Whistleblowing Policy

Approvato dal Consiglio di Amministrazione il 12 luglio 2023

Aggiornata il 21 Luglio 2026

Unieuro S.p.A.

Sede Legale in Forlì (FO), Palazzo Hercolani, Via Piero Maroncelli, 10, 47122
Partita Iva: 00876320409

Storico delle modifiche

Revisione corrente:
3.0

Versione	Causale modifiche	Data
1.0	Approvazione del Consiglio di Amm. ne	15 Marzo 2019
2.0	Aggiornamento	12 Luglio 2023
3.0	Aggiornamento	21 Luglio 2026

INDICE

Premessa 4
1. Scopo e campo di applicazione 5
2. Destinatari 6
3. Riferimenti 7
4. Definizioni 7
4.1 Violazione 7
4.2 Segnalante 7
4.3 Segnalazione interna 7
4.4 Segnalazione "anonima" 8
4.5 Segnalazione in "mala fede" 9
4.6 Delegati Privacy 9
5. Responsabilità 9
6. Canali di Segnalazione interna 10
7. Modalità di trasmissione e istruttoria delle segnalazioni 11
7.1 Modalità di trasmissione 11
7.2 Verifica preliminare della Segnalazione 11
7.3 Indagine 12
7.4 Esito dell'indagine 13
7.5 Follow up 14
8. Reporting periodico 14
9. Misure di protezione previste 14
9.1 Protezione del segnalante 14
9.2 Diritti del Segnalato 15
10. Protezione dei dati e archiviazione dei documenti 16
11. Approvazione ed aggiornamento della Policy 17

Premessa

Il 29 dicembre 2017 è entrata in vigore la legge n. 179 "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" (pubblicata sulla Gazzetta Ufficiale, Serie Generale n. 291 del 14 dicembre 2017). Tale legge, che mira a incentivare la collaborazione dei lavoratori per favorire l'emersione di atti o fenomeni, all'interno di enti pubblici e privati, illeciti in contrasto con le regole etiche aziendali, è stata oggetto di modifiche in conseguenza della pubblicazione in Gazzetta Ufficiale di un ulteriore decreto legislativo in materia.

Nello specifico, il D.Lgs. n. 24 del 2023[1], in attuazione della Direttiva (UE) 2019/1937, ha modificato la disciplina nazionale previgente in materia di Whistleblowing, racchiudendo in un unico testo normativo il regime di protezione dei soggetti che segnalano condotte illecite di cui siano venuti a conoscenza in un contesto lavorativo.

Tale quadro regolatore mira a garantire una piena tutela della libertà di manifestazione del pensiero del segnalante e il rafforzamento della legalità e trasparenza all'interno degli Enti in funzione della prevenzione dei reati.

Se tali tutele erano già statuite dalla precedente legge del 2017, il D.Lgs. n. 24 del 2023 comporta un significativo ampliamento del perimetro di protezione dei segnalanti in ambito privato.

Il D.Lgs. n. 24 del 2023 è intervenuto modificando l'art. 6 del D.lgs. 231/2001[2] prevedendo al comma *2-bis* dello stesso che i Modelli di Organizzazione, Gestione e Controllo devono garantire un sistema di segnalazione al fine di evidenziare comportamenti illegittimi, garantendo canali di segnalazione interni, nonché un regime di protezione del segnalante, volto ad impedire condotte ritorsive del datore di lavoro e a sanzionare le violazioni della normativa in materia.

Le modifiche di maggior rilievo riguardano: i) l'ampliamento dei soggetti segnalanti; ii) l'estensione del perimetro di violazioni che possono costituire oggetto di segnalazione; iii) maggiore procedimentalizzazione delle attività interne agli enti (canali di segnalazione interni) al fine di assicurare la riservatezza del segnalante e dei soggetti coinvolti nella segnalazione, nonché per garantire una gestione tempestiva ed efficiente della stessa; iv) l'introduzione di un canale

[1] Pubblicato sulla Gazzetta Ufficiale, Serie Generale n. 63 del 15 marzo 2023.

[2] Il D.lgs. n. 24 del 10 marzo 2023 ha modificato il testo dell'art. 6 comma 2-bis D.lgs. n. 231/2001 e ha abrogato invece i commi 2-ter e 2-quater dell'art. 6 D.lgs. n. 231/2001, in precedenza disciplinati dalla Legge n. 179/2017.

esterno affidato all'ANAC, anche per il settore privato[3]; v) l'introduzione della possibilità di effettuare divulgazioni pubbliche delle violazioni, al ricorrere di determinate condizioni[4]; vi) il rafforzamento del ruolo e dei poteri sanzionatori dell'ANAC in funzione della corretta attuazione della disciplina in materia.

Infine, viene ampliato il raggio dei soggetti tutelati dalla normativa, includendo anche i c.d. facilitatori, ossia coloro i quali prestano assistenza al segnalante durante il processo di segnalazione e la cui attività deve rimanere riservata, ai soggetti terzi ed ai soggetti giuridici connessi al segnalante[5].

In ottica di compliance alla normativa, Unieuro (di seguito anche "la Società") ha adottato la presente Policy al fine di disciplinare le segnalazioni di comportamenti illegittimi e/o di violazioni di disposizioni nazionali ed europee che consistono in illeciti riguardanti specifici settori e mette a disposizione dei destinatari strumenti per effettuare le segnalazioni idonei a garantire, con modalità informatiche, 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.

1. Scopo e campo di applicazione

Il presente documento (di seguito "Policy") è volto a:

- stabilire le procedure attraverso cui effettuare una segnalazione di condotte o comportamenti illeciti o illegittimi, commissivi o omissivi, che costituiscono o possano

[3] Oltre alle segnalazioni c.d. "interne", viene stabilita, anche per i soggetti privati, la possibilità di rivolgere segnalazioni all'ANAC (c.d. "esterne") in determinati casi: 1) quando non previsto, nel contesto lavorativo nel quale opera il segnalante, l'obbligo di attivazione del canale di segnalazione interno, ovvero se, qualora obbligatorio, non sia stato attivato o, se presente, non sia conforme; 2) quando sia già stata presentata una segnalazione interna non processata o con provvedimento finale negativo; 3) quando il segnalante ha fondati motivi di ritenere che se effettuasse la segnalazione correrebbe il rischio di possibili ritorsioni; 4) quando il segnalante ha fondati motivi di ritenere che la violazione possa costituire pericolo imminente o palese per il pubblico interesse.
Verranno emesse dall'ANAC le linee guide relative alle modalità di presentazione e di gestione nel concreto delle segnalazioni esterne.

[4] Viene stabilita anche la possibilità di tutelare colui che segnala attraverso "divulgazioni pubbliche", purché vengano rispettate determinate condizioni (abbia prima segnalato internamente ed esternamente o direttamente esternamente, ma non sia stata intrapresa un'azione appropriata in risposta alla segnalazione entro il termine di tre mesi, oppure abbia fondati motivi di ritenere che possa esservi un pericolo imminente o palese per il pubblico interesse o le prospettive che la violazione sia affrontata efficacemente siano scarse).

[5] Ai sensi dell'art. 3 del D.lgs. 24 del 10 marzo 2023, si intendono ad esempio colleghi di lavoro e/o familiari o anche i soggetti giuridici connessi al segnalante.

costituire una violazione, o induzione a violazione, del Codice Etico di Gruppo, del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01 adottato dalla Società o delle policy e/o norme che regolano i processi aziendali, nonché violazioni di specifiche disposizioni nazionali ed europee[6];

- garantire un ambiente di lavoro in cui i Dipendenti ed i collaboratori possano serenamente segnalare le violazioni poste in essere all'interno della Società.

La presente Policy si applica a Unieuro.

2. Destinatari

Destinatari della presente Policy (di seguito "Destinatari" e/o "Segnalanti") sono:

- i Vertici aziendali ed i componenti degli organi sociali di Unieuro;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- tutti i dipendenti, lavoratori autonomi ed i collaboratori interni di Unieuro;
- liberi professionisti e consulenti che prestano la propria attività presso Unieuro;
- i lavoratori o i collaboratori, che forniscono beni o servizi o che realizzano opere a favore di Unieuro;
- volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso Unieuro.

[6] Ai sensi dell'art. 2 comma 1 lett. a) n. 5) del D.lgs. n. 24 del 10 marzo 2023 e degli allegati al decreto, si intendono gli illeciti nei seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi. Sono incluse altresì le violazioni: violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposte sulle società.

In aggiunta, ai sensi delle modifiche del D.lgs. n. 24 del 10 marzo 2023 sulla disciplina Whistleblowing, agli artt. 2 e 3 del Decreto è stabilito, inoltre, che la tutela del segnalante si applica anche: i) se il rapporto giuridico non è iniziato; ii) durante il periodo di prova; iii) dopo lo scioglimento del rapporto di lavoro.

3. Riferimenti

- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01 (di seguito anche "Modello 231");
- Codice Etico di Unieuro S.p.A. (di seguito anche "Codice Etico");
- D. Lgs. 8 giugno 2001, n. 231 e s.m.i;
- Legge 30 novembre 2017, n. 179;
- D.Lgs. 10 marzo 2023, n. 24;
- Policy e procedure aziendali;
- Modello Organizzativo Privacy (Regolamento UE 679/2016);
- Policy Anticorruzione.

4. Definizioni

4.1 Violazione

Per violazione si intende qualsiasi comportamento, atto o omissione che lede l'interesse pubblico o l'integrità della Società e che consista in una violazione del Codice Etico, del Modello 231, delle policy/procedure adottate dalla Società e/o in illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea o nazionali indicati nel decreto e nell'allegato al decreto.

4.2 Segnalante

Si intende la persona fisica (interna o esterna all'organizzazione di Unieuro) che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito della relazione professionale o lavorativa intercorsa con la Società.

4.3 Segnalazione interna

Per segnalazione interna, ai fini della presente Policy, si intende la comunicazione, scritta o orale, effettuata tramite i canali messi a disposizione dalla Società, da un segnalante avente ad oggetto

delle informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse in Unieuro.

Le segnalazioni devono essere effettuate in buona fede, fondate su elementi di fatto precisi e concordanti e circostanziate con informazioni specifiche in modo da risultare facilmente verificabili.

È particolarmente importante che la segnalazione includa, ove tali elementi siano conosciuti dal Segnalante:

- l'indicazione della funzione aziendale / punto vendita al quale si riferisce la segnalazione;
- i nominativi e ruolo delle persone coinvolte (interne e/o esterne) o elementi che possano consentirne l'identificazione;
- i nominativi di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione;
- la data / arco temporale e luogo in cui l'evento è accaduto;
- l'ambito / oggetto della violazione (Codice Etico, Modello 231, policy, disposizioni nazionali o dell'Unione Europea, ecc.);
- una descrizione dettagliata dei fatti verificatisi e modalità con cui se ne è venuti a conoscenza;
- indicare se i fatti sono già stati segnalati ad altri soggetti (autorità di controllo, soggetti interni o esterni, ecc.);
- riferimento ad eventuali documenti che possano confermare la fondatezza dei fatti riportati;
- l'indicazione circa la gestione dei dati personali del segnalante.

4.4 Segnalazione "anonima"

Per segnalazione anonima si intende la segnalazione di violazioni o sospette violazioni pervenuta alla Società senza l'indicazione dell'identità del segnalante.

A seguire, il concetto di "anonima" è da intendersi nel senso di "non nominativa". Sul piano della normativa a protezione dei dati personali (Regolamento Generale sulla Protezione dei Dati 2016/679/UE – di seguito "GDPR"), la segnalazione veicolata attraverso la piattaforma ha natura "pseudonima", nel senso che le viene assegnato un codice identificativo alfanumerico e che Unieuro può interagire con il segnalante dandogli riscontro e compiendo le attività previste dal D.Lgs. 24/2023. Dunque, il Segnalante ha piena garanzia che la sua identità rimanga riservata, in

conformità al D.Lgs. 24/2023 e alla politica di protezione del segnalante quale soggetto vulnerabile perseguita da Unieuro ai sensi del GDPR.

La segnalazione, anche se "anonima", deve essere documentata e circostanziata, così da fornire gli elementi utili e opportuni per consentire un'appropriata attività di verifica sulla fondatezza dei fatti segnalati.

4.5 Segnalazione in "mala fede"

Per segnalazione in "mala fede" si intende la segnalazione priva di fondamento, calunniosa o diffamatoria, fatta allo scopo di danneggiare o recare pregiudizio a dipendenti, a collaboratori interni, a membri di organi sociali o a terzi (es. clienti, fornitori, partner, consulenti, collaboratori) in relazione d'affari con Unieuro.

Nel caso in cui si dimostri che il dipendente abbia effettuato una segnalazione in mala fede, la Società potrà attivare il sistema disciplinare previsto dal proprio Modello 231 e in linea con quanto previsto dalla disciplina sul whistleblowing.

4.6 Delegati Privacy

Per Delegati Privacy si intendono le Funzioni aziendali interessate dalla segnalazione, ovvero sia i soggetti che hanno ricevuto da Unieuro le istruzioni specifiche privacy concernenti la gestione delle segnalazioni Whistleblowing.

5. Responsabilità

La verifica sulla fondatezza delle segnalazioni e le decisioni in merito alla gestione delle stesse sono affidate all'Internal Audit Director ("di seguito anche "IA Director") della Società.

Nello svolgimento di tale attività l'IA Director, nel caso in cui lo ritenga opportuno, può condividere l'oggetto della segnalazione ed essere supportato operativamente da Chief Legal & Risk Officer, Chief People & Culture Officer, RSPP e/o dal DPO della Società, mantenendo e garantendo la riservatezza dell'identità del Segnalante, salvo diversa indicazione del Segnalante stesso.

L'IA Director, pertanto:

- esegue tutte le attività istruttorie (verifica preliminare dell'esistenza dei presupposti, re-indirizzamento segnalazioni non di pertinenza);

- valuta le verifiche da compiere, le funzioni da coinvolgere nelle analisi, la richiesta di informazioni aggiuntive o l'eventuale archiviazione;
- garantisce la confidenzialità delle informazioni ricevute, anche in merito all'identità del segnalante;
- predispone la reportistica periodica riguardante le segnalazioni ricevute.

Nel caso in cui l'oggetto della segnalazione coinvolga l'IA Director, il segnalante può trasmettere la segnalazione direttamente ed in via esclusiva (tramite gli strumenti messi a disposizione della Società) al Chief Legal & Risk Officer. In tal caso, quest'ultimo procederà in autonomia nello svolgimento degli approfondimenti ritenuti necessari.

6. Canali di Segnalazione interna

In conformità alla normativa Whistleblowing, la Società mette a disposizione canali di segnalazione interna.

Le segnalazioni interne sono raccolte attraverso i seguenti canali:

- **in forma scritta**, tramite l'utilizzo del **Portale Whistleblowing** messo a disposizione dalla Società sul proprio sito web istituzionale e che prevede un percorso guidato per il segnalante.

  L'accesso al Portale Whistleblowing è soggetto alla politica "no-log" al fine di impedire l'identificazione del segnalante che intenda mantenere riservata la sua identità: ciò significa che, qualora l'accesso venga effettuato da un dispositivo non connesso alla rete aziendale, i sistemi informatici di Unieuro non sono in grado di identificare il punto di accesso al portale (indirizzo IP); nei casi in cui, invece, l'accesso al Portale Whistleblowing avvenga tramite un dispositivo connesso alla rete aziendale, Unieuro implementa soluzioni tecniche e organizzative per impedire di risalire all'utente che effettua la segnalazione. Per ciascuna segnalazione inserita, il Portale assegna un codice identificativo univoco che permette a ciascun segnalante di verificare lo stato di avanzamento della segnalazione, in modo del tutto riservato. Parimenti, nel caso in cui una segnalazione risulti non adeguatamente circostanziata, l'IA Director o il Chief Legal & Risk Officer[7], avvalendosi del Portale e della sua strumentazione, avrà facoltà di richiedere al segnalante, sempre e solo mediante tale codice ed all'interno della piattaforma,

[7] La segnalazione viene trasmessa al Chief Legal & Risk Officer, che procederà in autonomia nello svolgimento degli approfondimenti ritenuti necessari, nel caso in cui l'oggetto della segnalazione coinvolga l'Internal Audit Director

ulteriori elementi di dettaglio, ai fini di una analisi approfondita della fattispecie segnalata.

- **in forma orale**, tramite l'utilizzo del Portale Whistleblowing messo a disposizione dalla Società sul proprio sito web istituzionale mediante la registrazione di un messaggio vocale o mediante richiesta di incontro diretto con il gestore del canale di segnalazione. Nel caso di incontro diretto il gestore della segnalazione garantisce lo svolgimento dell'incontro entro un termine ragionevole.

7. Modalità di trasmissione e istruttoria delle segnalazioni

7.1 Modalità di trasmissione

Con riferimento al canale di segnalazione interna, questo è idoneo ad assicurare la riservatezza sull'identità del segnalante, del segnalato o delle persone coinvolte, nonché sul contenuto della segnalazione e sulla documentazione ad essa relativa.

I destinatari possono inviare le segnalazioni, secondo le modalità di seguito esposte, non appena vengano a conoscenza degli eventi che le hanno generate.

Le segnalazioni – come evidenziato al capitolo 6 "Canali di Segnalazione interna" - possono essere effettuate in forma scritta o in forma orale (mediante messaggistica vocale oppure richiesta di incontro con l'IA Director), tramite l'utilizzo del Portale on-line messa a disposizione da Unieuro e che prevede un percorso guidato per il Segnalante.

Per maggiori dettagli inerenti al corretto utilizzo del Portale Whistleblowing e alla compilazione dei relativi campi inerenti alla segnalazione, si rinvia alle FAQ dedicate sul sito web istituzionale di Unieuro.

7.2 Verifica preliminare della Segnalazione

Tutte le segnalazioni ricevute sono gestite dall'IA Director che procede ad una verifica preliminare al fine di verificare che la segnalazione rientri nel campo di applicazione della presente Policy e che siano stati forniti dati ed informazioni utili a consentirne una prima valutazione.

In tale fase, potrà essere condiviso l'oggetto della segnalazione e richiesto il supporto di altre funzioni (Chief Legal & Risk Officer, Chief People & Culture Officer, , RSPP, DPO) al fine di valutare

la presenza di idonei presupposti a procedere alla fase di indagine, sempre mantenendo e garantendo la riservatezza dell'identità del segnalante.

In qualunque caso, al termine della segnalazione, il segnalante riceve un codice identificativo che consente al segnalante di verificare sul Portale lo status di avanzamento della sua segnalazione e costituisce avviso di avvenuto ricevimento della segnalazione sul Portale medesimo.

Il segnalante potrà anche essere contattato, secondo le modalità esposte (attraverso la messagistica interna alla piattaforma) in precedenza, dall'IA Director o dal Chief Legal & Risk Officer[8] per la richiesta di ulteriori informazioni che risultassero necessarie.

7.3 Indagine

L'IA Director, nel rispetto dei termini previsti da normativa:

- può rigettare la segnalazione perché non ritenuta procedibile e/o ammissibile;
- può richiedere ulteriori informazioni aggiuntive per effettuare approfondimenti relativi alla segnalazione prima di decidere se prendere in carico o meno la segnalazione;
- può avviare analisi specifiche, avvalendosi delle strutture competenti, nonché coinvolgendo le Funzioni aziendali interessate dalla segnalazione (Delegati Privacy);
- assicura che l'indagine sia accurata, che abbia una durata ragionevole e che rispetti la riservatezza del segnalante e delle persone coinvolte, incluso il soggetto eventualmente segnalato;
- provvede, all'interno del portale whistleblowing, alla stesura di una sintesi dell'oggetto della segnalazione, utilizzata per la popolazione della reportistica destinata all'Organismo di Vigilanza.

Qualora l'IA Director ritenga procedibile e ammissibile la segnalazione provvederà quindi ad informare:

- l'Organismo di Vigilanza qualora si tratti di una segnalazione riguardante la violazione del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01, del Codice Etico, della Policy Anticorruzione;

[8] La segnalazione viene trasmessa all'Ufficio Legal nel caso in cui l'oggetto della segnalazione coinvolga l'Internal Audit Director

- il Top Management qualora la segnalazione riguardi la violazione di procedure o linee guida aziendali per attività che esulano dall'ambito di applicazione del D. Lgs. 231/01, ed anche in caso di violazioni di specifiche disposizioni nazionali ed europee.

7.4 Esito dell'indagine

Al termine dell'indagine, l'IA Director (o il Chief Legal & Risk Officer) comunica l'esito delle indagini svolte all'OdV o al Top Management, per competenza. Il segnalante, che tramite l'inserimento del codice identificativo a lui fornito, sul Portale online può monitorare l'iter della propria segnalazione, deve ricevere riscontro circa il seguito che si intende dare alla segnalazione entro tre mesi dalla data di avviso del suo ricevimento.

Qualora l'OdV o il Top Management per competenza rilevi la fondatezza di quanto emerso, si procede alla condivisione, in base agli esiti, con le Funzioni aziendali di volta in volta competenti (sempre nella persona dei Delegati Privacy), al fine di definire gli eventuali piani di intervento da implementare e le azioni da avviare a tutela della Società. Diversamente, qualora a conclusione delle analisi l'Organismo di Vigilanza o il Top Management per competenza dovesse rilevare l'assenza di elementi sufficientemente circostanziati o, comunque, l'infondatezza dei fatti richiamati nella segnalazione, quest'ultima sarà archiviata, unitamente alle relative motivazioni, dall'IA Director.

La Società potrà intraprendere le più opportune misure disciplinari e/o legali a tutela dei propri diritti, beni e della propria immagine, nei confronti del dipendente che abbia commesso o sia stato coinvolto in una violazione; eventuali misure disciplinari saranno intraprese in accordo con la Direzione HR e nel rispetto del CCNL di riferimento.

In aggiunta, in ottemperanza alla disciplina Whistleblowing, a garanzia del rispetto degli obblighi in materia, sono previste una serie di sanzioni amministrative pecuniarie che l'ANAC può applicare ai soggetti privati in caso di violazione delle regole stabilite dal decreto.

Il Dipendente che abbia commesso o sia stato coinvolto in una violazione non sarà immune da eventuali provvedimenti disciplinari per il solo fatto di aver segnalato una propria o altrui violazione, ai sensi della presente Policy. Tuttavia, tale circostanza potrà essere presa in considerazione nella valutazione del provvedimento disciplinare da adottare.

7.5 Follow up

L'IA Director, su indicazione dell'Organismo di Vigilanza o del Top Management, può prevedere l'esecuzione di interventi di follow-up per verificare l'effettiva risoluzione delle criticità o lo stato di avanzamento del relativo piano di azione, richiedendo informazioni ai Responsabili individuati.

8. Reporting periodico

L'IA Director elabora, con cadenza annuale, una relazione riepilogativa delle segnalazioni ricevute, delle attività di indagine effettuate o ancora in corso e delle evidenze emerse, includendo un'analisi dell'andamento delle stesse rispetto agli esercizi precedenti, che viene condivisa con l'Organismo di Vigilanza e, ove ritenuto opportuno, con il Top Management.

9. Misure di protezione previste

9.1 Protezione del segnalante

Il segnalante non subirà condotte ritorsive o discriminatorie per aver effettuato la segnalazione.

Per ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini, in via diretta o indiretta, un danno ingiusto al soggetto tutelato. Costituiscono fattispecie ritorsive, a titolo esemplificativo e non esaustivo: i) il licenziamento, la sospensione o misure equivalenti; ii) la retrocessione di grado o la mancata promozione; iii) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro; iv) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; v) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Unieuro garantisce la riservatezza dell'identità del segnalante e di ogni altra informazione, inclusa l'eventuale documentazione allegata, dalla quale si possa direttamente o indirettamente risalire alla sua identità. Resta ferma la facoltà per il segnalante di rendersi reperibile a contatti da lui stesso liberamente forniti o per Unieuro, nei casi previsti dall'art. 12 del D.Lgs. 24/2023, la possibilità di chiedere al segnalante il consenso alla rivelazione della sua identità.

La divulgazione non autorizzata dell'identità del segnalante oppure di informazioni in base a cui la stessa si possa dedurre, è considerata una violazione della presente Policy.

Inoltre, è necessario che:

- la medesima garanzia di riservatezza prevista per il segnalante sia prevista in favore delle persone coinvolte e/o menzionate nella segnalazione, nonché ai facilitatori;
- la gestione delle segnalazioni sia tenuta separata dalla gestione degli altri dati personali. Le informazioni raccolte e trattate nell'ambito della gestione delle segnalazioni devono essere trasmesse, per quanto necessario, esclusivamente ai soggetti incaricati del trattamento e competenti ad avviare il procedimento di verifica o ad adottare le misure necessarie in funzione delle risultanze. In ogni caso i destinatari delle informazioni devono garantire che queste ultime siano sempre gestite in regime di riservatezza e che siano applicate le dovute misure di sicurezza.

Le medesime misure di protezione si applicano anche: a) ai facilitatori; b) alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado; c) ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente; d) agli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

9.2 Diritti del Segnalato

Al segnalato devono essere riconosciute le medesime garanzie di riservatezza riconosciute alla persona segnalante, fino alla conclusione del procedimento avviato in ragione della segnalazione[9].

Durante l'attività di verifica e di accertamento di possibili non conformità, gli individui oggetto delle segnalazioni potrebbero essere coinvolti o ricevere notifica di questa attività ma, in nessun caso, verrà avviato un procedimento unicamente a motivo della segnalazione, in assenza di concreti riscontri riguardo al suo contenuto. Ciò potrebbe avvenire eventualmente in base ad altre evidenze riscontrate e accertate a partire dalla segnalazione stessa.

[9] Ai sensi dell'art. 12 comma 7 del D.lgs. n. 24 del 10 marzo 2023.

Al fine di garantire il diritto di difesa dei segnalati, è prevista la facoltà di interpellarli mediante procedimento cartolare, attraverso l'acquisizione di osservazioni scritte e documenti.

Qualora, infine, la segnalazione dovesse risultare infondata o in mala fede, al solo scopo di danneggiare la persona del segnalato, resta ferma l'irrogazione di sanzioni disciplinari nei confronti del segnalante, nonché la sua eventuale responsabilità penale e civile in caso di segnalazione diffamatoria o calunniosa.

10. Protezione dei dati e archiviazione dei documenti

Le informazioni ed ogni altro dato personale acquisiti sono trattati – anche nel contesto del Portale – nel rispetto del GDPR e del decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali) e ss.mm.ii., nonché nel rispetto delle pronunce delle autorità garanti in materia di protezione dei dati personali comunitarie e nazionali.

Al fine di garantire la riservatezza del Segnalante, il soggetto che gestisce le segnalazioni ha l'obbligo di usare le stesse solo per darvi seguito, nonché il divieto di rivelare l'identità del Segnalante o informazioni da cui la si possa evincere, senza il suo consenso espresso, a persone diverse da quelle competenti e autorizzate dalla legge.

La documentazione relativa alle segnalazioni deve essere archiviata in maniera sicura e nel rispetto delle norme vigenti all'interno della Società sulla classificazione e trattamento delle informazioni. Tale documentazione deve essere archiviata presso l'IA Director e deve essere accessibile solo al personale autorizzato.

Tale documentazione include almeno il nome, il codice identificativo e la struttura/ufficio del segnalante (laddove disponibili), i dettagli del segnalato, le dichiarazioni, le attività compiute, l'esito dell'indagine e le azioni intraprese.

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle relative attività, l'IA Director cura la predisposizione e l'aggiornamento di tutte le informazioni riguardanti le segnalazioni ed assicura, valendosi del Portale e della sua strumentazione informatica, l'archiviazione di tutta la correlata documentazione di supporto per il tempo necessario al trattamento della stessa e comunque non oltre un periodo di 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione.

11. Approvazione ed aggiornamento della Policy

Unieuro approva con delibera del Consiglio di Amministrazione la presente Policy. Questa è soggetta a revisione qualora le normative, cui si fa riferimento in qualità di best practice, siano soggette a cambiamenti o interpretazioni giurisprudenziali. In caso di modifiche ed interventi di natura sostanziale (e.g. significativo aggiornamento normativo), è previsto che la Policy sia soggetta ad ulteriore approvazione dell'Amministratore Delegato; in caso, invero, di modifiche di natura meramente formale (e.g. aggiornamenti organizzativi o afferenti al Portale Whistleblowing), il Chief Legal & Risk Officer cura l'aggiornamento e l'eventuale revisione della Policy e si impegna affinché questa venga correttamente diffusa e applicata.