C.C.A.M.
Consorzio Comuni
Acquedotto Monferrato

Sede Legale e Direzione
Via Senatore Ferraris 3, 14036 Moncalvo (AT)
www.ccam.it / info@ccam.it / ccam@legalmail.it
CENTRALINO 0141.91.11.11 / FAX 0141.91.11.42
SERVIZIO CLIENTI 800.62.22.55
PRONTO INTERVENTO 800.91.55.52

Sistema Compliance Normativa
PRO Whistleblowing

Doc ID SCN_PRO 01 Whistleblowing

Versione 1.0

Riassunto Questo documento descrive la procedura per assicurare lo svolgimento degli adempimenti previsti dal D.Lgs 24/2023, che recepisce la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Num. pagine 13

	Nome	Ruolo	Data	Firma
Autore	CCAM	Team CCAM	20 /12/2023	
Revisione	DPO	Data Protection Officer	17/12/2023	Marco Canetti 17.12.2023 13:48:37 GMT+01:00
	ODV	Organismo di vigilanza ex 231/01	20/12/2023	
	RPCT	Responsabile Prevenzione Corruzione e Trasparenza	20/12/2023	
Validazione	CDA	Titolare Trattamento	/ /2023	Il Presidente del Consiglio (QUALIFICA) Consorzio Comuni per l'Acquedotto del Monferrato MONCALVO AT

INDICE

1 Scopo

Lo scopo del presente documento è quello di definire le modalità, le procedure, gli strumenti e le responsabilità con le quali il Consorzio dei Comuni dell'Acquedotto del Monferrato (da ora in poi CCAM) intende definire, implementare e manutenere misure organizzative e tecnologiche necessarie e sufficienti a:

- garantire, per le persone che effettuano le segnalazioni, un livello adeguato di protezione secondo quanto previsto dal D.Lgs. 24/2023 e s.m.i;
- garantire che il processo di gestione delle segnalazioni delle violazioni avvenga nel pieno rispetto dei diritti e delle libertà garantite dalle vigenti normative in materia di protezione dei dati personali;
- definire le modalità di svolgimento delle istruttorie successive alle segnalazioni;
- monitorare l'efficacia ed efficienza della presente procedura, in modo da assicurare nel tempo la conformità alle evoluzioni normative, organizzative e tecnologiche.

2 Ambito

2.1 Processi coinvolti

La presente procedura si applica a tutte le attività correlate con la protezione delle persone che segnalano 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[1].

2.2 Ambito temporale

E' possibile effettuare la segnalazione:

- quando il rapporto giuridico è in corso;
- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso (pensionati).

2.3 Soggetti interessati (stakeholder)

Whistleblower (Sentinella)	Il Whistleblower è la persona che segnala, divulga ovvero denuncia all'autorità giudiziaria o contabile, 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 è venuto a conoscenza in un contesto lavorativo pubblico privato[2].
	Dipendenti pubblici (compresi i Dipendenti di società in house, concessionari di pubblico servizio, etc) Lavoratori subordinati Lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato Collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato Volontari e i tirocinanti, retribuiti e non retribuiti,

[1] comma 1 art. 1 D.Lgs. n. 24/2023
[2] combinato disposto dell'art. 1 e dell'art. 2 del d.lgs. 24/2023

	Azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.
Facilitatori	Sono le figure, interne e/o esterne all'organizzazione, deputate a mettere in atto ogni risorsa utile a gestire in conformità con il D.Lgs. n. 24/2023 il processo di gestione delle segnalazioni
RPCT	Responsabile Prevenzione Corruzione Trasparenza – responsabile operativo per la gestione delle segnalazioni e la garanzia in materia di applicazione delle tutele previste dal c.d. "Whistleblowing"
ODV	Organismo di Vigilanza – consultato per la valutazione in merito alle segnalazioni potenzialmente impattanti in ambito 231, MOG e Codice Etico, responsabile operativo per il follow up delle segnalazioni in tale ambito
DPO	Data Protection Officer – consultato per la valutazione in merito alle segnalazioni potenzialmente impattanti in ambito protezione dati personali, responsabile operativo per il follow up delle segnalazioni in tale ambito, responsabile operativo per garantire la riservatezza "by design" e "by default" del processo Whistleblowing

2.4 Ambito della segnalazione

E' possibile segnalare comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- Violazione di disposizioni normative nazionali
  - illeciti amministrativi, contabili, civili o penali
  - condotte illecite rilevante ai sensi del D.Lgs. n. 231/2001 oppure violazione dei modelli di organizzazione e gestione ivi previsti
- Violazione di disposizioni normative europee illeciti che rientro nell'ambito di applicazione degli atti dell'Unione Europea relativi ai settori in elenco[3]
  - 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;
  - sicurezza delle reti e dei sistemi informativi.
- Atti e/o omissioni che ledono gli interessi finanziari dell'unione europea
- Atti e/o omissioni riguardato il mercato interno (violazioni in materia di concorrenza di aiuti di Stato)
- Atti e/o comportamenti che vanificano l'oggetto la finalità delle disposizioni di cui agli atti dell'unione

Possono inoltre essere oggetto di segnalazione:

[3] Sono qui sottolineati i settori nei quali l'Azienda / Ente è direttamente coinvolto

- i comportamenti volti a occultare le condotte illecite oppure a sviare eventuali verifiche in corso
- informazioni, concrete, precise e concordanti, che il segnalatore ritenga possano condurre ad attività illecite[4]

2.5 Criterio di valutazione della segnalazione

Coloro i quali sono deputati a valutare la liceità della segnalazione devono escludere il criterio della motivazione, che deve essere ritenuto irrilevante. In altri termini, l'oggetto, la veridicità e l'affidabilità della segnalazione di attività illecite che riguardino la Società in senso lato sono gli elementi fondamentali ed in quest'ottica non dovrà essere esclusa la segnalazione pur potenzialmente motivata (a mero titolo di esempio) dall'interesse personale.

2.6 Ambito di esclusione

Viceversa non si applicano le disposizioni tutelanti del D.Lgs 24/2023, qualora la segnalazione riguardasse esclusivamente questioni relative ad interessi lavorativi personali (contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate).

3 Riferimenti normativi

I riferimenti normativi sono elencati nell'allegato omonimo, in modo da semplificare e massimizzare l'efficacia in previsione di aggiornamenti futuri in ottica di manutenzione ed aggiornamento della presente procedura.

4 Responsabilità

Di seguito sono riportati i ruoli e le responsabilità dei soggetti coinvolti, per fasi di attività

Attività	Responsible (operativo)	Accountable (decisionale)	Consulted	Informed
Budget e risorse	RPCT	CDA	RPCT, ODV, DPO, CIO	Assemblea Soci
Protezione dati personali	RPCT / ODV / DPO / CIO	Titolare del trattamento	DPO	CDA
Formazione ed informazione	HR	CDA	RPCT, ODV, DPO	Stakeholder
Predisposizione strumenti tradizionali ed avanzati di gestione del canale interno	RPCT / ODV / DPO / CIO	RPCT / CIO	RPCT / ODV / DPO / CIO	Stakeholder
Strumenti tradizionali gestione canale interno (email, cassetta dedicata, incontro diretto, etc)	RPCT / CIO	RPCT	DPO	Stakeholder
Gestione Piattaforma (IT)	CIO	RPCT	DPO, RPCT, ODV	CDA
Ricezione e valutazione segnalazioni	RPCT	CDA	RPCT, ODV, DPO	Stakeholder

[4] L'ANAC indica anche i c.d. "fondati sospetti", la cui definizione puntuale dovrà essere oggetto di ulteriori approfondimenti

Follow-up segnalazioni	RPCT	CDA	DPO, RPCT, ODV[5]	CDA, Stakeholder

4.1 Budget e risorse

Il CDA deve assicurare le risorse necessarie e sufficienti a garantire la conformità normativa alle disposizioni attuali e future in materia di Whistleblowing, assicurando che siano disponibili per i responsabili delle attività sia il budget sia le competenze ed il tempo necessario.

5 Fasi del processo

La protezione dei Whistleblower inizia dall'analisi del rischio inerente al processo di segnalazione ex D.Lgs. 24/2023.
L'insieme di procedure, attività, strumenti che concorrono al raggiungimento dello scopo della presente Whistleblowing è definito da ora in poi "processo Whistleblowing".

5.1 Analisi e gestione del rischio

Sono di seguito elencate le categorie di rischio prese in esame dalla presente procedura:

5.1.1 Rischio di mancata segnalazione

Si intende il rischio di mancate segnalazioni di attività illecite poiché il potenziale Segnalante è portato a ritenere che:

a) la Sua segnalazione verrà ignorata / sottovalutata dall'Organizzazione;
b) la Sua persona possa essere oggetto di attività persecutorie da parte dell'Organizzazione alla quale appartiene e la Sua immagine diffamata attribuendo alla segnalazione una caratteristica negativa di delazione;

e pertanto sceglie di non procedere alla segnalazione, temendo per l'inefficacia della segnalazione versus un impatto negativo sulla Sua vita sociale e lavorativa.
E' responsabilità del CDA del CCAM predisporre le seguenti misure organizzative allo scopo di mitigare l'accadimento di tale rischio inerente:

Rischio	Mitigazione
Ambiente culturalmente e organizzativamente ostile alla cultura del Whistleblowing	Formazione del personale coinvolto nel processo. Informative pubblicate e diffuse tramite il sito aziendale. Diffusione a tutti gli stakeholder della cultura del Whistleblowing, come fattore mitigante delle malversazioni. Evidenza di misure organizzative e tecnologiche, documentate e sottoposte a monitoraggio e miglioramento continuo, poste a protezione dei soggetti segnalanti. Inserimento nel MOG 231, nel PTPCT e nel Codice Etico delle disposizioni in materia di protezione del Segnalante, con pubblicazione della sopra menzionata documentazione nelle sezioni apposite del sito aziendale.

5.1.2 Rischio di inefficacia

Questo rischio riguarda la possibilità che – una volta ricevuta – la segnalazione non sia correttamente ed adeguatamente processata, rendendo inefficace l'attività e alimentando un clima di sfiducia nel processo Whistleblowing.

Rischio	Mitigazione

[5] per quanto di competenza, relativamente al contenuto delle segnalazioni

Segnalazione ignorata / sottovalutata	Implementazione di un insieme di procedure, sottoposte a continua valutazione e miglioramento, per massimizzarne l'efficacia (gestione del ciclo di segnalazione che giunge agli obiettivi leciti del segnalante) ed efficienza (gestione rapida del ciclo, entro i termini normativamente previsti) del processo Whistleblowing Corretta attribuzione delle responsabilità per la gestione del ciclo di segnalazione. Monitoraggio dell'effettiva esecuzione delle fasi di gestione e di follow-up della segnalazione, da parte degli attori principali (RCPT, ODV, DPO), con report al CDA. Inserimento nell'agenda delle riunioni CDA della fase di valutazione sia delle segnalazioni pervenute sia del complessivo funzionamento del processo Whistleblowing.
Mobbing lavorativo e diffamazione del segnalante	Progettazione "by design" di sistemi di raccolta e gestione delle segnalazioni, così che garantiscano ab origine la riservatezza del segnalante. Stipula di adeguati contratti di riservatezza (NdA) con gli attori interni e Contratti protezione dati con i Responsabili del trattamento. Coinvolgimento, ove necessario, delle Rappresentanze Sindacali interne a protezione del Segnalante nell'ambito lavorativo e del DPO aziendale per gli aspetti generali di protezione dei dati personali del Segnalante. Progettazione ed applicazione di misure di protezione dei soggetti segnalanti, misure documentate e sottoposte a monitoraggio e miglioramento continuo.

5.1.3 Rischio di mancata protezione del Segnalante

Rischio	Mitigazione
Mobbing lavorativo e diffamazione del segnalante	Progettazione "by design" di sistemi di raccolta e gestione delle segnalazioni, così che garantiscano *ab origine* la riservatezza del segnalante. Divieto di ogni forma di ritorsione (anche tentata / minacciata) tramite procedure che prevedano l'esame collegale di eventuali forme di pressione indebita sul Segnalante, coinvolgimento, ove necessario, delle Rappresentanze Sindacali (interne / esterne) a protezione del Segnalante nell'ambito lavorativo e del DPO aziendale per gli aspetti generali di protezione dei dati personali. Stipula di adeguati contratti di riservatezza (NdA) con gli attori interni e Contratti protezione dati con i Responsabili del trattamento. Progettazione ed applicazione di misure di protezione preventiva dei soggetti segnalanti, misure documentate e sottoposte a monitoraggio e miglioramento continuo.

5.1.4 Rischi protezione dati personali

Il rischio che i diritti e le libertà riconosciute al Segnalante ed a tutti gli stakeholder coinvolti, deve essere preventivamente misurato tramite DPIA (Valutazione degli Impatti Protezione Dati, allegata alla presente procedura come documento riservato).

I rischi connessi ai trattamenti necessari all'esecuzione del processo Whistleblowing devono essere misurati sia periodicamente sia ad ogni segnalazione, qualora sussista la possibilità che le mitigazioni applicate non risultino efficaci, nello specifico caso in esame.
E' responsabilità del Titolare monitorare il rischio in questo ambito, con il supporto operativo del DPO e dei Referenti interni in materia di protezione dati personali.

La tutela delle persone segnalanti e degli stakeholder coinvolti nel processo Whistleblowing, previste dal D.Lgs. 24/2023 si applica anche quando

- il rapporto giuridico non è ancora iniziato (se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali);
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico (se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso);

si estende anche ai facilitatori, alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado, ai colleghi di lavoro della persona segnalante che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente, agli enti di proprietà della Persona Segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.
Il RPCT e tutti gli stakeholder coinvolti nella segnalazione (figure di supporto del RPCT, ADS, ODV, amministratore di sistema, personale incaricato autorizzato al trattamento dei dati personali) sono passibili di sanzione disciplinare qualora venisse violata la riservatezza dell'identità del segnalante, il contenuto della segnalazione e le informazioni ivi contenute.

5.1.4.1 Limitazioni all'esercizio dei diritti

Sono applicate le previsioni novellate dal comma f) dell'art. 2-undecies del D.Lgs. 196/2003, a protezione della riservatezza del segnalante. Riportiamo di seguito – per facilità di lettura – il comma sopra citato:
"*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;*"

La segnalazione (compresa la documentazione eventualmente allegata) deve essere pertanto sottratta al diritto di accesso agli atti amministrativi (art. 22 e ss. Legge n.241/1990), nonché all'accesso civico generalizzato (art. 5 comma 2 D. Lgs. n.33/2013).
E' responsabilità del RPCT provvedere in tal senso, sentito se necessario il DPO.

5.1.4.2 Rischio di diffamazione

Si intende il rischio che la segnalazione venga dolosamente effettuata dal Segnalante per danneggiare terzi.

Rischio	**Mitigazione**
Diffamazione tramite il processo di Whistleblowing	Tutti gli stakeholder coinvolti nel processo hanno il dovere di approfondire adeguatamente le informazioni ricevute tramite la segnalazione e di verificarne la veridicità con la maggior obiettività possibile. Il DPO deve inoltre supportare il Titolare del

	trattamento nella necessità di coinvolgere i controinteressati dalla segnalazione, tutelando i diritti e le libertà garantite dalle vigenti normative in materia di protezione dati personali.

5.1.5 Data retention

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. In adempimento al principio di minimizzazione dei dati (lett c) del comma 1) art. 5 del GDPR – Principi applicabili al trattamento di dati personali), i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, devono essere immediatamente eliminati.
I dati personali raccolti nel processo di segnalazione sono trattati dal CCAM in qualità di Titolare del trattamento nel rispetto dei principi e degli obblighi sanciti dalla normativa sulla protezione dei dati personali (Regolamento UE n. 2016/679 – GDPR e D. lgs n. 196/2003 – Codice Privacy) e sono protetti con misure di sicurezza adeguate. Ulteriori informazioni sul trattamento dei dati personali sono reperibili nell'informativa resa disponibile al seguente link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9844945

5.1.6 Protezione degli stakeholder coinvolti

Sono adottate tutte le misure necessarie a tutelare l'integrità fisica, la dignità e la salute mentale del Segnalante, assicurando un'adeguata tutela da qualsiasi forma di ritorsione, penalizzazione, discriminazione o minacce.

Il CCAM, in qualità di Titolare del trattamento dati personali, disporrà a far sì che le misure di sicurezza "by default" implementate in ambito protezione dati personali, siano poste a salvaguardia dei dati personali di tutti gli attori coinvolti nel processo Whistleblowing e puntualmente durante il trattamento della segnalazione, con le seguenti caratteristiche specifiche:

- le misure di sicurezza dovranno essere parametrizzate alla necessità di trattare i dati della segnalazione come se appartenessero alla categoria "dati particolari" e/o "dati relativi alla salute", quindi con il massimo livello di protezione possibile;
- dovrà essere eseguita opportuna valutazione degli impatti (DPIA), le cui risultanze sono discriminanti per la progettazione iterativa di misure di sicurezza sempre più efficaci e stringenti, fino a che il risultato sia che il rischio complessivo dei trattamenti subordinati al processo Whistleblowing non sia valutato "basso" dal DPO;
- stipula di contratti di riservatezza con i facilitatori, con i Responsabili del trattamento e con tutti gli attori del processo;
- audit DPO del processo, sia periodico sia contestuale a segnalazioni particolarmente impattanti dal punto di vista privacy.

5.2 Progettazione dei canali di segnalazione

5.2.1 Canali interni

Sono previsti i seguenti canali di segnalazione interna:

Canale	Misura di sicurezza
Applicativo dedicato, progettato per assicurare un adeguato livello di sicurezza (misurata secondo i paradigmi di disponibilità, riservatezza ed integrità)	SLA[6] tecnologico ed organizzativo per lo scouting della miglior soluzione (inclusa una versione on premise), come da allegata "Scheda SLA applicativo Whistleblowing"

[6] Service Level Agreement – contratto livelli di servizio

accessibile a tutti gli stakeholder tramite il link https://ccam.whistleblowing.it/#/ ;	DPA[7] con gli (eventuali) fornitori coinvolti, in qualità di responsabili
Pubblicazione del link di collegamento all'applicativo sul sito Istituzionale, nell'Area "Amministrazione Trasparente" sezione "WhistleBlowing"	Audit RPCT e DPO di verifica - dell'avvenuta pubblicazione, - dei parametri di sicurezza concordati (SLA)
Sistema di messaggistica vocale, contattando il numero verde 800662255;	DPA con il Responsabile Customer Care Audit RPCT e DPO
Servizio postale (o posta interna), inviando all'attenzione del Responsabile Prevenzione Corruzione e Trasparenza (RPCT) la segnalazione scritta in busta chiusa contenente la dicitura "STRETTAMENTE RISERVATA"	Protocollo riservato posta tradizionale CCAM
Apposite cassette affisse sia nella sede Uffici sia nei siti operativi, come da procedura "Sentinella" già in vigore presso il CCAM	Audit RPCT e procedura "Sentinella" in vigore
Incontro con il RPCT, contattando il centralino CCAM	DPA con il Responsabile del trattamento che offre il servizio Customer Care; NDA receptionist CCAM

5.2.2 Canali esterni

La scelta del canale di segnalazione non è più rimessa alla discrezione del whistleblower, che deve anzitutto procedere tramite il canale interno a meno che non si verifichi almeno una delle seguenti condizioni:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo oppure, anche se attivato, non è conforme a quanto previsto dall'articolo 4 del D.Lgs. n. 24/2023 ("Canali segnalazione interna") poiché:
  - non vi sono adeguate garanzie di riservatezza
  e/o
  - il RPCT CCAM non è adeguatamente formato oppure non lo sono gli altri attori essenziali (DPO e ODV anzitutto)[8]
- la persona segnalante ha già effettuato una segnalazione interna senza ottenere adeguato riscontro;
- la persona segnalante ha fondati motivi di ritenere che la segnalazione interna possa essere inefficace oppure innescare rivalse e ritorsioni;
- il segnalante ritiene che vi sia un pericolo immediato ed evidente per il pubblico interesse.

Qualora il segnalante ritenesse che neppure con il canale esterno vi fossero adeguate garanzie per l'efficacia ed efficienza della segnalazione e per la tutela della Sua persona, può ricorrere alla segnalazione pubblica.
Pertanto è necessario che il segnalante sia adeguatamente informato della necessità di tenere traccia delle segnalazioni effettuate, per dimostrare la necessità assoluta del ricorso alla soluzione esterna oppure pubblica.

[7] Data Processing Agreement – Contratto Protezione Dati
[8] In generale, il personale / ufficio assegnato alla gestione della segnalazione: è pertanto necessario che la formazione sia tracciata ed il livello di competenza adeguatamente mantenuto nel tempo

In caso contrario, il segnalante potrebbe non disporre delle protezioni previste dal D.Lgs 24/2023.
E' compito del Titolare del trattamento, sentito il DPO, provvedere a far sì che le informative in materia di Whistleblowing siano adeguate, sia in termini di rispetto normativo in materia di protezione dati personali sia per gli aspetti peculiari del processo Whistleblowing.
Il RPCT dovrà consultare il DPO e/o il Titolare per ogni aspetto propedeutico ("by design") e per eventuali aspetti puntuali delle segnalazioni in esame.

5.2.3 Riservatezza "by design" e "by default" dei canali interni

In ogni fase del processo "Whistleblowing" viene protetta l'identità della persona segnalante, della persona segnalata e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.
Qualora il Segnalante non intendesse rivelare la propria identità, gli strumenti:

- piattaforma digitale gestione segnalazione
- protocollo riservato interno
- cassette di deposito delle segnalazioni

devono essere configurate "by design" per garantire l'anonimato e mantenere comunque la possibilità di dialogo ed approfondimento – per quanto necessario ed opportuno – della segnalazione.
Il RPCT darà seguito alle segnalazioni pervenute tramite i canali "posta" e "cassetta sentinella" esponendo in bacheca sindacale e/o tramite comunicazione email dell'avvenuta ricezione di una segnalazione pregnante in ambito Whistleblowing e della necessità di ulteriori approfondimenti, indicando l'ulteriore canale più opportuno per consentire al Segnalante la comunicazione di ulteriori informazioni ritenute necessarie.

6 Fasi operative

6.1 Fase 1 – Registrazione segnalazione

Il RPCT provvede a riportare i dati fondamentali della segnalazione su registro informatico riservato (normalmente uno spreadsheet), inserendo un codice univoco progressivo, data ora e dati minimi necessari a identificare la tipologia della segnalazione, in modo da facilitare la successiva fase di valutazione.
In presenza di piattaforma informatica, il RPCT provvede a inoltre a registrare il codice restituito al segnalante, nell'ipotesi che quest'ultimo intenda mantenere l'anonimato.
Tale codice è essenziale per proseguire l'interazione, mantenendo la caratteristica di riservatezza assoluta, con la finalità di approfondire gli aspetti pregnanti della segnalazione e rendere quanto più possibile valutarne l'ammissibilità, mitigando il rischio di classificazioni errate.

6.2 Fase 2 – Valutazione preliminare e ammissibilità segnalazione

Fase di valutazione preliminare della segnalazione, al fine di assegnare:

- la rilevanza della segnalazione relativamente al campo di applicazione del D.Lgs. n. 24/2023
- la gravità della segnalazione
- la presenza di interessi personali del Segnalante e di eventuali altri soggetti
- la necessità di approfondire il contenuto della segnalazione e con quali mezzi avviare l'indagine

e di identificare gli stakeholder coinvolti, con relativa tabella RACI, ai quali verrà assegnato il compito di avviare un'istruttoria puntuale.
Il RPCT dovrà documentare i criteri di valutazione e tracciare la decisione di consegnare il materiale documentale alla successiva fase istruttoria.

Il RPCT è tenuto a concludere la fase di valutazione preliminare e ammissibilità entro 15 giorni, decorrenti dalla ricezione della segnalazione.

6.3 Fase 3 – Istruttoria

Fatta salva la fase di valutazione positiva dell'ammissibilità della segnalazione, viene avviata la fase Istruttoria.
E' responsabilità del RPCT vigilare in modo da assicurare al processo istruttorio le caratteristiche di

- Tempestività
- Indipendenza
- Equità
- Riservatezza

tracciando opportunamente ogni decisione, richiesta di supporto interno e/o esterno e acquisizione di informazioni, con l'obiettivo di giungere ad una conclusione sulla veridicità della segnalazione e sulla necessità di segnalare alle Autorità competenti il potenziale reato, corredato di tutte le informazioni raccolte strutturate e delle decisioni motivate e tracciate.

6.4 Fase 4 – Trasmissione

Qualora la segnalazione possa – a questo nodo del processo – sollevare dubbi concreti ovvero non risulti manifestamente infondata, il RPCT deve procedere alla trasmissione degli atti alle Autorità Competenti oppure al Responsabile HR, qualora se ne ravvedano gli estremi (la segnalazione riguardi una figura interna).

7 Pubblicazione

La presente Procedura è pubblicata sul sito internet del CCAM nella sezione "Amministrazione trasparente" sotto sezione "Whistleblowing" e sulla intranet aziendale. E' inoltra diffusa a tutti i Dipendenti tramite pubblicazione sulla bacheca interna e durante le fasi di formazione interna.

8 Archiviazione della documentazione

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nella presente procedura è conservata a cura della Direzione che dovrà documentare, se del caso, l'attribuzione ad altri soggetti aziendali della responsabilità della conservazione in originale della documentazione.
La stessa è, inoltre, messa a disposizione, su richiesta, solo ed esclusivamente ai soggetti autorizzati sulla base delle procedure aziendali e dell'organizzazione interna.
I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per il periodo previsto dalle normative vigenti.

9 Audit interni

La verifica periodica (con periodicità adeguata alla struttura ed al livello di rischio di ispezione) della corretta applicazione della presente procedura deve essere condotta da RPCT (in veste simulata di "Internal Audit") con attività di simulazione di segnalazione Whistleblowing.
Si considera metrica di misura l'efficienza e l'efficacia nella valutazione della liceità della segnalazione, nella corretta attribuzione della categoria di segnalazione effettuata, nella valutazione di aspetti privacy (presenza di controinteressati, livello di riservatezza, etc) ed infine nell'efficacia ed efficienza complessiva nel portare a termine la simulazione.

10 Allegati

Riferimento	Documento
[1] RIF_NORM	Riferimenti normativi
[2] REG_WHI	Registro segnalazioni

10.1 Allegato 1: Riferimenti Normativi

D.Lgs. 24/2023 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.
Comunicato stampa e Parere del Garante Privacy.
Ulteriori informazioni sul trattamento dei dati personali sono reperibili nell'informativa CCAM resa disponibile al seguente link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9844945

10.2 Allegato 2: Registro segnalazioni

Il registro segnalazioni è archiviato nella rete intranet, con accesso riservato al RPCT. Qualora necessario, lo stesso renderà temporaneamente disponibile (con accesso in sola lettura) il registro agli aventi diritto, per le sole finalità di tracciabilità della segnalazione.
Il registro segnalazioni deve essere considerato documento riservato e le protezioni devono almeno essere comparabili a quelle adottate per il trattamento di dati personali particolari.