoro, rischi finanziari, indebitamento, impossibilità di lavorare, incapacità di ricollocazione lavorativa, ecc.) - Conseguenze psicologiche significative (es. esposizione a ricatti, cyberbullismo e molestie psicologiche, danni reputazionali, ricatti, conseguenze psicologiche gravi, senso di violazione della privacy e di un danno irreparabile, ecc.)
Principali minacce che potrebbero concretizzare il rischio.	Utilizzo improprio delle credenziali di accesso alle segnalazioni e accesso non autorizzato delle stesse. Negligente nella custodia delle credenziali di accesso. Accesso non autorizzato ai locali fisici presso cui sono poste le segnalazioni scritte. Mancato aggiornamento / revoca delle autorizzazioni all'accesso.

Fonti di rischio.	Mancato aggiornamento del SO. Mancanza di firewall e/o antivirus sul pc/server. Dipendenti negligenti. Dipendenti infedeli. Ex-dipendenti. Amministratori di sistema. Soggetti che decidono di portare un attacco ai dati dell'Ente.
Misure che contribuiscono a mitigare il rischio.	Come da Sezione 3 della presente DPIA.
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.	Il rischio è IMPORTANTE
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.	Il rischio è IMPORTANTE
Modifiche indesiderate dei dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	Ove il rischio si concretizzasse, gli impatti sugli interessati sarebbero a un livello massimo, poiché i medesimi potrebbero avere: - Conseguenze fisiche significative (es. aggravamento dello stato di salute) - Conseguenze materiali significative (es. furto di identità, perdite monetarie non indennizzate, perdita del posto di lavoro, rischi finanziari, indebitamento, impossibilità di lavorare, incapacità di ricollocazione lavorativa, ecc.) - Conseguenze psicologiche significative (es. esposizione a ricatti, cyberbullismo e molestie psicologiche, danni reputazionali, ricatti, conseguenze psicologiche gravi, senso di violazione della privacy e di un danno irreparabile, ecc.)
Principali minacce che potrebbero concretizzare il rischio.	Utilizzo improprio delle credenziali di accesso alle segnalazioni e accesso non autorizzato delle stesse. Negligente nella custodia delle credenziali di accesso. Accesso non autorizzato ai locali fisici presso cui sono poste le segnalazioni scritte. Mancato aggiornamento / revoca delle autorizzazioni all'accesso.
Fonti di rischio.	Mancato aggiornamento del SO. Mancanza di firewall e/o antivirus sul pc/server. Dipendenti negligenti. Dipendenti infedeli. Ex-dipendenti. Amministratori di sistema. Soggetti che decidono di portare un attacco ai dati dell'Ente.
Misure che contribuiscono a mitigare il rischio.	Come da Sezione 3 della presente DPIA.
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.	Il rischio è IMPORTANTE
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.	Il rischio è LIMITATO
Perdita dei dati	
Potenziali impatti sugli interessati se il rischio si	Ove il rischio si concretizzasse, gli impatti sugli interessati sarebbero a un livello importante, poiché i medesimi potrebbero avere potrebbero

dovesse concretizzare.	avere: - Conseguenze fisiche significative (es. aggravamento dello stato di salute) - Conseguenze materiali significative (es. furto di identità, perdite monetarie non indennizzate, perdita del posto di lavoro, rischi finanziari, indebitamento, impossibilità di lavorare, incapacità di ricollocazione lavorativa, ecc.) - Conseguenze psicologiche significative (es. esposizione a ricatti, cyberbullismo e molestie psicologiche, danni reputazionali, ricatti, conseguenze psicologiche gravi, senso di violazione della privacy e di un danno irreparabile, ecc.).
Principali minacce che potrebbero concretizzare il rischio.	Utilizzo improprio delle credenziali di accesso alle segnalazioni e accesso non autorizzato delle stesse. Negligente nella custodia delle credenziali di accesso. Accesso non autorizzato ai locali fisici presso cui sono poste le segnalazioni scritte. Mancato aggiornamento / revoca delle autorizzazioni all'accesso. Malfunzionamenti del sistema / del server / degli impianti, Vandalismo, Furto di componenti. Rottura del sistema / del server.
Fonti di rischio.	Mancato aggiornamento del SO. Mancanza di firewall e/o antivirus sul pc/server. Dipendenti negligenti. Dipendenti infedeli. Ex-dipendenti. Amministratori di sistema. Soggetti che decidono di portare un attacco ai dati dell'Ente. Incendio. Allagamento. Cali di tensione elettrica. Sovraccarichi di tensione elettrica.
Misure che contribuiscono a mitigare il rischio.	Come da Sezione 3 della presente DPIA.
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.	Il rischio è IMPORTANTE
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.	Il rischio è IMPORTANTE

Il valore finale di cui si tiene conto è il valore più alto di G e di P per ogni parametro RID, dunque:

Parametro RID	**Rischio**	**Abbreviazione**	**Valore**
Riservatezza	Accesso ai dati	(A)	IMPORTANTE
Integrità	Modifiche indesiderate ai dati	(M)	IMPORTANTE
Disponibilità	Perdita dei dati	(P)	IMPORTANTE

Ri = IMPORTANTE

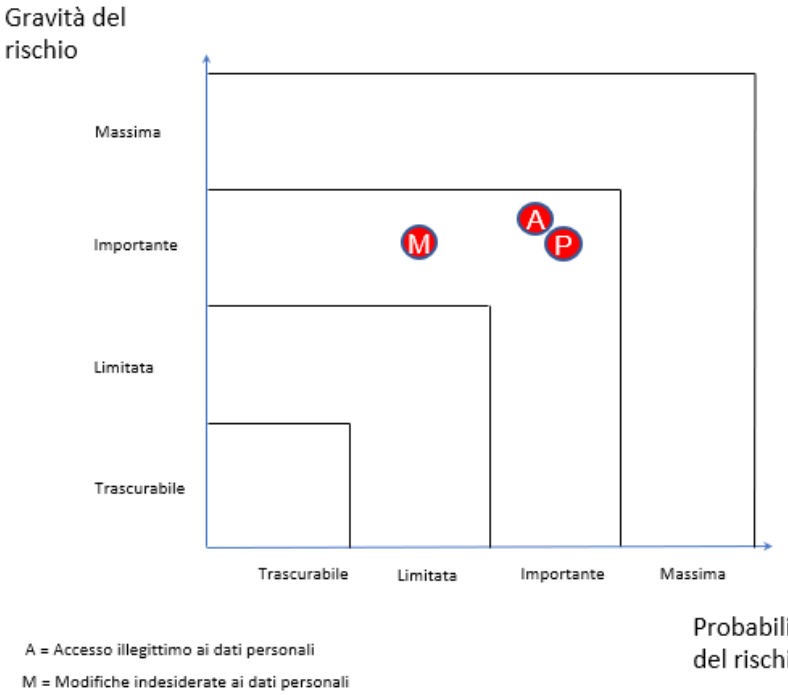

Grafico della valutazione del Rischio Inerente (Ri) ossia il rischio prima del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

Quarrata, 26 luglio 2023

Il Sindaco
Gabriele Romiti

_____

N.B.: La presente DPIA viene trasmessa al Referente privacy dell'Ente per l'elaborazione dei passaggi successivi (Revisione).