POLITICA WHISTLEBLOWER

CONTENUTI

INTRODUZIONE

A CHI SI APPLICA QUESTA POLITICA?

COSA SEGNALARE?

COME SEGNALARE?

DA CHI E COME VENGONO ELABORATI I RAPPORTI?

COSA È LA RITORSIONE E COME SONO PROTETTI I SEGNALANTI DA ESSA?

PER QUANTO TEMPO VENGONO CONSERVATE LE SEGNALAZIONI?

A CHI SI APPLICA QUESTA POLITICA?

Questa politica si applica ai whistleblower e recepisce quanto previsto dal decreto legislativo 10 marzo 2023, n. 24 (il “Decreto Whistleblowing”) 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*”. I whistleblower sono persone che segnalano e che hanno acquisito informazioni su violazioni in un contesto lavorativo che possono ledere l’interesse o l’integrità dell’azienda. Questo include, ma non si limita a, i nostri attuali e precedenti dipendenti, lavoratori autonomi, consulenti, azionisti e persone appartenenti all'organo di gestione o di sorveglianza della nostra azienda, inclusi i loro membri non esecutivi, così come volontari, tirocinanti, stagisti retribuiti o non, nonché qualsiasi persona che lavora sotto la supervisione e direzione dei nostri partner in joint venture, appaltatori, subappaltatori e fornitori. Questa politica si applica anche ai whistleblower la cui relazione lavorativa deve ancora iniziare nei casi in cui le informazioni sulle violazioni siano state acquisite durante il processo di selezione o altre trattative precontrattuali. Protezione in base a questa politica deve essere fornita anche a persone che assistono i whistleblower nel processo di segnalazione (facilitatori), a terze persone che sono collegate al whistleblower (colleghi o parenti) e che potrebbero subire ritorsioni in un contesto lavorativo, e ad entità legali di cui il whistleblower è proprietario, per cui lavora o con cui è altrimenti connesso in un contesto lavorativo.

COSA SEGNALARE?

Il canale di segnalazione interna è destinato alle segnalazioni attuali o potenziali, che sono avvenute, stanno avvenendo attualmente o sono molto probabili che avvengano, oltreché a tentativi di occultare tali violazioni.

Una violazione è qualsiasi comportamento, atto od omissione che lede l'interesse o l'integrità dell'azienda, di cui il whistleblower sia venuto a conoscenza nel contesto lavorativo.

La normativa prevede due parametri, per il contesto privato, per definire il possibile contenuto della violazione:

a) Parametro dei dipendenti (Sopra i 50 dipendenti): Violazioni del diritto UE

Si tratta di: illeciti commessi in violazione della normativa dell'UE indicati nelle parti 1B e 2 dell'Allegato al Decreto e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato). Si precisa che le disposizioni normative contenute nelle parti indicate dell'Allegato sono da intendersi come un riferimento dinamico in quanto vanno naturalmente adeguate al variare della normativa stessa.

In particolare, si tratta di illeciti relativi ai seguenti settori:

1) contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.

A titolo esemplificativo, si pensi ai cd. reati ambientali, quali, scarico, emissione o altro tipo di rilascio di materiali pericolosi nell'aria, nel terreno o nell'acqua oppure raccolta, trasporto, recupero o smaltimento illecito di rifiuti pericolosi;

2) atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE.

Si pensi, ad esempio, alle frodi, alla corruzione e a qualsiasi altra attività illegale connessa alle spese dell'Unione;

3) atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle imprese e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle imprese;
4) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori indicati ai punti precedenti. In tale ambito vanno ricondotte, ad esempio, le pratiche abusive quali definite dalla giurisprudenza della Corte di Giustizia dell'Ue.

Si pensi ad esempio a un'impresa che opera sul mercato in posizione dominante. La legge non impedisce a tale impresa di conquistare, grazie ai suoi meriti e alle sue capacità, una posizione dominante su un mercato, né di garantire che concorrenti meno efficienti restino sul mercato. Tuttavia, detta impresa potrebbe pregiudicare, con il proprio comportamento, una concorrenza effettiva e leale nel mercato interno tramite il ricorso alle cd. pratiche abusive (adozione di prezzi cd. predatori, sconti target, vendite abbinate) contravvenendo alla tutela della libera concorrenza.

b) Parametro dell'adozione del Modello di Gestione ex D.lgs. 231/01 (anche meno di 50 dipendenti): Violazione dei reati presupposto indicati nel Modello di Gestione ex D.lgs. 231/01

Si tratta, tra gli altri, di:

- Indebita percezione di erogazioni, truffa in danno dello Stato, frode informatica in danno dello Stato o di un ente pubblico;
- Delitti informatici e trattamento illecito di dati;
- Delitti di criminalità organizzata;
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- Delitti contro l'industria e il commercio;
- Reati societari;
- Delitti con finalità di terrorismo;
- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- Delitti in materia di violazione del diritto d'autore;
- Reati tributari;

Oltreché qualsiasi comportamento non etico, in violazione delle politiche o delle procedure aziendali indicate nel Modello di Gestione.

LE SEGNALAZIONI CHE SONO ESCLUSE DALL'APPLICAZIONE DELLA NORMATIVA SONO:

- le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona Segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria 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.
  Sono quindi, escluse, ad esempio, le segnalazioni riguardanti vertenze di lavoro e fasi precontenziose, discriminazioni tra colleghi, conflitti interpersonali tra la persona Segnalante e un altro lavoratore o con i superiori gerarchici, segnalazioni relative a trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di lesioni dell'interesse pubblico o dell'integrità dell'amministrazione pubblica o dell'ente privato;
- le segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al d.lgs. 24/23 ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al d.lgs. 24/23;
- le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

COME SEGNALARE?

Il personale autorizzato (vedi sotto) è disponibile a fornire supporto o consigli sul processo di segnalazione di illeciti dell'azienda.

CANALI DI SEGNALAZIONE

Le segnalazioni possono essere presentate utilizzando la soluzione online di segnalazione di "Trusty."

La gestione delle segnalazioni interna può avvenire solo da parte di personale formato che gestirà la segnalazione in base a quanto previsto dalla normativa.

Resta fermo l'onere del whistleblower di conservare e non diffondere le credenziali di accesso al portale per verificare lo stato della sua segnalazione su "La tua casella di posta", dove è possibile anche trasmettere ulteriori approfondimenti.

Inoltre, le segnalazioni possono essere inviate tramite altri canali, elencati nella piattaforma "Trusty" o in un documento separato. Quando inviano le segnalazioni attraverso questi canali, gli informatori sono invitati a fornire i recapiti a cui desiderano ricevere le conferme di ricezione delle segnalazioni e i feedback sulle stesse da parte dell'azienda.

È sempre possibile richiedere un incontro di persona con il personale autorizzato e presentare la propria segnalazione direttamente a loro.

I whistleblower sono liberi di fare segnalazioni anche all'esterno. Tali segnalazioni devono essere indirizzate alle autorità competenti, come elencato in un documento separato.

Si sottolinea solo l'Autorità Nazionale Anticorruzione (ANAC) attiva un canale esterno per le segnalazioni che garantisce, tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità del whistleblower, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione. Le segnalazioni esterne devono essere trasmesse ad ANAC quale unico ente competente alla loro gestione, ad eccezione delle denunce alle Autorità giudiziarie.

Si precisa che il ricorso al canale di Segnalazione esterna istituito presso l'ANAC può avvenire solo se:

1) il canale di segnalazione interna indicato nella policy non risulti attivo;

2) il whistleblower ha già effettuato una segnalazione al canale indicato e la stessa non ha avuto seguito;

3) il whistleblower ha fondati motivi di ritenere che, se effettuasse una segnalazione interna tramite il canale previsto dalla presente policy, alla stessa non verrebbe dato seguito ovvero la segnalazione potrebbe determinare il rischio di ritorsione;

4) il whistleblower ha fondato motivo di ritenere che la violazione da segnalare possa costituire un pericolo imminente o palese per l'interesse pubblico.

CONTENUTO E IDENTITÀ DEL SEGNALANTE

Una segnalazione dovrebbe includere quanti più dettagli possibili su chi, cosa, dove, quando, come e perché in relazione alla violazione segnalata, così come qualsiasi prova a supporto. Sono benvenute anche qualsiasi altre informazioni su come l'azienda possa procedere al meglio nell'elaborazione della violazione segnalata.

I segnalanti possono presentare segnalazioni in modo anonimo o possono scegliere di divulgare la loro identità.

La piattaforma "Trusty" permette una comunicazione bidirezionale anonima anche se un segnalante sceglie di segnalare una violazione senza divulgare la propria identità.

Si incoraggiano i segnalanti a identificarsi. Ciò consente un trattamento più produttivo ed efficiente delle loro segnalazioni e la loro protezione contro le ritorsioni.

Le identità dei segnalanti, così come qualsiasi altra informazione dalla quale si possa dedurre direttamente o indirettamente le loro identità, non dovranno essere divulgate a nessuno al di fuori dei membri del personale autorizzato competenti a ricevere e dare seguito alle segnalazioni, senza il consenso esplicito dei segnalanti.

È opportuno considerare, inoltre, i seguenti obblighi specifici di riservatezza:

- nel procedimento penale l'identità del Segnalante è coperta dal segreto nei modi e nei limiti di cui all'art. 329 c.p.p.

- nel procedimento disciplinare:

a) l'identità del 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;

b) qualora la contestazione disciplinare sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato, la Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del Segnalante alla rivelazione della propria identità. In tal caso, è dato avviso al Segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati.

Nonostante la disposizione precedente, l'azienda dovrà divulgare l'identità di un segnalante quando richiesto dalla legge, informando in tal caso il segnalante prima di tale divulgazione, a meno che tali informazioni non possano mettere a rischio le relative indagini o procedimenti giudiziari.

Qualsiasi tentativo non autorizzato di identificare un segnalante o una persona interessata non è consentito e sarà sanzionato disciplinarmente.

DA CHI E COME VENGONO ELABORATI I RAPPORTI?

PERSONALE AUTORIZZATO

Il canale di segnalazione interno all'azienda è gestito da personale autorizzato, nominato in un documento separato. Il personale autorizzato è incaricato di ricevere e dare seguito alle segnalazioni.

Il personale autorizzato ha accesso diretto, illimitato e riservato all'organo di governo dell'azienda e all'alta direzione, a cui riferisce direttamente sull'andamento del sistema di gestione delle segnalazioni. Il personale autorizzato ha accesso diretto e illimitato alle risorse adeguate necessarie per garantire l'imparzialità, l'integrità e la trasparenza del sistema di gestione delle segnalazioni e dei suoi processi.

ELABORAZIONE DELLE SEGNALAZIONI

L'elaborazione di una segnalazione viene condotta nei seguenti passaggi, a seconda del contenuto della segnalazione e della sua natura:

- ricevuta – la segnalazione è stata ricevuta dall'azienda;
- triage iniziale – il contenuto della segnalazione viene valutato ai fini della categorizzazione, dell'adozione di misure preliminari, della priorità e dell'assegnazione per un ulteriore trattamento;
- elaborata – la segnalazione viene gestita, l'accuratezza dellla stessa viene valutata, viene condotta un'indagine interna;
- in indagine – la segnalazione è in fase di indagine;
- chiusa – l'elaborazione della segnalazione è stata completata; nessuna azione è considerata necessaria in risposta a una segnalazione, l'accertamento dei fatti determina che non è necessaria un'ulteriore indagine, la segnalazione viene deferita a un altro processo per essere trattata, o l'indagine è stata completata (sia che la violazione sia confermata o meno).

L'azienda mira a elaborare le segnalazioni in modo tempestivo. Circostanze come la complessità della violazione segnalata, priorità concorrenti e altre ragioni impellenti possono richiedere un periodo prolungato per il completamento dell'elaborazione della segnalazione.

L'azienda elabora le segnalazioni in modo confidenziale, imparziale e senza pregiudizi o prevenzioni contro il segnalante o qualsiasi altra persona coinvolta in, o testimone della violazione segnalata.

Le persone interessate, ovvero le persone citate nelle segnalazioni, godono della presunzione di innocenza. Possono essere informate delle rispettive segnalazioni in un momento appropriato. Qualsiasi indagine sarà condotta in modo da preservare la confidenzialità nella misura possibile e appropriata per garantire che le persone interessate non siano esposte a danni alla reputazione (le informazioni vengono condivise su base strettamente necessaria a sapere).

COMUNICAZIONE CON I SEGNALANTI

Dopo aver presentato una segnalazione, il segnalante riceverà un'accusa di ricevuta immediatamente e non oltre sette giorni da tale ricezione.

L'accusa di ricevuta viene inviata all'indirizzo e-mail fornito dal segnalante durante il processo di presentazione della segnalazione online sulla piattaforma di segnalazione "Trusty". La conferma della ricezione della segnalazione viene fornita anche nella casella di posta del segnalante, accessibile sulla piattaforma "Trusty" utilizzando le credenziali di accesso fornite al segnalante al termine del processo di presentazione della segnalazione. Queste sono fornite anche ai segnalanti anonimi.

Se la segnalazione viene presentata attraverso altri canali interni di segnalazione disponibili, l'accusa di ricevuta viene inviata ai dettagli di contatto forniti dal segnalante.

Il personale autorizzato mantiene la comunicazione con il segnalante e, se necessario, richiede ulteriori informazioni o prove e fornisce feedback al segnalante. Tale comunicazione viene condotta attraverso la casella di posta del segnalante sulla piattaforma "Trusty" o tramite altri canali di comunicazione concordati con il segnalante.

Il feedback al segnalante viene fornito al più tardi 3 mesi dopo aver presentato la segnalazione. Il feedback include informazioni sull'azione prevista o intrapresa come follow-up e sulle motivazioni di tale follow-up. Il feedback può essere limitato per evitare di compromettere eventuali indagini o altri procedimenti legali, così come a causa delle restrizioni legali su ciò che può essere comunicato riguardo al follow-up e ai risultati. In tal caso e se possibile, al segnalante verrà notificato il motivo della comunicazione limitata del feedback.

L'azienda può decidere di riconoscere e dare merito al segnalante per aver segnalato una violazione, con il consenso preventivo del segnalante (incluso, ma non limitato a, esprimere gratitudine e pubblica lode da parte della direzione).

COSA È LA RITORSIONE E COME SONO PROTETTI I SEGNALANTI DA ESSA?

DEFINIZIONE DI RITORSIONE

La ritorsione significa qualsiasi atto o omissione, minacciato, proposto o effettivo, diretto o indiretto, che avviene in un contesto lavorativo, è stimolato da una segnalazione interna o esterna o da una divulgazione pubblica e che causa o può causare un danno ingiustificato al segnalante.

In particolare, costituiscono ritorsioni, tra le altre, qualora riconducibili a tale configurazione:

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

La società ha una politica di tolleranza zero per la ritorsione. Qualsiasi forma di ritorsione, inclusi minacce di ritorsione e tentativi di ritorsione, sono proibiti e devono essere segnalati immediatamente. Tali segnalazioni possono essere presentate utilizzando il canale di segnalazione interna dell'azienda.

Chiunque si renda responsabile di ritorsione può affrontare gravi conseguenze interne - e potenzialmente esterne - ai sensi della legislazione o delle normative applicabili. Se l'azienda identifica persone coinvolte in atti di ritorsione, questi individui saranno soggetti a provvedimenti disciplinari, che possono includere il licenziamento.

Le azioni per affrontare una violazione propria del segnalante, oppure comportamenti scorretti non correlati al ruolo di segnalante, non sono considerate ritorsioni.

PROTEZIONE CONTRO LE RITORSIONI

L'azienda prenderà tutti i passi ragionevoli per proteggere i segnalanti dalle ritorsioni.

Se si stabilisce che sta avvenendo o è avvenuta una ritorsione, l'azienda prenderà misure ragionevoli per fermare e affrontare tale comportamento e supportare il segnalante. Se è richiesto un rimedio, l'azienda, nella misura più ampia possibile, ripristinerà il segnalante nella situazione che avrebbe avuto se non avesse subito ritorsioni. Ad esempio:

- reinstaurare il segnalante nella stessa posizione o in una equivalente, con lo stesso salario, responsabilità, posizione lavorativa e reputazione;
- accesso equo a promozioni, formazione, opportunità, benefici e diritti;
- ripristino alla precedente posizione commerciale rispetto all'organizzazione;
- ritirare cause legali;
- scuse date per qualsiasi danno subito;
- compensazione per i danni subiti.

Dopo che è stato fatto un rapporto, il personale autorizzato effettuerà una valutazione del rischio di ritorsioni contro il segnalante. A seconda delle probabili fonti di danno identificate attraverso la valutazione del rischio, il personale autorizzato identificherà ed attuerà strategie e azioni per prevenire tali ritorsioni o contenere comportamenti ritorsivi identificati per prevenire ulteriori danni, ad esempio:

- proteggere l'identità del segnalante;
- condividere informazioni su una base strettamente necessaria a conoscenza;
- comunicazione regolare con il segnalante;
- fornire supporto emotivo, finanziario, legale o reputazionale durante tutto il processo;
- incoraggiare e rassicurare il segnalante sul valore della segnalazione della violazione e prendere misure per assistere il loro benessere;
- cambiare il luogo di lavoro o gli accordi di segnalazione;
- avvertire le persone coinvolte o altre parti interessate che comportamenti ritorsivi o violazione della riservatezza possono essere un reato disciplinare.

Il personale autorizzato monitorerà e rivedrà i rischi in vari punti del processo, come quando si decide di investigare, durante l'indagine sul rapporto e una volta che il risultato di un'indagine è noto, così come, dove appropriato, dopo che il caso è stato chiuso.

Le protezioni sotto questa politica si applicano al segnalante anche se la violazione riportata non è confermata, se il segnalante aveva motivi ragionevoli per credere che le informazioni sulla

violazione riportata fossero vere al momento della segnalazione. Inoltre, i segnalanti che hanno riportato o divulgato pubblicamente informazioni sulle violazioni in modo anonimo, ma che in seguito sono stati identificati e hanno subito ritorsioni, avranno diritto alla protezione sotto questa politica.

Qualsiasi persona che faccia segnalazioni false consapevolmente sarà soggetta a azioni disciplinari e/o legali, che possono includere il licenziamento.

SANZIONI

È soggetto a sanzioni disciplinari chiunque si renda responsabile di una delle seguenti condotte:

1) compimento di atti di ritorsione ai danni del Segnalante o delle Persone Collegate in relazione a Segnalazioni;

2) ostacolo o tentato ostacolo all'effettuazione della Segnalazione;

3) violazione degli obblighi di riservatezza previsti dalla Procedura e dal d.lgs. 24/23;

4) mancata istituzione dei canali di Segnalazione secondo i requisiti previsti dal d.lgs. 24/23;

5) mancata adozione di una procedura per l'effettuazione e la gestione delle segnalazioni o mancata conformità della stessa al d.lgs. 24/23;

6) mancata verifica e analisi delle Segnalazioni ricevute.

È, inoltre, prevista l'irrogazione di una sanzione disciplinare nei confronti del Segnalante quando (fuori da specifici casi previsti dal d.lgs. 24/23) è accertata in capo allo stesso:

- anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria

ovvero

- la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

PROTEZIONE DEI DATI PERSONALI

Il trattamento dei dati personali nella gestione del canale di segnalazione interno e delle segnalazioni ricevute è effettuato a norma del GDPR e del Codice Privacy.

L'azienda ha definito 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, anche sulla base di una valutazione di impatto sulla protezione dei dati, ai sensi dell'art. 35 GDPR.

Il rapporto con fornitori esterni che trattano dati personali per conto dell'azienda è disciplinato tramite un accordo sul trattamento dei dati, ai sensi dell'art. 28 del GDPR che definisce la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, in conformità a quanto previsto dall'art. 28 GDPR.

Le persone competenti a ricevere o a dare seguito alle segnalazioni ai sensi della presente Policy sono state autorizzate a trattare i dati personali relativi alle segnalazioni ai sensi degli artt. 29 e 32 GDPR e dell'art. 2-quaterdecies del Codice Privacy.

Al whistleblower e alle Persone Coinvolte saranno fornite idonee informazioni ai sensi degli artt. 13 e 14 GDPR.

Con riferimento all'esercizio dei diritti e delle libertà dell'interessato, nel caso in cui lo stesso sia la Persona Coinvolta, i diritti di cui agli articoli da 15 a 22 GDPR non potranno essere esercitati (con richiesta al Titolare ovvero con reclamo ai sensi dell'articolo 77 GDPR) qualora ne possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del whistleblower (art. 2-undecies del Codice Privacy e articolo 23 GDPR) e/o al perseguimento degli obiettivi di conformità alla normativa in materia di segnalazione di condotte illecite. L'esercizio dei diritti da parte della Persona Coinvolta (incluso il diritto di accesso) potrà essere esperito, pertanto, nei limiti in cui la legge applicabile lo consente e successivamente ad un'analisi da parte degli organismi preposti, al fine di contemperare l'esigenza di tutela dei diritti degli individui con la necessità di contrasto e prevenzione delle violazioni delle regole di buona gestione societaria ovvero delle normative applicabili in materia. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti, devono essere cancellati immediatamente.

PER QUANTO TEMPO VENGONO CONSERVATE LE SEGNALAZIONI?

Se la violazione segnalata non viene comprovata dal personale autorizzato e i relativi dati non sono necessari all'azienda per ulteriori procedimenti, la segnalazione e tutte le informazioni raccolte relative alla segnalazione e al suo trattamento saranno cancellate definitivamente dopo la chiusura del caso e dopo che sarà trascorso il periodo di conservazione definito in un documento separato.

Se una violazione riportata è confermata, la segnalazione e tutte le informazioni raccolte relative alla segnalazione e al suo trattamento saranno conservate per tutto il tempo necessario per l'affermazione e l'esercizio di, o la difesa contro rispettive rivendicazioni legali, fino a 5 anni dalla chiusura.