uniting

Procedura Whistleblowing

Sommario

Whistleblowing: voglio saperne di più

Strumento di CSR (Corporate Social Responsability), essenziale per gestire i rischi e tutelare i lavoratori

Una corretta ed efficace gestione delle segnalazioni (Whistleblowing) è di estrema importanza per garantire il rispetto dei principi di legalità e di trasparenza definiti dal gruppo Uniting e dalle sue controllate (di seguito anche "Società" o "Organizzazioni"), nel rispetto delle disposizioni legislative vigenti e delle regole di condotta delle Società stesse.

La finalità del sistema di Whistleblowing è quella di consentire alle Società di venire a conoscenza di situazioni di rischio o di danno e di affrontare il problema segnalato in modo più tempestivo possibile. Un sistema evoluto e formalizzato attraverso policy e formazione specifiche permette inoltre una reale tutela del Segnalante.

Lo strumento di Whistleblowing contribuisce ad individuare e combattere le condotte illecite rilevanti ai sensi del D.lgs. 10 marzo 2023, n. 24 in attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, a tutelare i soci da danni economici e all'immagine, a diffondere la cultura dell'etica, della legalità e della trasparenza all'interno dell'azienda e a rafforzare il sistema dei controlli interni e della gestione dei rischi.

Gli obiettivi delle Società attraverso la presente procedura sono dunque:

- garantire trasparenza ed efficienza dei canali di segnalazione applicato;
- gestire tempestivamente le segnalazioni avanzate dai soggetti così come definiti;
- garantire la tutela dei dati personali dei soggetti segnalanti ed eventualmente l'anonimato qualora ne facessero richiesta;
- proteggere i soggetti segnalanti da potenziali ed eventuali situazioni di ritorsione.

Le finalità perseguite sono, dunque, di incoraggiare e facilitare le Segnalazioni all'interno della realtà aziendale e di ridurre i rischi di illeciti, costruendo e rafforzando il rapporto di fiducia con gli stakeholder e promuovendo e accrescendo una cultura aziendale basata su fattori di trasparenza, integrità, buona governance e compliance aziendale. Attraverso il Sistema Whistleblowing e la presente procedura le Società garantiscono inoltre che le condotte illecite rilevanti per legge siano indagate, sanate e sanzionate da ciascuna Società del Gruppo seguendo standard uniformemente applicabili. Ogni Società rimane tuttavia singolarmente responsabile del perseguimento e della sanzione delle violazioni commesse dai propri dipendenti identificati attraverso le procedure che compongono il Sistema Whistleblowing.

Il sistema EthicPoint

EthicPoint è un servizio esterno e certificato in termini di tutela della riservatezza del segnalante. Il suo approccio è quello del "servizio", ossia non offrire solo un canale per inviare le segnalazioni, ma una vera e propria forma di assistenza e consulenza (professionale) al segnalante, che è libero di utilizzarla anche senza formalizzare la segnalazione in completa riservatezza.
Per questo è essenziale che prima di ogni azione siano contattati gli esperti di EthicPoint che potranno fornire tutte le informazioni necessarie.

1. Scopo e campo di applicazione

Il presente documento definisce le regole per una gestione corretta ed efficace di una segnalazione da parte di un soggetto (Segnalante), anche al fine di individuare e rimuovere i possibili fattori di rischio e attivare, se necessario, le autorità competenti.

L'obiettivo del presente documento è quello di fornire al segnalante ed a tutti i soggetti coinvolti chiare indicazioni operative circa oggetto, contenuti, destinatari e modalità di trasmissione e gestione delle segnalazioni, nonché di tutte le forme di tutela che sono offerte, ai sensi di legge e delle procedure interne.

La presente procedura è stata definita anche come guida per la preparazione di circolari o documenti informativi e formativi per i soggetti coinvolti.

Si applica a tutte le attività svolte da Uniting Group Holding S.r.l. Società Benefit e dalle sue società controllate (ALL S.r.l., Kiwi Digital S.r.l., Flu S.r.l) di seguito anche "Società" o "Organizzazioni".

Nota 1: la presente procedura è stata adottata dall'Organo amministrativo quale atto organizzativo delle disposizioni di legge e come segnalazione[1] agli organi di rappresentanza dei lavoratori.

Nota 2: il servizio di Whistleblowing EthicPoint è il canale di segnalazione interna ai sensi del Decreto legislativo 24 del 2023, che esternalizza alcune attività della segnalazione attraverso una società certificata, che è qualificata attraverso specifico contratto di servizio e nomina a responsabile del trattamento dei dati personali ai fini del corretto trattamento degli stessi in conformità al Regolamento (UE) n.2016/679 ("GDPR") e del Decreto legislativo 24 del 10 marzo 2023.

2. Riferimenti normativi

- Decreto legislativo 24 del 10 marzo 2023
- Linee guida ANAC (versione applicabile)
- Guida Operativa per gli enti privati – Confindustria (versione applicabile)
- ISO 37002 - Guida per la gestione del whistleblowing

Vedere anche Allegato 1.

3. Termini e Definizioni: concetti essenziali da conoscere

Prima di procedere con la lettura della presente procedura relativa alla gestione delle segnalazioni, occorre precisare il significato che viene attribuito a taluni termini all'interno della presente Policy.

- **Segnalazione (interna):** comunicazione, orale o scritta, delle informazioni sulle possibili violazioni o illeciti, presentata tramite il canale di segnalazione interna.
- **Segnalante**: la persona fisica che effettua la segnalazione (la denuncia o la divulgazione pubblica) di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.
- **Segnalati**: coloro che sono oggetto di Segnalazione
- **Persona coinvolta**: la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
- **Seguito**: l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.
- **Riscontro**: comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione.
- **Violazione**: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

[1] Come previsto dall'articolo 51 del Decreto legislativo 81 del 2015: *"... sentite le rappresentanze o le organizzazioni sindacali per acquisire eventuali osservazioni ... (sulle) ... procedure per il ricevimento delle segnalazioni e per la loro gestione."*

- **Ritorsione**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.
- **Segnalazione in "mala fede":** la Segnalazione effettuata al solo scopo di danneggiare o, comunque, recare pregiudizio all'azienda, al soggetto segnalato o a terzi.
- **Denuncia:** atto con cui una persona porta a conoscenza dell'autorità competente (per esempio ufficiale di polizia giudiziaria) un reato procedibile del quale ha avuto notizia.
- **Divulgazione pubblica**: rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Si raccomanda sempre di consultare l'Allegato 2 per capire chiaramente cosa si può segnalare e cosa sono le segnalazioni non corrette.

Importante: per chiarire ogni dubbio contattare EthicPoint secondo i riferimenti forniti nella presente procedura.

4. I canali di segnalazione

Strumenti di segnalazione interna

In linea con quanto previsto dalle disposizioni normative in materia di tutela dei soggetti che segnalano illeciti o irregolarità, le Società hanno istituito un canale di segnalazione indipendente e certificato dotandosi di un apposito indirizzo per la raccolta e la gestione delle segnalazioni.

Il canale adottato consente di segnalare qualsiasi violazione prevista dal Decreto 24 del 2023 e dalle procedure aziendali da parte di tutti gli stakeholder, interni ed esterni, garantendo una comunicazione efficace e riservata.

Tale soluzione ha la caratteristica di tutelare al massimo la riservatezza del segnalante.

Le modalità di segnalazione attivati sono i seguenti:

1	***Landing page***	ethicpoint.eu/uniting-group/ Pagina web dedicata (incluso indirizzo email strumentale al funzionamento del servizio - uniting@ethicpoint.eu, all@ethicpoint.eu, kiwi@ethicpoint.eu, flu@ethicpoint.eu)
2	***Numero verde***	800 985 231 con messaggistica vocale registrata, previo consenso del segnalante (valido solo per l'Italia)

Ai sensi dell'Articolo 4, comma 3 del Decreto legislativo 24 del 2023 il Segnalante, attraverso i canali precedentemente descritti, può richiedere un incontro diretto (in presenza) per esporre oralmente la propria segnalazione con le modalità e nei termini che seguono.

Canali di segnalazione esterni

ANAC
Per poter ricorrere al canale di segnalazione istituito dall'ANAC, devono sussistere alcune condizioni, ai sensi dell'art. 6 del Decreto, In particolare:

- nel suo contesto lavorativo non è prevista l'attivazione del canale interno come obbligatoria o, se prevista, non è stata attivata

- la segnalazione interna non ha avuto seguito
- sussistano fondati motivi per ritenere che alla segnalazione interna non sarebbe dato efficace seguito
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse
- la persona ha fondati motivi di ritenere che, se effettuasse la segnalazione interna, questa non avrebbe seguito o che andrebbe incontro a ritorsioni

DIVULGAZIONE PUBBLICA
La normativa introduce anche la possibilità per il segnalante di effettuare una divulgazione pubblica beneficiando della protezione.

Si tratta di una novità estremamente delicata per le imprese, in ragione delle potenzialità lesive per l'ente di una denuncia effettuata in assenza di giustificati motivi o di fondati elementi di prova.

Per ricorrere a tale procedura deve ricorrere almeno una delle seguenti condizioni:

- che si sia previamente utilizzato il canale interno e/o esterno, ma non vi sia stato riscontro o non vi sia stato dato seguito entro i termini previsti dal decreto;
- che il segnalante ritenga sussistere fondati motivi di un "pericolo imminente e palese per il pubblico interesse", considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti.
- che il segnalante ritenga sussistere fondati motivi per ritenere che la segnalazione esterna possa comportare un rischio di ritorsione oppure non avere efficace seguito perché ad esempio

potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta a ricevere la segnalazione e l'autore della violazione. Dovrebbe in altri termini trattarsi di situazioni particolarmente gravi di negligenza o comportamenti dolosi all'interno dell'ente.

5. Comunicazione, informazione, formazione e sensibilizzazione

Il Sistema di gestione delle segnalazioni e il contenuto della presente procedura sono oggetto di comunicazione, informazione, formazione[2] e sensibilizzazione presso tutti i destinatari.

La presente procedura è disponibile ai possibili segnalanti, in particolare è disponibile su:

1 Intranet aziendale
2 Sito internet aziendale
3 bacheche aziendali

6. Gestione delle segnalazioni

I soggetti coinvolti (potenziali segnalanti)

È necessario prima di tutto individuare e definire, in modo chiaro ed esaustivo, i soggetti interessati dalla presente policy, ovvero chi può effettuare una segnalazione.

Le Società individuano quali potenziali segnalanti sia gli stakeholder interni che esterni. A titolo di esempio, si citano:

[2] Vedere programma specifico in funzione dei ruoli.

- i dipendenti delle amministrazioni pubbliche, i dipendenti degli enti pubblici economici, degli enti di diritto privato sottoposti a controllo pubblico, delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio;
- i lavoratori subordinati di soggetti del settore privato;
- i lavoratori autonomi, i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- i facilitatori;
- le 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;
- i 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.

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.

Obbligo di riservatezza

L'obiettivo della presente procedura è di assicurare la tutela del Segnalante, mantenendo riservata la sua identità, solo nel caso di segnalazioni provenienti da soggetti individuabili e riconoscibili.

Le segnalazioni anonime, ove queste siano adeguatamente circostanziate e rese con dovizia di particolari, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati, sono equiparate alle segnalazioni ordinarie. Le segnalazioni anonime e il loro trattamento avvengono comunque attraverso gli stessi strumenti previsti per quelle riservate, anche qualora l'interlocuzione con il segnalante anonimo non fosse possibile dopo la segnalazione stessa.

Anche le segnalazioni anonime sono soggette alla presente procedura, per quanto applicabile.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati.

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[3].

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.

[3] L'articolo 329 c.p.p. stabilisce, infatti, che gli atti di indagine compiuti dal pubblico ministero e dalla polizia giudiziaria sono coperti dal segreto fino a quando l'imputato (o l'indagato) non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari.

Oggetto e contenuto della segnalazione

Vengono considerate rilevanti le segnalazioni che riguardano ragionevoli e sinceri sospetti relativi ad un dipendente con riferimento a possibili frodi, pericoli o altri seri rischi che possano minacciare clienti, colleghi, stakeholders, il pubblico in generale o la reputazione delle Società[4].

In particolare, in considerazione anche di quanto previsto dalle normative di riferimento, la segnalazione può riguardare azioni od omissioni, commesse o tentate, che:

- violino 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;
- siano passibili di sanzioni amministrative o penali o di altre misure amministrative, anche nei confronti delle Società ai sensi del Decreto legislativo 231 del 2001;
- siano riferibili all'abuso del potere affidato ad un dipendente, al fine di ottenere vantaggi privati;
- siano l'evidenza di un mal funzionamento delle Società a causa dell'uso a fini privati delle funzioni attribuite (ad esempio: sprechi, nepotismo, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro);
- siano poste in essere in violazione del Codice Etico, del Regolamento interno aziendale, del Modello di Organizzazione, Gestione e Controllo (Decreto legislativo 231 del 2001) o di ogni altra policy o procedura o regolamento aziendale applicabile
- siano suscettibili di arrecare un pregiudizio patrimoniale o di immagine alle Società o ai soci o azionisti;
- siano suscettibili di arrecare un pregiudizio ai dipendenti o ad altri soggetti che svolgono la loro attività presso le Società.

La segnalazione non può riguardare, invece, rimostranze di carattere personale del Segnalante o richieste che attengono alla disciplina del rapporto di lavoro o ai rapporti con il superiore gerarchico o i colleghi, per le quali occorre fare riferimento all'ufficio personale.

Nella segnalazione devono risultare chiari i seguenti elementi essenziali, anche ai fini del vaglio dell'ammissibilità:

1. i dati identificativi del segnalante, nonché un recapito a cui comunicare gli aggiornamenti (restano però salvi i casi di segnalazioni anonime);
2. le circostanze di tempo e luogo in cui si è verificato il fatto e relativa descrizione dettagliata dello stesso;
3. le generalità o altri elementi che consentano di identificare il soggetto a cui attribuire i fatti segnalati.

La segnalazione deve preferibilmente contenere i seguenti elementi:

1. l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
2. l'indicazione di eventuali documenti che possano confermare la fondatezza di tali fatti;
3. ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

In sintesi, le segnalazioni, per essere prese in considerazione, devono essere adeguatamente circostanziate e fondate su elementi di fatto precisi e concordanti.

[4] Per approfondimenti consultare ISO 37002.

I destinatari della segnalazione

La previsione di canali di segnalazione interna che garantiscano massima riservatezza dell'identità del Segnalante, delle persone coinvolte, del contenuto della segnalazione e della relativa documentazione deve essere in conformità al Decreto legislativo 24 del 2023.

La gestione delle segnalazioni interne è affidata da parte delle Società ad alcune funzioni, esterne ed interne, specificamente nominate ed istruite per la gestione di tale attività e in materia di tutela dei dati personali e vincolate per iscritto alla confidenzialità e riservatezza. Tali soggetti, che garantiscono integrità, indipendenza e riservatezza, assumono la veste di "Gestori" delle Segnalazioni.

I Gestori delle segnalazioni sono:

EthicPoint – Servizio esterno certificato a tutela del segnalante – Gestore di primo livello
Organismo di Vigilanza – Gestore di secondo livello
Amministratore Delegato – Gestore di terzo livello

7. Procedura e compiti di chi riceve la segnalazione

Verifica della fondatezza della segnalazione

I Gestori interni agiscono in modo da garantire la confidenzialità delle segnalazioni ricevute, garantendo la riservatezza dell'identità del Segnalante, della persona coinvolta e della persona comunque menzionata nella Segnalazione nonché del contenuto della Segnalazione e della relativa documentazione, salvo quanto previsto dall'art. 12 del Decreto legislativo 24 del 2023 o che tale riservatezza non sia opponibile per legge (es. indagini penali, ispezioni di organi di controllo, ecc.). Tutte le informazioni saranno pertanto gestite in accordo alle disposizioni in materia di tutela del segnalante e di protezione dei dati personali.

Il Gestore di primo livello prende in carico la segnalazione, che viene trasmessa attraverso la casella di posta dedicata per ciascuna Società, al Gestore interno di secondo livello, rilasciando alla persona segnalante avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione. Il Gestore di secondo livello ne garantirà la riservatezza, anche nei confronti delle Società controllate non coinvolte nella segnalazione, per ruolo nonché in ottemperanza alle istruzioni rese ed al vincolo di confidenzialità e riservatezza sottoscritto. In caso di possibile conflitto di interesse o di indisponibilità del Gestore di secondo livello è possibile per il Segnalante richiedere o per il Gestore di primo livello far pervenire la segnalazione direttamente al Gestore di terzo livello, che agirà anch'esso in assoluta riservatezza, anche nei confronti delle altre Società del Gruppo non coinvolte nella segnalazione.

Se richiesto dal Segnalante attraverso i canali di segnalazione attivati dalle Società sopra indicati, è possibile un incontro diretto con il Gestore di secondo o, nei casi appena indicati, di terzo livello, che dovrà essere fissato entro un termine ragionevole, per svolgere la Segnalazione in forma orale; in tal caso, previo consenso del Segnalante, la Segnalazione resa in forma orale è documentata a cura del predetto Gestore mediante trascrizione. Il Segnalante può verificare, rettificare e confermare il verbale dell'incontro apponendo la propria sottoscrizione.

I Gestori interni danno diligente seguito alla segnalazione (analisi, istruttoria, trattazione e riscontro) , fornendone riscontro al Segnalante entro 3 mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione, attraverso l'indirizzo e-mail di cui sopra o attraverso i riferimenti che il segnalante eventualmente trasmetterà nella modalità di segnalazione optata.

Se indispensabile, i Gestori interni richiedono chiarimenti al segnalante o a eventuali altri soggetti coinvolti nella segnalazione, con l'adozione delle necessarie cautele. Verificano inoltre la fondatezza delle

circostanze rappresentate nella segnalazione attraverso ogni attività che si ritiene opportuna, compresa l'acquisizione di documentazione e l'audizione di eventuali altri soggetti che possano riferire sui fatti segnalati, nel rispetto dei principi di imparzialità, riservatezza e tutela dell'identità del Segnalante.

Il risultato delle valutazioni del Gestore interno incaricato della segnalazione, che dovrà essere formalizzato per iscritto, sarà comunicato agli organi societari preposti per l'adozione degli eventuali opportuni provvedimenti.

Le Società, sulla base di una valutazione dei fatti oggetto della segnalazione, possono decidere, in caso di evidente e manifesta infondatezza, di archiviare la segnalazione, dandone comunicazione al segnalante.

Le Società dispongono l'archiviazione diretta delle segnalazioni nei casi di:

- manifesta mancanza di interesse all'integrità delle Società;
- manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- manifesta insussistenza dei presupposti di legge per l'applicazione della sanzione;
- finalità palesemente emulativa;
- accertato contenuto generico della segnalazione o tale da non consentire la comprensione dei fatti, ovvero segnalazione corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;
- mancanza dei dati che costituiscono elementi essenziali della Segnalazione.

In linea con la normativa vigente in materia di tutela dei dati personali, per preservare le finalità investigative e nei casi previsti dalla legge, il/la segnalato/a può non essere immediatamente messo a conoscenza del trattamento dei propri dati da parte della Società, fintanto che sussista il rischio di compromettere la possibilità di verificare efficacemente la fondatezza della denuncia o di raccogliere le prove necessarie. Si prega di consultare in proposito per maggiori dettagli l'Informativa sul trattamento dei dati personali allegata al presente documento.

I dati personali relativi alle segnalazioni e la relativa documentazione vengono conservati per il periodo necessario al completamento della verifica dei fatti esposti nella segnalazione, non oltre i successivi 5 anni a decorrere dalla data di comunicazione dell'esito finale della Segnalazione, salvo eventuali procedimenti scaturenti dalla gestione della segnalazione (per esempio disciplinari, penali, contabili) nei confronti del/la segnalato/a o del segnalante (per esempio dichiarazioni in mala fede, false o diffamatorie). In tal caso saranno conservati per tutta la durata del procedimento e fino allo spirare dei termini di impugnazione del relativo provvedimento. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Verifica della fondatezza della segnalazione anonima

La fase di verifica della fondatezza della segnalazione da parte delle Società è analoga sia per la segnalazione riservata che per quella anonima. Tuttavia, per la segnalazione anonima si terrà conto delle seguenti indicazioni:

- la necessità di un maggiore approfondimento nella verifica degli elementi che ne escludono la archiviazione diretta;
- il contatto del Segnalante da parte delle Società avverrà se tecnicamente possibile.

8. Tutela del segnalante

Le Società dichiarano formalmente che non verrà messa in atto nessuna forma di discriminazione o ritorsione nei confronti del segnalante; al contrario, ogni comportamento in tale direzione sarà sanzionato. In particolare, ai sensi dell'articolo 17 del Decreto legislativo 24 del 2023, è espressamente statuito che i soggetti segnalanti (whistleblower), non possono subire alcuna ritorsione. La tutela non trova applicazione nei casi in cui la segnalazione riporti informazioni false rese con dolo o colpa grave.

In caso di sospette discriminazioni o ritorsioni nei confronti del Segnalante, correlabili alla segnalazione, o di abusi dello strumento di segnalazione da parte dello stesso, le Società possono provvedere all'irrogazione di sanzioni disciplinari.

Sono previste misure di sostegno per il soggetto segnalante:

- Informazioni;
- assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni.

La tutela non trova applicazione nei casi in cui la segnalazione riporti informazioni false rese con dolo o colpa grave.

9. Responsabilità del segnalante

La presente policy lascia impregiudicata la responsabilità penale, civile e disciplinare nell'ipotesi di segnalazione calunniosa o diffamatoria anche ai sensi del Codice penale e dell'art. 2043 del Codice civile[5].

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente policy, quali le segnalazioni manifestamente opportunistiche o compiute al solo scopo di danneggiare il denunciato o altri soggetti e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione delle Società oggetto della presente procedura, nonché di segnalazioni infondate effettuate con dolo o colpa grave.

10. Il trattamento dei dati personali

I dati personali dei soggetti segnalanti, del facilitatore, delle persone coinvolte o comunque menzionate nella Segnalazione e nella relativa documentazione sono trattati dalle Società, in qualità di Contitolari del trattamento, in conformità con il Regolamento (UE) n. 2016/679 ("GDPR"), del D. Lgs. n. 196/03 e s.m.i. ("Codice in materia di protezione dei dati personali") e del D.Lgs.n. 24/2023, secondo quanto indicato nell'Informativa sulla protezione dei dati personali unita al presente documento sub Allegato 5 e resa disponibile all'interno della piattaforma di WB.

11. Il Sistema sanzionatorio

Un sistema di whistleblowing efficace deve prevedere delle sanzioni sia nei confronti del Segnalante, in caso di abuso dello strumento di segnalazione, che nei confronti dei segnalati in caso di accertamento degli illeciti segnalati secondo quanto disposto dalla normativa vigente, inclusa la contrattazione

[5] Articolo 2043 Codice civile: Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno. Il reato di calunnia consiste, essenzialmente, nell'incolpare un'altra persona di aver commesso un reato, pur sapendola innocente (Articolo 368 del Codice Penale). Diffamazione: chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione (Articolo 595 del Codice penale).

collettiva applicabile, e nello specifico dal Decreto legislativo 24 del 2023 in materia protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali.

12. Ulteriori informazioni e contatti

Per ogni ulteriore informazione relativa alla procedura di cui sopra è possibile rivolgersi a:

1	Denise Lo Piparo – Head of ESG

ALLEGATO 1 - Scenario di riferimento legislativo

La tutela del dipendente e del collaboratore, segnalante condotte illecite all'interno dell'ambiente di lavoro sia del settore pubblico che del settore privato, è già ampiamente prevista in documento ufficiali di ampio respiro internazionale, quali le Convenzioni internazionali dell'ONU, OCSE, e Consiglio d'Europa, tutte ratificate dall'Italia in quanto di contenuto vincolante, e le Raccomandazioni dell'Assemblea parlamentare del Consiglio d'Europa.

A livello nazionale, il concetto di "whistleblowing" è stato introdotto per la prima volta con la Legge 190 del 2012 - Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione- che, limitatamente all'ambito del settore pubblico, con la disposizione dell'art. 1, co. 51, ha introdotto l'art. 54-bis nel Decreto legislativo 165 del 2001 - Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche - disciplinando un sistema di tutele per il dipendente pubblico che decide di segnalare condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro.

Successivamente, con la Legge 179 del 2017 - Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato - è stato poi introdotto il concetto di segnalazione nel settore privato, modificando l'art. 6 del Decreto legislativo 231 del 2001 ed apportando correttivi alla disciplina delle segnalazioni nel settore pubblico. Per quanto riguarda il settore privato, tale provvedimento statuisce che i Modelli di Organizzazione, gestione e controllo di cui al Decreto, debbano prevedere:

a. uno o più canali che consentano, ai soggetti apicali o posti sotto il controllo o la vigilanza dei medesimi – a tutela dell'integrità dell'ente – segnalazioni circostanziate di condotte illecite (rilevanti ai sensi della "231" e fondate su elementi di fatto precisi e concordanti) o di violazioni del Modello di organizzazione e gestione, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Inoltre, il medesimo articolo prevede che tali strumenti di segnalazione garantiscano la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione
b. almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante
c. il divieto di atti di ritorsione o discriminatori (diretti o indiretti) nei confronti del segnalante, per motivi collegati (direttamente o indirettamente) alla segnalazione
d. all'interno del sistema disciplinare, sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Infine, il Decreto legislativo 24 del 2023 ha recepito la Direttiva europea 1937 del 2019 in materia, riguardante la protezione delle persone che segnalano violazioni. Esso vuole dare piena ed effettiva attuazione ai principi di trasparenza e di responsabilità nella gestione delle segnalazioni, in quanto considerate strumento essenziale, non solo in termini di gestione dei rischi e di compliance generale, ma anche come strumento di relazione con gli stakeholder secondo le regole di governance più moderne.

In conformità alla Direttiva 1937 del 2019 e, pertanto, al suddetto decreto, i soggetti - in particolare quelli indicati all'articolo 3 del decreto 24 del 2023 - sono tenuti a segnalare eventuali comportamenti o situazioni che possano essere considerati non corretti o non coerenti con le procedure interne e più in generale alle disposizioni di legge vigenti[6].

[6] Le segnalazioni devono essere possibili come da procedure definite dalle Società e attraverso specifici canali di segnalazione interna (come previsto dall'articolo 4), al fine di garantire la riservatezza del segnalante e la sua protezione da eventuali ritorsioni.

ALLEGATO 2 – Esempi di illeciti o irregolarità da segnalare (non esaustivo)

- molestie
- discriminazione
- irregolarità amministrative e negli adempimenti contabili e fiscali
- false dichiarazioni, falsificazione o alterazione di documenti
- violazione delle norme ambientali e di sicurezza sul lavoro
- furto di beni di proprietà delle Società o di terzi
- appropriazione indebita di denaro, valori, forniture appartenenti alle Società o a terzi
- distruzione, occultamento o uso inappropriato di documenti, archivi, mobili, installazioni e attrezzature
- accettazione di danaro, beni, servizi o altro beneficio come incentivi per favorire fornitori o aziende
- falsificazione di note spese (ad esempio, rimborsi "gonfiati" o per false trasferte)
- falsificazione delle presenze al lavoro
- rivelazione di informazioni che per loro natura o per esplicita indicazione della legge o di disposizioni aziendali hanno carattere riservato, sia che si tratti di informazioni di proprietà delle Società che appartenenti a terzi (ad esempio competitor)
- utilizzo delle risorse e dei beni delle Società per uso personale, senza autorizzazione
- irregolarità in materia di antiriciclaggio
- frodi informatiche
- azioni o omissioni che risultino in danni o pericoli ai diritti umani, all'ambiente, alla salute pubblica, alla sicurezza e all'interesse pubblico
- la sussistenza di rapporti con soggetti (persone fisiche o giuridiche) aderenti a organizzazioni criminose di qualsiasi natura ovvero che partecipino in violazione ai principi di legalità
- la violazione delle misure restrittive nei rapporti economici e commerciali o delle sanzioni adottate in ambito nazionale, dell'UE ed internazionale
- appalti pubblici
- comunicazione non corretta su servizi o prodotti o sicurezza e conformità dei prodotti immessi nel mercato interno, rischi di mancata protezione dei consumatori
- utilizzo improprio di informazioni sensibili
- finanziamento del terrorismo
- tutela dell'ambiente o salute pubblica
- protezione dei dati personali
- sicurezza delle reti e dei sistemi informatici
- violazioni delle norme europee in materia di concorrenza e di aiuti di Stato
- violazioni riguardanti il mercato interno e in materia fiscale di imposte sulle Società

ALLEGATO 3 - Esempi[7] di illeciti o irregolarità che non si possono segnalare (non esaustivo)[8]

- 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
- Segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al decreto 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 decreto (Il d.lgs. n. 24/2023)
- Segnalazioni in materia di abusi di mercato di cui al Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio alla direttiva di esecuzione (UE) 2015/2392 della Commissione adottata sulla base del suddetto regolamento, che contengono già disposizioni dettagliate sulla protezione degli informatori
- Segnalazioni riguardanti gli enti creditizi e le imprese di investimento di cui alla Direttiva (UE) 2013/36 del Parlamento europeo e del Consiglio
- Segnalazioni di violazioni nel settore bancario.

[7] Linee guida Anac, par. 2.1.1.
[8] Segnalazioni non corrette possono prevedere sanzioni anche al Whistleblower anche di natura penale o amministrativa anche dopo il primo grado di giudizio, fatte salve quelle relative al rapporto di lavoro (per esempio CCNL) o contrattuale.

ALLEGATO 4 - Esempi di ritorsione

- sospensione
- eliminazione non motivate di vantaggi o benefit (incluso lo smartworking)
- la retrocessione di grado o la mancata promozione
- la riduzione dello stipendio
- la modifica dell'orario di lavoro
- la sospensione della formazione
- mancata assegnazione di note di merito o referenze negative
- l'imposizione o amministrazione di misure disciplinari ingiustificate
- la coercizione, l'intimidazione, le molestie o l'ostracismo
- la discriminazione, il trattamento svantaggioso o iniquo
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro permanente, laddove il lavoratore avesse legittime aspettative di vedersi offrire un impiego permanente
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- danni, anche alla reputazione della persona, in particolare sui social media, o la perdita finanziaria, comprese la perdita di opportunità economiche e la perdita di reddito
- l'inserimento in cosiddette "black list" sulla base di un accordo settoriale o industriale formale o informale, che possono comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro
- lo scioglimento del contratto per beni o servizi
- l'annullamento di una licenza o di un permesso
- la sottoposizione ad accertamenti psichiatrici o medici

Tali azioni sono vietate anche nei riguardi dei seguenti soggetti, al fine di evitare condotte di ritorsione "trasversale":

- facilitatori, ossia coloro che assistono il Segnalante nel processo di segnalazione e la cui assistenza deve essere riservata
- terzi soggetti connessi con i Segnalanti (per esempio colleghi o familiari)
- soggetti giuridici collegati al Segnalante

ALLEGATO 5 – Informativa sul trattamento dei dati personali - Whistleblowing

La presente Informativa è resa ai sensi degli artt. 13 e 14 del Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati, di seguito "Regolamento"), del D. Lgs. n. 196/03 e s.m.i. ("Codice in materia di protezione dei dati personali") e del D.Lgs. n. 24/2023 ("Decreto Whistleblowing") allo scopo di rendere informazioni sui trattamenti dei dati personali effettuati in relazione alla gestione delle Segnalazioni disciplinate dalla Procedura Whistleblowing societaria.

Contitolari del Trattamento

I Contitolari del trattamento dei Dati personali per le finalità indicate nella presente Informativa sono le seguenti società facenti parte del Gruppo Uniting (di seguito il "Gruppo"):

- Uniting Group Holding S.r.l. SB con sede legale in Monza (MB), Via Nino Bixio 1, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi, p. iva e c.f. 06737800968 (di seguito "Uniting");
- All S.r.l. con sede legale in Monza (MB), Via Nino Bixio 1, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi, p. iva e c.f. 08055240967 (di seguito "All");
- Kiwi Digital S.r.l. con sede legale in Monza (MB), Via Nino Bixio 1, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi, p. iva e c.f. 08114580965 (di seguito "Kiwi");
- Flu S.r.l. con sede legale in Monza (MB), Via Nino Bixio 1, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi, p. iva e c.f. 10328000962 (di seguito "Flu");

(di seguito congiuntamente le "Società" o le "Contitolari" del trattamento)

Le Società, nella gestione del Sistema di Whistleblowing, agiscono in qualità di Contitolari del trattamento, dovendosi intendere per tali "due o più società che determinano congiuntamente le finalità ed i mezzi del trattamento" così come previsto dall'articolo 26 del Regolamento ("trattamento congiunto dei dati").

Per questa ragione, le Società del Gruppo hanno sottoscritto un accordo di contitolarità del trattamento ai sensi dell'art. 26 del Regolamento (l'"Accordo"). L'Accordo definisce gli specifici doveri, i diritti e le responsabilità delle singole Società del Gruppo connessi al trattamento congiunto dei dati posto in essere nell'ambito del Sistema di Whistleblowing. Per le finalità perseguite congiuntamente le Contitolari del Trattamento hanno altresì determinato congiuntamente le modalità di Trattamento ed hanno definito, in modo chiaro e trasparente, le procedure per fornire agli Interessati, come di seguito definiti, un tempestivo riscontro qualora desiderassero esercitare i propri diritti, così come previsti dagli articoli 15, 16, 17, 18 e 21 del Regolamento.

Le società Contitolari del Trattamento, al fine di garantire una corretta gestione ed esecuzione dell'Accordo di contitolarità, hanno individuato nella società capogruppo Uniting il soggetto cui attribuire l'attività di trattamento indicata nella presente Informativa.

Per consultare il contenuto principale dell'Accordo e per qualunque informazione inerente al trattamento dei dati personali da parte delle Contitolari può scrivere al seguente indirizzo: privacy@uniting.it.

Responsabili del Trattamento e Persone autorizzate al trattamento dei dati

Come indicato nella Procedura Whistleblowing, la gestione delle Segnalazioni interne è affidata da parte delle Società ad alcune funzioni, esterne ed interne, specificamente nominate ed istruite per la gestione di tale attività e in materia di tutela dei dati personali.

Tali soggetti, che garantiscono integrità, indipendenza e riservatezza, assumono la veste di "Gestori" delle Segnalazioni, essendo stati istruiti dalle Contitolari ai relativi trattamenti e vincolati alla riservatezza.

Si precisa che i Gestori di primo livello, che, come indicato nella Procedura Whistleblowing, si occupano della ricezione, trasmissione e comunicazione delle Segnalazioni nel rispetto dei termini previsti dal Decreto Whistleblowing, appartengono alla società Audit People S.r.l. Società Benefit, con sede in Milano, Via Carlo Goldoni 1, iscritta al Registro delle Imprese di Camera di Commercio di Milano Monza Brianza Lodi, p.iva e c.f. 05755790960, la quale rende i servizi di ricezione e gestione delle Segnalazioni attraverso la soluzione tecnologica "Ethicpoint" da essa stessa fornita alle Contitolari, che se ne avvalgono come canale per le Segnalazioni nei termini indicati nella Procedura Whistleblowing. Pertanto, Audit People S.r.l. è stata nominata dalle Contitolari quale Responsabile del trattamento dei dati personali per tali finalità ai sensi dell'art. 28 del Regolamento.

Atteso, inoltre, che Uniting, quale Società Capogruppo, ha istituito l'Organismo di Vigilanza, nominato ai sensi dell'art. 6, punto 1, lett. b) del d.lgs. n. 231/2001, dotato di autonomi poteri d'iniziativa e controllo, il predetto Organismo di Vigilanza Uniting è stato individuato dalle Società quale Gestore di secondo livello, come specificato nella Procedura Whistleblowing, incaricato della gestione delle Segnalazioni, i cui membri sono stati anch'essi debitamente autorizzati al trattamento dei dati personali ed hanno ricevuto, al riguardo, adeguate istruzioni.

Infine, Gestore di terzo livello incaricato dalle Società della gestione delle Segnalazioni, come indicato nella Procedura Whistleblowing, è l'Amministratore Delegato di Uniting, anch'egli debitamente autorizzato ed istruito al trattamento dei dati personali.

Si rimanda integralmente alla Procedura Whistleblowing delle Società per le modalità di invio e gestione delle segnalazioni ai Gestori delle Segnalazioni qui indicati.

Categorie di dati personali

a) Dati personali comuni, di cui all'art. 4, comma 1 del Regolamento, del Segnalante (nel caso di Segnalazioni non anonime) nonché di eventuali persone coinvolte o menzionate nella Segnalazione e Facilitatori, come definiti dalla Procedura Whistleblowing (di seguito "Interessati") quali a titolo esemplificativo: dati anagrafici e dati di contatto;

b) Categorie particolari di dati di cui all'art. 9) del Regolamento ("i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale […] dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"), qualora inseriti nella Segnalazione o nella relativa documentazione.

c) dati cd. giudiziari ai sensi dell'art.10 del Regolamento (ovvero dati relativi a condanne penali e reati) qualora inseriti nella Segnalazione o nella relativa documentazione.

In generale, invitiamo a non fornire le categorie di dati di cui ai punti b) o c) o altre categorie particolarmente "sensibili" a meno che non sia strettamente necessario ai fini della Segnalazione Whistleblowing. Eventuali trattamenti di dati personali rientranti nelle categorie di dati particolari o dati giudiziari, laddove forniti, potranno essere trattati dalle Contitolari in adempimento di obblighi in materia di sicurezza del lavoro e di sicurezza sociale. Come specificato nel prosieguo della presente Informativa, i Dati Personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati tempestivamente.

Finalità e base giuridica del trattamento

I suddetti dati personali sono trattati dalle Contitolari per le seguenti finalità:

a) ricezione e gestione della Segnalazione effettuata ai sensi del Decreto Whistleblowing;

b) adempimento di obblighi previsti dalla legge o dalla normativa comunitaria;

c) difesa o accertamento di un proprio diritto in contenziosi civili, amministrativi o penali.

La base giuridica del trattamento è costituita:

i) per la finalità di cui alla lettera a), dall'adempimento di un obbligo legale a cui è soggetto il Contitolare del trattamento (art. 6, par. 1, lett. c) del Regolamento), fatta eccezione per la Società Flu la cui base giuridica è rappresentata dal legittimo interesse della stessa all'esecuzione di una richiesta dell'Interessato, nell'ambito dell'implementazione di Gruppo del Sistema Whistleblowing, e di quest'ultimo di inviare una Segnalazione Whistleblowing (art. 6, par. 1, lett. f); inoltre, per le Segnalazioni registrate raccolte telefonicamente o tramite sistemi di messaggistica vocale o comunque per la trascrizione di quelle raccolte in forma orale, dal consenso del Segnalante (art. 6, par. 1, lett. a) del Regolamento);

ii) per le finalità di cui alla lettera b) dall'adempimento di un obbligo legale a cui è soggetto il Contitolare del trattamento (art. 6, par. 1, lett. c) del Regolamento);

iii) per le finalità di cui alla lettera c) dal legittimo interesse del Contitolare (art. 6, par. 1, lett. f) del Regolamento).

Ferma restando la facoltà del Segnalante di richiede l'anonimato al momento della proposizione di una Segnalazione, come indicato nella Procedura Whistleblowing e quindi fatta eccezione in tal caso per i dati identificativi del Segnalante (che in ogni caso potrebbero nei limiti di legge rendersi necessari in un secondo momento nel corso della gestione della Segnalazione o della eventuale successiva istruttoria), il conferimento dei dati personali è necessario per il conseguimento delle finalità di cui sopra; il loro mancato, parziale o inesatto conferimento potrebbe avere come conseguenza l'impossibilità di ricevere e/o gestire la Segnalazione Whistleblowing e pertanto di adempiere un obbligo di legge.

Modalità del trattamento

I dati personali sono trattati sia con strumenti automatizzati che con strumenti manuali esclusivamente per le finalità sopra indicate. Specifiche misure di sicurezza sono osservate per garantire la riservatezza, l'integrità e la disponibilità dei dati, nonché la riservatezza dell'identità del segnalante e delle persone coinvolte/ o comunque menzionate nella Segnalazione e del contenuto della Segnalazione stessa e della relativa documentazione. In particolare, si precisa che il sistema di gestione delle Segnalazioni tramite il canale digitale "Ethic Point" adottato dalle Contitolari garantisce, anche tramite l'utilizzo di tecniche di crittografia in ogni fase, la riservatezza dell'identità del Segnalante (e ove richiesto il suo anonimato), delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione, fatto salvo quanto previsto dall'art. 12 del Decreto Whistleblowing.

Categorie di soggetti terzi ai quali i dati potrebbero essere comunicati

Il trattamento dei Dati ha luogo in Italia e non sussiste alcuna attività di trasferimento all'estero, inclusi Paesi al di fuori dello Spazio Economico Europeo (SEE).

I Soggetti autorizzati alla gestione delle Segnalazioni, come sopra indicati, potranno avere accesso ai Dati Personali trattati. Resta inteso che, in linea con il principio di tutela della riservatezza del Segnalante, delle persone coinvolte e del contenuto della segnalazione la condivisione dei dati personali sarà limitata allo stretto necessario per consentire l'inoltro e la gestione della Segnalazione stessa. Alcuni trattamenti possono, infine, essere effettuati da ulteriori soggetti terzi, per le finalità di cui al punto 3); tali soggetti opereranno in qualità di Titolari autonomi e sono essenzialmente ricompresi nelle seguenti categorie:

a. Consulenti (Organizzazione, Contenzioso, Studi Legali, ecc.);
b. Istituzioni e/o Autorità Pubbliche, Autorità Giudiziaria, Organi di Polizia.

Conservazione dei Dati Personali

Le Contitolari conservano i Dati Personali nei termini previsti dall'art. 14 del Decreto Whistleblowing, cioè per il tempo necessario al trattamento della Segnalazione e comunque per non oltre 5 anni a decorrere dalla data di comunicazione dell'esito finale della Segnalazione, salvo eventuali procedimenti scaturenti dalla gestione della segnalazione (per esempio disciplinari, penali, contabili) nei confronti del segnalato o del segnalante (per esempio dichiarazioni in mala fede, false o diffamatorie). In tal caso saranno conservati per tutta la durata del procedimento e fino allo spirare dei termini di impugnazione del relativo provvedimento.

I Dati Personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati tempestivamente.

Diritti degli interessati

L'interessato, nelle persone del Segnalante o del Facilitatore, ha diritto di accedere in ogni momento ai dati personali che lo riguardano e di esercitare i diritti previsti dagli articoli da 15 al 22 del Regolamento (diritto di accesso ai dati personali, diritto a rettificarli, diritto di ottenerne la cancellazione o cd. diritto all'oblio, diritto alla limitazione del trattamento, diritto alla portabilità dei dati personali o quello di opposizione al trattamento, laddove applicabili), inviando una e-mail all'indirizzo: privacy@uniting.it. Inoltre, l'Interessato ha diritto di proporre un reclamo al Garante per la protezione dei dati personali con sede in Piazza Venezia n. 11 - 00187 Roma (http://www.garanteprivacy.it/).

I suddetti diritti non sono esercitabili dalla persona coinvolta o dalla persona menzionata nella Segnalazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, ai sensi dell'art. 2- undecies del Codice in materia di protezione dei dati personali in quanto dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.