

Sistema di segnalazione

POLICY WHISTLEBLOWING

Sommario

1	Scopo	3
2	Ambito di applicazione	3
3	Contenuti	3
3.1	Obiettivo del sistema di segnalazione	3
3.2	Ambito di applicazione del sistema di segnalazione	4
3.3	Chi può inviare segnalazioni?	5
3.4	Canali di segnalazione	6
3.4.1	Canale interno	6
3.4.2	Canale esterno	7
3.4.3	Divulgazioni pubbliche	7
3.5	Conflitto di interessi del Gestore delle segnalazioni	8
3.6	Invio di segnalazioni	8
3.6.1	Indice	8
3.6.2	Esclusione di false segnalazioni	9
3.6.3	Segnalazioni anonime	9
3.7	Elaborazione delle segnalazioni	9
3.7.1	Comunicazione con l'informatore	9
3.7.2	Indagine sulle segnalazioni e avvio di misure	9
3.8	Protezione degli informatori e delle persone accusate	10
3.8.1	Riservatezza e tutele garantite	10
3.8.2	Divieto di ritorsioni	10
3.8.3	Presunzione di innocenza	12
3.9	Conseguenze delle violazioni	12
3.10	Protezione dei dati	12
4	Documenti associati	12

1 Scopo

La presente procedura descrive il sistema di segnalazione delle violazioni delle disposizioni di legge, del Modello di organizzazione, gestione e controllo ex d. lgs. 231/2001, del Codice etico, della Politica di prevenzione della corruzione, del Modello Anticorruzione e del Codice di condotta adottati da Dussmann Service S.r.l. (da ora anche “la Società”). Essa illustra i canali per la presentazione delle segnalazioni, le condizioni e la procedura per la loro gestione.

2 Ambito di applicazione

La presente procedura si applica a tutti i dipendenti o consulenti esterni, che ricoprono il ruolo di Gestori della segnalazione nell'ambito del sistema di segnalazione della Società.

3 Contenuti

3.1 Obiettivo del sistema di segnalazione

Dussmann Group e, dunque, anche Dussmann Service S.r.l., dispone di un sistema di segnalazione per venire a conoscenza tempestivamente di potenziali violazioni gravi all'interno dell'azienda e poter dare seguito alle informazioni in modo adeguato. Un sistema di segnalazione è un efficiente sistema di allerta precoce per identificare e intervenire in relazione a comportamenti scorretti. Esso offre l'opportunità di chiarire internamente i casi sospetti, ridurre al minimo i danni finanziari e reputazionali e implementare misure per il futuro. Le segnalazioni tramite l'apposito sistema sono soggette a riservatezza e le persone che utilizzano il sistema di segnalazione interno sono protette da eventuali ritorsioni.

Precisamente, la presente policy è finalizzata a:

- garantire la riservatezza dei dati personali del soggetto segnalante e del presunto responsabile della violazione, fatta salva la normativa contenuta nei codici di rito e in normative collegate con riferimento alle indagini preliminari o a procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione, o comunque i procedimenti disciplinari in caso di segnalazioni effettuate in male fede;
- tutelare adeguatamente il soggetto segnalante contro condotte ritorsive e/o discriminatorie, dirette o indirette, per motivi collegati “direttamente o indirettamente” alla segnalazione;
- assicurare per la segnalazione un canale specifico, indipendente e autonomo.

La presente policy è stata redatta alla luce delle seguenti normative:

- Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio in tema di protezione delle persone che segnalano violazioni del Diritto dell'Unione e violazioni delle disposizioni normative nazionali;
- Decreto legislativo 10 marzo 2023, n. 24, pubblicato in Gazzetta Ufficiale il 15 marzo 2023, con il quale l'Italia ha recepito la Direttiva (UE) 2019/1937;

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (Regolamento generale sulla protezione dei dati).

3.2 Ambito di applicazione del sistema di segnalazione

Le segnalazioni devono riguardare violazioni che ledono l'interesse pubblico o l'integrità della pubblica amministrazione o dell'ente privato di cui si viene a conoscenza nel contesto della propria attività lavorativa o all'interno della catena di fornitura. Si può trattare di:

- a) violazioni commesse,
- b) fondati sospetti,
- c) violazioni non ancora commesse che il segnalante, ragionevolmente, ritiene potrebbero essere commesse sulla base di elementi concreti.

I fatti e gli illeciti che possono essere segnalati riguardano illeciti penali, civili, amministrativi, contabili, violazioni di normative comunitarie e sono elencati tassativamente dal **d. lgs. 24/2023**.

I) VIOLAZIONI DEL D. LGS. 231/2001, DEL CODICE ETICO, DEL CODICE DI CONDOTTA DI GRUPPO E DELLA POLITICA DI PREVENZIONE DELLA CORRUZIONE

In presenza di un Modello di organizzazione, gestione e controllo, possono essere segnalate le condotte illecite rilevanti ai sensi del d. lgs. 231/2001, in materia di responsabilità amministrativa degli enti derivante da reato presupposto, nonché le violazioni del Codice Etico, parte integrante del Modello di Organizzazione, Gestione e Controllo, del Codice di condotta di Gruppo, della Politica di prevenzione della corruzione e del Modello Anticorruzione.

II) ILLECITI CHE RIENTRANO NELL'AMBITO DI APPLICAZIONE DEGLI ATTI DELL'UNIONE EUROPEA O NAZIONALI

- **Appalti pubblici** = violazione delle norme per l'aggiudicazione di appalti pubblici e di concessioni nei settori della difesa, della sicurezza, dell'acqua, dell'energia, dei trasporti, dei servizi postali e qualsiasi altro contratto previsto dal decreto legislativo 31 marzo 2023, n. 36.
- **Tutela dell'ambiente** = scarico, emissione o rilascio di materiali pericolosi nell'aria, nel terreno, nell'acqua. Oppure raccolta, trasporto, recupero o smaltimento illecito di rifiuti pericolosi.
- **Sicurezza dei trasporti** = es. messa in pericolo di un aereo, dei suoi passeggeri, compromissione dell'operatività dell'aereo stesso.
- **Sicurezza alimenti e mangimi** = violazione delle norme riguardanti la sicurezza alimentare, l'integrità, la salubrità; tutela delle pratiche commerciali leali, degli interessi dei consumatori.
- **Salute e benessere degli animali**, per esempio negli allevamenti o nelle operazioni di trasporto, cautele durante la macellazione.
- **Sicurezza e conformità dei prodotti.**
- **Protezione dei consumatori.**

- **Radioprotezione e sicurezza nucleare** = sicurezza degli impianti nucleari, sicurezza relativamente alle sostanze radioattive presenti nelle acque destinate al consumo umano, rischi derivanti dall'esposizione alle radiazioni.
- **Servizi, prodotti e mercati finanziari** = tutela nei settori bancario, del credito, dell'investimento, dell'assicurazione, dei prodotti pensionistici individuali, dei titoli.
- **Antiriciclaggio e antiterrorismo**.
- **Salute pubblica** = tutela per gli organi e le sostanze di origine umana, per i prodotti medicinali e i dispositivi di impiego medico.
- **Sicurezza delle reti** dei sistemi informativi.
- **Tutela della vita privata** e della privacy (GDPR).

III) ATTI OD OMISSIONI CHE LEDONO GLI INTERESSI FINANZIARI DELL'UNIONE EUROPEA

- Corruzione.
- Frodi fiscali.
- Malversazioni o truffe aggravate ai danni dell'Unione europea.
- Attività illecite connesse alle spese o contributi dell'Unione europea.

IV) ATTI OD OMISSIONE RIGUARDANTI IL MERCATO INTERNO

- Compromissione della libera circolazione delle merci, delle persone, dei servizi e dei capitali.
- Violazione delle norme riguardanti la concorrenza e gli aiuti di Stato.
- Violazioni delle norme in materia di imposte sulle società o meccanismi il cui obiettivo è quello di ottenere un vantaggio fiscale che vanifica l'imposta sulla società.
- Messa in pericolo della tutela della libera concorrenza (es. controllo dei prezzi).

Lo strumento del Whistleblowing **non trova applicazione** in caso di

- A. mere contestazioni, rivendicazioni o richieste legate ad interessi di carattere personale (come ad esempio attinenti esclusivamente a rapporti individuali di lavoro o di pubblico impiego). Sono escluse, per esempio,
 - le segnalazioni riguardanti vertenze di lavoro e fasi precontenziose,
 - rivendicazioni o ritorsioni personali,
 - conflitti interpersonali tra la persona segnalante e un altro lavoratore o con i superiori gerarchici;
- B. segnalazioni prive di fondamento, presentate con dolo o colpa grave;
- C. informazioni acquisite sulla base di indiscrezioni, voci di corridoio;
- D. segnalazioni calunniose o diffamatorie.

3.3 Chi può inviare segnalazioni?

I soggetti che possono segnalare le violazioni sono i seguenti:

- a) dipendenti;
- b) collaboratori;
- c) fornitori, subfornitori, dipendenti e collaboratori degli stessi;
- d) liberi professionisti, consulenti, lavoratori autonomi,

- e) volontari e tirocinanti, retribuiti o non retribuiti;
- f) azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza;
- g) ex dipendenti, ex collaboratori o persone che non ricoprono più le posizioni indicate in precedenza, se le informazioni sono state apprese prima dello scioglimento del rapporto giuridico;
- h) soggetti in fase di selezione, prova o il cui rapporto giuridico con l'ente non sia ancora iniziato, se le informazioni sono state apprese durante le fasi precontrattuali;
- i) più in generale, le terze parti contrattuali (es. clienti, ecc.).

3.4 Canali di segnalazione

Il d. lgs. 24/2023 disciplina i canali di segnalazione e tutela i soggetti segnalanti.

Vi sono, infatti, tre canali di segnalazione:

3.4.1 Canale interno

La Società individua con atto separato il Gestore delle segnalazioni.

Canale scritto

Il primo canale è quello della piattaforma informatica crittografata, ovvero il software di segnalazione "Integrity Line".

Le segnalazioni di violazioni possono essere inviate preferibilmente tramite il software di segnalazione "Integrity Line" in diverse lingue, nel rispetto delle leggi locali sulla protezione degli informatori, al fine di garantire un trattamento sicuro, riservato ed efficiente. Le segnalazioni possono essere inviate per iscritto o tramite messaggio vocale.

È possibile accedere alla piattaforma di segnalazione Integrity Line tramite l'apposita sezione *whistleblowing* sul sito internet della Società: www.dussmann.it

In alternativa, è possibile effettuare la segnalazione attraverso posta ordinaria o a mezzo raccomandata A/R presso la sede della Società, sita in Via Papa Giovanni XXIII 4 - 24042 Capriate San Gervasio (BG).

In vista della protocollazione riservata della segnalazione a cura del Gestore, si raccomanda che la segnalazione venga inserita in due buste chiuse: la prima con i dati identificativi del segnalante unitamente, a discrezione di quest'ultimo, alla fotocopia del documento di identità; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "riservata al gestore delle segnalazioni di Dussmann S.r.l." La segnalazione è poi oggetto di protocollazione riservata da parte del gestore.

Canale orale

La piattaforma consente al segnalante di inoltrare note audio direttamente al Gestore.

In ogni caso, è possibile effettuare la segnalazione anche mediante un incontro in presenza o videoconferenza, fissato entro un termine ragionevole, con il Gestore delle segnalazioni. Per attivare tale modalità è possibile richiedere un appuntamento inoltrando la richiesta di colloquio sempre all'interno della piattaforma.

Al momento della ricezione della segnalazione, il Gestore della segnalazione deve documentarla mediante resoconto dettagliato del messaggio e il contenuto dev'essere controfirmato dal segnalante, previa verifica ed eventuale rettifica. Del resoconto sottoscritto deve essere fornita copia al segnalante. Per quanto attiene alle modalità di svolgimento dell'incontro in videoconferenza o in presenza (in un luogo adatto a garantire la riservatezza del segnalante) è sempre consigliabile procedere – previo consenso della persona segnalante – alla registrazione dello stesso attraverso dispositivi idonei alla conservazione e all'ascolto. Nel caso in cui non si possa procedere alla registrazione (ad esempio, perché il segnalante non ha dato il consenso o non vi è temporaneamente la disponibilità di strumenti informatici idonei alla registrazione) è necessario stilare un verbale che dovrà essere sottoscritto anche dalla persona segnalante, oltre che dal soggetto che ha ricevuto la dichiarazione. Copia del verbale dovrà essere consegnata al segnalante.

3.4.2 Canale esterno

Predisposto e gestito da ANAC (Autorità Nazionale Anticorruzione), al seguente indirizzo <https://whistleblowing.anticorruzione.it/#/>.

Tale strumento può essere utilizzato solo alle seguenti condizioni.

- Non è prevista l'attivazione del canale interno oppure, anche se obbligatorio, non è stato attivato oppure non è conforme ai requisiti richiesti dalla legge.
- Il segnalante ha già effettuato una segnalazione avvalendosi del canale interno ma la stessa non ha avuto seguito.
- Il segnalante ha fondati motivi di ritenere che la segnalazione interna non avrebbe un seguito o che ne deriverebbe un rischio di ritorsioni.
- La persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente per il pubblico interesse.

3.4.3 Divulgazioni pubbliche

Il segnalante può rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o altri mezzi di comunicazione di massa soltanto se:

- ha previamente effettuato una segnalazione interna e/o esterna alla quale non è stato dato riscontro entro i termini stabiliti;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere un efficace seguito in ragione delle specifiche circostanze del caso concreto.

Il primo canale che deve essere esperito, pertanto, è il canale interno (piattaforma digitale/canale orale). Lo scopo è quello di facilitare la comunicazione di informazioni concernenti violazioni riscontrate durante l'attività lavorativa.

3.5 Conflitto di interessi del Gestore delle segnalazioni

Il componente del Gestore delle segnalazioni che si trovi in una situazione di conflitto di interessi è obbligato ad astenersi in modo da garantire una gestione efficace, indipendente ed autonoma della segnalazione.

Le ipotesi di conflitto possono verificarsi nel caso in cui il Gestore coincida con il Segnalante, con il Segnalato o sia comunque una persona coinvolta o interessata dalla segnalazione.

La composizione collegiale del Gestore garantisce altresì continuità operativa nel caso in cui uno dei componenti si trovi in una situazione di impossibilità anche temporanea (es. ferie e/o malattia).

Qualora tutti i componenti del Gestore si trovino in una delle ipotesi di conflitto di interessi, la persona segnalante può rivolgersi ad ANAC mediante il canale esterno.

Trovano comunque applicazione tutte le disposizioni previste dalla presente procedura in quanto compatibili.

3.6 Invio di segnalazioni

3.6.1 Indice

È importante fornire tutte le informazioni rilevanti per chiarire efficacemente una segnalazione.

Se possibile, una segnalazione dovrebbe contenere le seguenti informazioni:

Dove?	Dove si è verificato l'incidente o dove si manifestano i suoi effetti? In quale società e in quale filiale/reparto o area si è verificato?
Quando?	Quando è stata commessa la violazione? Il periodo dovrebbe essere circoscritto nel modo più preciso possibile.
Cosa?	Cos'è successo? Cosa è stato fatto o cosa viene fatto in questo momento? Si sono verificati danni? Una descrizione precisa (concisa) dei fatti è utile.
Chi?	Chi ha commesso una violazione o è molto probabile che ne commetta una? Quali persone sono coinvolte nella situazione?
Come?	Come è stata commessa la violazione? Come ne sei venuto a conoscenza? Dettagli rilevanti aiutano a ottenere un chiarimento rapido ed efficace.

Se sono disponibili documenti o altre prove a sostegno della segnalazione, è opportuno caricarli su Integrity Line o inviarli in forma crittografata via e-mail o contrassegnati come riservati per posta all'ufficio di segnalazione.

3.6.2 Esclusione di false segnalazioni

Per evitare un uso improprio del sistema di segnalazione, è possibile fornire solo informazioni che, secondo le proprie conoscenze, possono essere ritenute corrette. Non sono tollerate segnalazioni intenzionalmente false e informazioni false.

3.6.3 Segnalazioni anonime

Sono ammesse anche **segnalazioni anonime** purché siano adeguatamente **circostanziate** e documentate, ossia corredate da elementi e informazioni tali che permettano di relazionare i fatti segnalati a contesti determinati (per esempio indicazione di specifiche aree aziendali, di nominativi, qualifiche, uffici, eventi particolari, dove e quando è stato commesso l'illecito, ecc). È bene precisare che, di fronte ad una segnalazione anonima, la tutela è assicurata qualora la persona segnalante sia stata successivamente identificata o la sua identità si sia palesata soltanto in un secondo momento.

3.7 Elaborazione delle segnalazioni

Le segnalazioni ricevute vengono elaborate dal soggetto designato come Gestore delle segnalazioni, tenuto alla riservatezza.

3.7.1 Comunicazione con l'informatore

La comunicazione tra il segnalante e il Gestore avviene tramite la Integrity Line. Quando viene presentata una segnalazione, il segnalante riceve un ID del caso e imposta una password che gli consente di accedere alla propria segnalazione e di contattare l'ufficio incaricato delle segnalazioni tramite una casella di posta sicura in qualsiasi momento.

Dopo l'invio, i segnalanti ricevono una conferma di ricezione entro il termine di 7 giorni previsto dalla legge. Se necessario, durante l'indagine possono essere poste domande di approfondimento o possono essere richieste ulteriori informazioni o documenti. Infine, il segnalante riceve un feedback sulle azioni intraprese o sui motivi del rigetto dell'indagine entro il termine di 3 mesi dalla data dell'avviso di ricevimento o, in mancanza, entro 3 mesi dalla data di scadenza del termine di 7 giorni per tale avviso.

3.7.2 Indagine sulle segnalazioni e avvio di misure

Il Gestore della segnalazione valuta inizialmente se la segnalazione è plausibile e valida. Viene effettuata una verifica per stabilire se sussistono ragionevoli sospetti che consentano un'ulteriore indagine e l'adozione di eventuali misure. Se la segnalazione è plausibile, viene avviata un'indagine che comprende, ad esempio, l'analisi dei dati o lo svolgimento di colloqui con le parti coinvolte. Per maggiori dettagli sulla procedura di gestione della segnalazione, si rinvia integralmente alla policy *Gestione delle segnalazioni*.

Sulla base dei risultati dell'indagine, se necessario vengono avviate misure volte a porre rimedio alla violazione e possibili azioni per prevenire comportamenti scorretti in futuro, quali corsi di formazione o adeguamenti dei processi aziendali. Possono essere applicate anche sanzioni disciplinari (si veda par. 4.8).

3.8 Protezione degli informatori e delle persone accusate

3.8.1 Riservatezza e tutele garantite

Gli uffici preposti alla segnalazione mantengono la riservatezza sull'identità del segnalante, delle persone oggetto della segnalazione e delle altre persone menzionate nella segnalazione.

Lo strumento del *Whistleblowing* tutela l'identità del soggetto segnalante e anche del soggetto facilitatore (ovvero la persona fisica che assiste il segnalante nel processo di segnalazione). L'identità, infatti, non può essere rivelata senza il consenso del segnalante. La riservatezza è garantita attraverso strumenti tecnologici, quali la piattaforma software crittografata per le segnalazioni, e anche tramite l'impossibilità di registrare i cookies del browser.

Per tale ragione, nel caso in cui la piattaforma fornita sia open source, soprattutto con chiavi condivise, chi fornisce la piattaforma deve garantire anche la conservazione delle chiavi crittografiche, indicando le modalità di conservazione delle stesse.

Sono irrilevanti i motivi che hanno indotto la persona ad effettuare la segnalazione: le tutele devono essere sempre garantite.

Le misure di protezione si applicano anche alle persone del medesimo contesto lavorativo del segnalante e che sono legate da uno stabile legame affettivo o di parentela entro il quarto grado, ai colleghi di lavoro che lavorano nello stesso contesto e che hanno un rapporto abituale e corrente con il segnalatore, agli enti di proprietà del segnalante o per i quali lo stesso lavora, nonché agli enti che operano nello stesso contesto lavorativo.

Il segnalante beneficia delle tutele garantite dal decreto solo se, al momento della segnalazione, aveva **fondato motivo di ritenere che le informazioni sulle violazioni segnalante, divulgate o denunciate fossero vere**. Se invece è accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia e diffamazione oppure la responsabilità civile per dolo o colpa grave, allora vengono meno le tutele garantite ed è possibile applicare una sanzione disciplinare.

3.8.2 Divieto di ritorsioni

Il Gestore delle segnalazioni non può rilevare l'identità del segnalante senza il suo consenso.

Il d. lgs. 24/2023 infatti tutela la riservatezza dell'identità del segnalante e prevede adeguate misure di protezione da eventuali ritorsioni collegate alla segnalazione direttamente o indirettamente.

Per ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che provoca o può provocare al segnalante un danno ingiusto e che possa provocare

danni fisici, psicologici, alla reputazione della persona, perdite economiche (per es. licenziamento, sospensione o misure equivalenti, retrocessione di grado o mancata promozione, riduzione dello stipendio o modifica dell'orario di lavoro, ecc.).

Precisamente, ai sensi dell'art. 17 del d. lgs. 24/2023, le seguenti fattispecie, qualora riconducibili a un comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere a seguito della segnalazione e che provoca o può provocare al segnalante, in via diretta o indiretta, un danno ingiusto, costituiscono ritorsioni:

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

Il segnalante può denunciare all'Anac le ritorsioni che ritiene di aver subito a causa di una segnalazione.

Gli atti di ritorsione accertati sono nulli e il segnalante ha diritto ad essere reintegrato nel posto di lavoro (in caso di licenziamento), al risarcimento del danno ed è previsto l'ordine di cessazione della condotta ritorsiva.

Al riguardo, l'ANAC ha specificato che la tutela, ancorché tardiva, va applicata anche in caso di sentenza di primo grado non confermata nei successivi gradi di giudizio, nei casi di archiviazione, nonché nei casi di accertata colpa lieve.

Infine, si ricorda che, come già detto, di fronte a una segnalazione anonima, la tutela è assicurata qualora la persona segnalante sia stata successivamente identificata o la sua identità si sia palesata soltanto in un secondo momento.

Le società del Dussmann Group sono tenute a proteggere i segnalanti da condotte ritorsive o discriminatorie dovute a una segnalazione, nonché le persone fisiche o giuridiche che hanno agevolato il segnalante nella presentazione della segnalazione.

3.8.3 Presunzione di innocenza

Le indagini seguono il principio di innocenza, per cui le persone accusate sono considerate presunte innocenti fino a quando non sia stata provata con ragionevole certezza una violazione.

3.9 Conseguenze delle violazioni

In caso di violazioni accertate, a seconda del soggetto ritenuto responsabile, possono essere adottate le misure disciplinari definite nel sistema disciplinare di cui al par. 9 della Parte Generale del Modello di organizzazione, gestione e controllo ai sensi del d. lgs. 231/2001, a cui si rinvia integralmente anche per l'iter da osservare.

Esempi di misure disciplinari, a seconda della gravità della violazione, includono:

- Ammonizione verbale;
- Ammonizione scritta;
- Sospensione dalle mansioni;
- Licenziamento disciplinare.

3.10 Protezione dei dati

Le segnalazioni ricevute, le attività di accertamento e le comunicazioni tra Gestore e persona segnalante sono documentate e conservate in conformità alle prescrizioni in materia di riservatezza e protezione dei dati (GDPR – Regolamento UE 2016/679).

Le segnalazioni, infatti, contengono dati personali, i quali possono essere trattati e conservati solo per il tempo necessario al loro trattamento e comunque non oltre cinque anni dalla data della comunicazione dell'esito finale della procedura di segnalazione

I dati personali sono conosciuti solo dal Gestore.

Le informazioni sulla raccolta, il trattamento e l'utilizzo dei dati personali nel contesto del sistema di segnalazione sono disponibili nella [dichiarazione sulla protezione dei dati per il sistema di segnalazione del Dussmann Group](#).

4 Documenti associati

- Policy whistleblowing di Dussmann Group
- Policy whistleblowing – Gestione delle segnalazioni

Documenti aggiuntivi applicabili:

- [Dichiarazione sulla protezione dei dati per il sistema di segnalazione del Dussmann Group](#).