15 – *POLICY WHISTLEBLOWING*

Policy aziendali

Storico delle versioni

Versione	Data Documento	Validato da	Principali variazioni
1.0	26/01/2018	Consiglio di Amministrazione	
1.1	22/06/2018	Consiglio di Amministrazione	Segnalazione presso Autorità di Vigilanza: inserito invito a consultare i siti di Consob e Banca d'Italia
1.2	10/04/2020	Consiglio di Amministrazione	Riferimenti al Regolamento Attuativo Banca d'Italia; cambio denominazione sociale e recapiti
1.3	24/10/2022	Consiglio di Amministrazione	Precisazione dell'oggetto della segnalazione nell'articolo "4.1 Contenuto della segnalazione"; previsione nuovo flusso verso l'Organismo di Vigilanza ex d.lgs. 231/2001
1.4	25/09/2023	Consiglio di Amministrazione	Recepimento della legge 30 novembre 2017, n. 179, che ha modificato l'art. 54-*bis* del d.lgs. 165/2001; Recepimento del d.lgs. 10 marzo 2023, n. 24 di attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019
1.5	27/02/2024	Consiglio di Amministrazione	Aggiornamento lato *privacy*; revisione del sistema di gestione delle segnalazioni, con implementazione del "filtro" verso il RPCT

Indice

1. Premessa

La SGR promuove una cultura aziendale caratterizzata da comportamenti corretti e da un buon sistema di *corporate governance*. Per tale ragione, la presente *Policy* definisce le modalità di comunicazione per la ricezione, l'analisi ed il trattamento delle segnalazioni di comportamenti illegittimi (c.d "*whistleblowing*").
Per comportamento illegittimo si intende qualsiasi azione od omissione, avvenuta nello svolgimento dell'attività lavorativa o che abbia un impatto sulla stessa, che arrechi o che possa arrecare danno o pregiudizio alla SGR e/o ai suoi Dipendenti e che:

- sia illecita, scorretta o eticamente scorretta;
- violi le disposizioni normative e regolamentari; o
- non sia conforme alle normative interne e ai protocolli adottati ai sensi del d.lgs. 231/01.

La presente *Policy* si applica a tutti i dipendenti, ai membri degli organi di supervisione strategica, gestione e controllo e ai collaboratori occasionali della SGR, ivi inclusi tirocinanti retribuiti e non retribuiti (i "Dipendenti"). La stessa deve, inoltre, essere comunicata a qualsiasi persona che presti servizi per la SGR, inclusi i consulenti finanziari o altri fornitori di servizi legati alla SGR in base ad un contratto.
In tale ambito, la presente *Policy* è volta a declinare idonee soluzioni organizzative in conformità a quanto previsto dalle disposizioni normative e proporzionalmente al profilo dimensionale e alla complessità operativa della SGR.

2. Glossario

- *Whistleblowing*: procedura volta a gestire le segnalazioni di comportamenti illegittimi posti in essere e ad assicurare le specifiche forme di tutela riconosciute dalla legge al segnalante;
- Segnalazione: comunicazione, scritta o orale, relativa a informazioni sulle violazioni, ossia sui comportamenti, atti o omissioni che ledono l'interesse pubblico o l'integrità della SGR;
- *Whistleblower*/segnalante: è la persona fisica che effettua la segnalazione o divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del contesto lavorativo della SGR;
- Facilitatore: la persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere riservata.

3. Riferimenti normativi

- Regolamento di attuazione degli articoli 4-*unidecies* e 6, comma 1, lettere b) e c-*bis*) del TUF, adottato dalla Banca d'Italia con provvedimento del 5 dicembre 2019 e ss.mm.ii. (di seguito "Regolamento Attuativo");
- Decreto Legislativo 24 febbraio 1998, n. 58 e ss.mm.ii. ("TUF");
- Decreto Legislativo 231/2007 e ss.mm.ii. (Sistemi interni di segnalazione delle violazioni), art. 48, come modificato dal d.lgs. n. 90/2017;
- Decreto Legislativo 10 marzo 2023 n. 24;
- Modello di Organizzazione Gestione e Controllo ex d.lgs. 8 giugno 2001, n 231;
- Codice Etico e di Comportamento.

Il *whistleblowing*, con limitato riferimento ai dipendenti delle pubbliche amministrazioni, è stato previsto per la prima volta in Italia dalla legge anticorruzione (legge n. 190/2012, che ha inserito, nel d.lgs. n. 165/2001, l'art. 54-*bis* Tutela del dipendente pubblico che segnala illeciti).

In materia di servizi di investimento, il recepimento della direttiva 2014/65/UE del 15 maggio 2014 (MiFID II), attraverso l'adozione del d.lgs. 3 agosto 2017, n. 129, ha costituito l'occasione per l'introduzione nel d.lgs. n. 58/98 (di seguito "TUF") di una disciplina unitaria dei sistemi di segnalazione delle violazioni nel settore del mercato finanziario. La nuova disciplina è contenuta negli articoli 4-*undecies* e 4-*duodecies* concernenti, rispettivamente, il c.d. "*whistleblowing* interno" e il c.d. "*whistleblowing* esterno".
Con la direttiva n. 2019/1937 è stato introdotto per tutti gli stati membri dell'UE, uno strumento uniforme per la segnalazione degli illeciti nel settore pubblico e privato, recepito in Italia con d.lgs. n. 24/2023.

4. Nomina del Responsabile dei sistemi di segnalazione interni

Conformemente con quanto previsto dalle disposizioni normative, la SGR individua un Responsabile dei sistemi interni di segnalazione (di seguito anche solo "il Responsabile") con il compito di:

- assicurare il corretto funzionamento delle procedure;
- riferire direttamente e senza indugio al Collegio Sindacale le informazioni oggetto di segnalazione, ove rilevanti;
- redigere una relazione annuale sul corretto funzionamento del sistema interno di segnalazione, contenente informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, da sottoporre al Consiglio di Amministrazione.

Il Consiglio di Amministrazione del 26 gennaio 2018 ha nominato il Responsabile della Funzione di Revisione Interna quale soggetto Responsabile dei sistemi interni di segnalazione, fermo restando, in conformità al disposto dell'art. 4, co. 6, d.lgs. n. 24/2023, quanto chiarito *infra* (Par. 4.3) circa **l'onere a carico del Responsabile di tempestiva comunicazione e trasmissione delle segnalazioni pervenute all'OdV ed al RPCT per quanto di rispettiva competenza**.

La SGR, coerentemente con le previsioni normative – alla luce del principio di proporzionalità – e con il proprio modello organizzativo e operativo, ha ritenuto di attribuire al Responsabile dei sistemi di segnalazione anche le attività di ricezione, nonché quelle di esame e valutazione delle segnalazioni.
Qualora il Responsabile dei sistemi interni, nonché della ricezione, esame e valutazione delle segnalazioni, sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio, le attività di ricezione, esame e valutazione delle segnalazioni sono svolte dalla "Funzione di Riserva", individuata dal Consiglio di Amministrazione del 26 gennaio 2018 nel Responsabile della Funzione di *Compliance*, conformemente all'articolo 6 del TUF.

5. Modalità di segnalazione

La SGR adotta un canale di segnalazione che garantisce la riservatezza del segnalante in conformità alle indicazioni ANAC (Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne. Approvate con Delibera n. 311 del 12 luglio 2023).
La segnalazione deve contenere le informazioni previste dal modello riportato in allegato alla presente Policy, cd**. "Modello di segnalazione"** (Allegato 1A ed Allegato 1B), ed è inviata dal soggetto segnalante al Responsabile dei sistemi interni.
In vista della protocollazione riservata della segnalazione a cura del gestore, il segnalante è tenuto a predisporre due buste chiuse contenenti, rispettivamente:

a) i propri dati identificativi, unitamente alla fotocopia del documento di riconoscimento (come da Allegato 1A);
b) l'oggetto della segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione (come da Allegato 1B).

In tal modo sarà possibile verificare la fondatezza della segnalazione in modalità anonima e, solo nei casi in cui sia strettamente necessario, rendere possibile la successiva associazione della segnalazione con l'identità del Segnalante.
Entrambe le buste devono essere inserite in una terza busta chiusa, da spedirsi tramite lettera raccomandata all'indirizzo TMF Compliance (Italy) S.r.l. – Corso Vercelli, 40 – 20145 Milano, all'attenzione personale del soggetto preposto alla ricezione della segnalazione.
Qualora tale soggetto sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio, all'indirizzo ConsiliaRegulatory S.r.l. - Via Larga, 8 – 20122 Milano, all'attenzione personale della "Funzione di Riserva" come sopra individuata.
La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

In alternativa, è possibile effettuare la segnalazione secondo le seguenti ulteriori modalità:

a) in forma orale, attraverso le seguenti linee telefoniche, non registrate:
    - 02/861914, per contattare il Responsabile dei sistemi di segnalazione interna;
    - 02/87389370, per contattare la Funzione di riserva.

b) su richiesta della persona segnalante, mediante un incontro diretto con il Responsabile dei sistemi interni di segnalazione, fissato entro un termine di tre giorni dall'invio della richiesta;

L'identità del segnalante sarà conosciuta solo dal Responsabile dei sistemi interni che ne garantisce la riservatezza, fatti salvi i casi in cui le informazioni siano necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.
In ogni caso, le segnalazioni anonime pervenute tramite il canale interno saranno considerate e gestite, nei limiti di quanto concretamente possibile, alla stregua di segnalazioni ordinarie.

5.1 Il *Whistleblower* ed il contenuto della segnalazione

Ai sensi del combinato disposto degli artt. 1 e 2 del d.lgs. n. 24/2023, per *whistleblower* si intende la persona che segnala, divulga ovvero denuncia all'Autorità giudiziaria o contabile violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato.

Oggetto di segnalazione:

possono essere segnalati comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica e che consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231 o violazione dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea (UE) relativi ai 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;
- atti od omissioni che ledono gli interessi finanziari dell'UE;
- atti od omissioni riguardanti il mercato interno (es. violazioni in materia di concorrenza ed aiuti di Stato);
- atti e comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'UE.

La segnalazione può avere ad oggetto anche:
- le informazioni relative alle condotte volte ad occultare le violazioni sopra indicate;
- le attività illecite non ancora compiute ma che il *whistleblower* ritenga ragionevolmente possano verificarsi in presenza di elementi concreti, precisi e concordanti;
- i fondati sospetti.

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

Contenuto della segnalazione:
È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni.
In particolare è necessario risultino chiare:
- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

5.2 Procedure di segnalazione

I canali di segnalazione
Con particolare riguardo al settore pubblico, nel quale rientra la SGR in quanto società *in house*, la disciplina in materia di *whistleblowing* prevede quattro diversi canali per la segnalazione delle violazioni, ossia: 1) canale interno; 2) canale esterno (gestito da ANAC); 3) divulgazioni pubbliche; 4) denuncia all'Autorità giudiziaria o contabile.
La scelta del canale di segnalazione non è rimessa al *whistleblower*, potendo questi ricorrere ai canali esterni solo al ricorrere delle ipotesi di cui all'art. 6, d.lgs. n. 24/2023.

In considerazione della natura di società finanziaria di Euregio Plus SGR S.p.A., alla stessa trova altresì applicazione la disciplina in materia di segnalazioni prevista dal d.lgs. n. 58/1998 (TUF).
In particolare, dal 3 gennaio 2018, ai sensi dell'articolo 4-*duodecies* del TUF e della Direttiva Ue 2015/2392 relativa al Regolamento UE n. 596/2014 in materia di abusi di mercato, il personale dei soggetti indicati dall'art. 4 *undecies* del TUF possono trasmettere le segnalazioni inerenti la violazione delle disposizioni contenute all'interno dello stesso decreto direttamente alle Autorità di Vigilanza (ANAC) in conformità a regole operative da loro definite. A tal fine si invitano gli interessati a consultare le sezioni dedicate sui siti istituzionali delle stesse e seguire le procedure ivi descritte.

Il canale interno

La SGR si è dotata di un sistema di segnalazione interna che:

a) garantisce la riservatezza e, per dati eventualmente trattati con modalità informatizzate, anche tramite il ricorso a strumenti di crittografia:
   - della persona segnalante,
   - del facilitatore,
   - della persona coinvolta o comunque dei soggetti menzionati nella segnalazione,
   - del contenuto della segnalazione e della relativa documentazione.

b) consente di effettuare segnalazioni:
   - in forma scritta;
   - orale, attraverso linee telefoniche / sistemi di messaggistica vocale;
   - su richiesta del segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

Una volta ricevuta la segnalazione, il Responsabile dei sistemi interni (ovvero la "Funzione di Riserva" qualora ricorrano i presupposti) comunica al segnalante (attraverso la stessa modalità di ricezione della segnalazione) l'avvio del procedimento di esame, mediante il rilascio di un avviso di ricevimento della segnalazione entro il termine di sette giorni dalla data di ricezione.
Il Responsabile procede quindi alla verifica della fondatezza o meno della segnalazione.
Nel corso del processo di analisi, il Responsabile dei sistemi interni effettua la valutazione della segnalazione in termini di rilevanza e gravità della stessa, mantenendo le interlocuzioni con il segnalante, ove lo stesso risulti rintracciabile, e richiedendo, se necessario, integrazioni.
Nel caso in cui la segnalazione risulti essere fondata, il Responsabile provvede a:

- dare diligente seguito alla segnalazione ricevuta;
- definire un apposito piano di intervento;
- informare tempestivamente il Consiglio di Amministrazione ed il Collegio Sindacale nei casi in cui si siano verificate violazioni di particolari gravità, nonché il Direttore Generale e l'unità Personale affinché valutino l'eventuale adozione di provvedimenti di competenza, incluso, ove sussistano i presupposti, l'esercizio dell'azione disciplinare.

Qualora oggetto della segnalazione sia il medesimo Responsabile dei sistemi interni di segnalazione e la segnalazione venga ritenuta fondata e rilevante, in via del tutto eccezionale l'informativa tempestiva agli Organi Aziendali dovrà essere fornita direttamente dalla "Funzione di Riserva".
Al termine dell'indagine, il Responsabile predispone una relazione all'interno della quale sono riportate:

- l'iter dell'indagine e le prove raccolte;
- le conclusioni alle quali si è giunti;
- le raccomandazioni e le azioni da porre in essere per sopperire alle violazioni riscontrate ed assicurare che queste non si verifichino in futuro.

In qualunque fase del procedimento – e senza attendere l'esito della valutazione – il Responsabile riferisce direttamente e senza indugio le informazioni rilevanti oggetto della segnalazione agli Organi Aziendali che provvedono, ove risulti necessario, ad adottare i relativi provvedimenti, anche d'urgenza, ivi incluso, se del caso, l'informativa al Responsabile Antiriciclaggio qualora ricorrano i presupposti per la segnalazione di un'Operazione Sospetta.
La procedura di segnalazione – dalla fase di ricezione alla fase di informativa agli Organi Aziendali – deve essere conclusa nel più breve tempo possibile secondo criteri che tengano conto della gravità della violazione, al fine di prevenire che il perdurare delle violazioni produca ulteriori aggravamenti per la SGR.
In ogni caso, la procedura deve concludersi entro 3 (tre) mesi dalla data dell'avviso di ricevimento. In mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione il Responsabile fornisce riscontro al segnalante sull'esito dell'istruttoria.

5.3 Provvedimenti decisionali

Qualora la segnalazione sia relativa o riconducibile a notizie relative alla commissione o al tentativo di commissione dei Reati, oltre che di violazione delle regole previste dal Modello 231 adottato dalla SGR, il Responsabile dei sistemi interni (ovvero la "Funzione di Riserva" qualora ricorrano i presupposti), dovrà inoltrare tempestivamente quanto ricevuto all'Organismo di Vigilanza 231 all'indirizzo odv@euregioplus.com per le opportune valutazioni di propria competenza.
Qualora la segnalazione sia relativa o riconducibile a notizie relative alla violazione delle disposizioni di cui alla l. n. 190 del 6.11.2012, recante "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*" e/o di cui al d.lgs. n. 33 del 14 marzo 2013 *"Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*", il Responsabile dei sistemi interni (ovvero la "Funzione di Riserva" qualora ricorrano i presupposti), dovrà inoltrare tempestivamente quanto ricevuto al Responsabile della Prevenzione della Corruzione e della Trasparenza all'indirizzo resp.anticorruzione@euregioplus.com per le opportune valutazioni di propria competenza.
Nel caso in cui le segnalazioni comportino l'assunzione di provvedimenti decisionali, gli stessi sono rimessi al Consiglio di Amministrazione, sentito il Collegio Sindacale.
Nel caso in cui il segnalante sia corresponsabile della violazione oggetto di segnalazione, il Consiglio di Amministrazione, sentito il Collegio Sindacale, prevede un trattamento privilegiato nei suoi confronti rispetto agli altri corresponsabili, salvi i casi in cui la condotta del segnalante risulti di particolare e critica gravità.

6. Forme di tutela adottate dalla SGR

6.1 Protezione del soggetto segnalante

6.1.1. Tutela della riservatezza

Al fine di evitare che il timore di subire conseguenze pregiudizievoli possa indurre a non segnalare le violazioni di cui al punto 1, l'identità e i dati personali del segnalante (*whistleblower*) non possono essere rivelati a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni senza il suo espresso consenso e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.
Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare seguito alle stesse.
La riservatezza, oltre che all'identità del segnalante, viene garantita anche a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante.
La riservatezza viene garantita anche nel caso di segnalazioni - interne o esterne - effettuate in forma orale attraverso linee telefoniche o, in alternativa, sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto con chi tratta la segnalazione.
La riservatezza del segnalante viene tutelata anche quando la segnalazione viene effettuata attraverso modalità diverse da quelle istituite in conformità alla disciplina di riferimento o perviene a personale diverso da quello autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo.
Fanno eccezione le ipotesi in cui sia configurabile in capo al segnalante una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o ai sensi dell'art. 2043 c.c., nonché le ipotesi in cui la riservatezza non sia opponibile per legge (quando, ad esempio, le informazioni siano

necessarie per lo svolgimento di indagini penali, tributarie o amministrative, oppure per le ispezioni degli organi di controllo).
Nell'ambito di procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione, l'identità del segnalante non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.
In particolare, in ambito giurisdizionale la tutela della riservatezza del segnalante è garantita con le modalità seguenti:

- nel procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p.;
- nel procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

Nell'ambito del procedimento disciplinare, la riservatezza del segnalante è garantita quando la contestazione al segnalato sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione (ipotesi che può verificarsi nei casi in cui la segnalazione è solo uno degli elementi che hanno fatto emergere l'illecito, mentre la contestazione disciplinare viene mossa sulla base di altri fatti da soli sufficienti a giustificare l'apertura del procedimento disciplinare). Nel caso in cui 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. In tale ultima ipotesi viene data comunicazione scritta al segnalante delle ragioni di tale rivelazione.
La segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della l. n. 241/1990. Le stesse sono altresì sottratte all'accesso civico generalizzato di cui agli artt. 5 e ss. del d.lgs. n. 33/2013.
La divulgazione non autorizzata dell'identità del segnalante o di informazioni in base alle quali si possa dedurre, è considerata una violazione della presente *Policy* ed è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.
Il trattamento dei predetti dati va quindi improntato alla massima cautela, a cominciare dall'oscuramento dei dati personali di tutti i soggetti (segnalante, facilitatore, segnalato, le altre persone menzionate nella segnalazione) la cui identità in base al d.lgs. 24/2023 deve rimanere riservata, qualora, per ragioni istruttorie, anche altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata.
Al fine di garantire il diritto alla protezione dei dati personali alle persone segnalanti o denuncianti, l'acquisizione e gestione delle segnalazioni, divulgazioni pubbliche o denunce, ivi incluse le comunicazioni tra le autorità competenti, avviene in conformità alla normativa in tema di tutela dei dati personali.

In base alle previsioni della normativa in materia di dati personali e del d.lgs. n. 24/2023, i titolari del trattamento, i responsabili del trattamento e le persone autorizzate a trattare i dati personali sono tenuti a rispettare, in particolare, i seguenti principi fondamentali:

- trattare i dati in modo lecito, corretto e trasparente nei confronti dei soggetti interessati («**liceità, correttezza e trasparenza**»);
- raccogliere i dati solo al fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce effettuate da parte dei soggetti tutelati dal d.lgs. 24/2023 («**limitazione della finalità**»);
- garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);
- assicurare che i dati siano esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, divulgazione pubblica o denuncia che viene gestita («**esattezza**»);

- conservare i dati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione («**limitazione della conservazione**»);
- effettuare il trattamento in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).
- rendere *ex ante* ai possibili interessati (ad es. segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) **un'informativa sul trattamento dei dati personali** mediante la pubblicazione di documenti informativi;
- assicurare l'aggiornamento del **registro delle attività di trattamento**, integrandolo con le informazioni connesse a quelle di acquisizione e gestione delle segnalazioni;
- Garantire **il divieto di tracciamento dei canali di segnalazione**;
- **Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato** nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante.

6.1.2. Divieto di condotte ritorsive e discriminatorie

Il soggetto che effettua una segnalazione non può essere sanzionato, licenziato o sottoposto a condotte ritorsive o discriminatorie[1], diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati, anche indirettamente, alla segnalazione.
Nei casi più gravi, e qualora sia possibile, il soggetto segnalante ha il diritto di chiedere il trasferimento in altro ufficio e, laddove necessario, l'assistenza psicologica indipendente in caso di *stress* derivante dalla segnalazione.
Le medesime misure di protezione si applicano anche:

- al facilitatore;
- alle persone del medesimo contesto lavorativo del segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una segnalazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del segnalante, della persona che ha di colui che ha sporto una denuncia o di colui che ha effettuato una segnalazione pubblica, che lavorano nel medesimo contesto lavorativo e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà del segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

È vietata, altresì, ogni forma di ritorsione o discriminazione avente effetti sulle condizioni di lavoro di chi collabora alle attività di riscontro della fondatezza della segnalazione.
Le presunte ritorsioni, anche solo tentate o minacciate, devono essere comunicate esclusivamente ad ANAC, alla quale è affidato il compito di accertare se esse siano conseguenti alla segnalazione, denuncia, divulgazione pubblica effettuata.

[1] Ai sensi dell'art. 2, co. 1, lett. m), d.lgs. n. 24/2023, per ritorsione si intende "*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*"

6.2 Protezione dei dati e archiviazione dei documenti

Al fine di assicurare la ricostruzione delle differenti fasi del processo di segnalazione, è cura del Responsabile dei sistemi interni garantire:

- la tracciabilità delle segnalazioni e delle relative attività istruttorie;
- la conservazione della documentazione inerente le segnalazioni e le relative attività di verifica, in appositi archivi (cartacei/informatici), con gli opportuni livelli di sicurezza e riservatezza;
- la conservazione della documentazione e delle segnalazioni per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione e nel rispetto delle procedure *privacy* vigenti nella SGR.
  Se per la segnalazione si utilizza il canale telefonico, la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del personale addetto. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.
  Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

È tutelato ai sensi della normativa vigente e delle procedure aziendali in materia di *privacy*, il trattamento dei dati personali delle persone coinvolte e/o citate nelle segnalazioni. A tal fine, viene fornita un'opportuna Informativa *Privacy* sulla gestione del trattamento di *whistleblowing* sia al segnalante che al segnalato.
L'identità del segnalante può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato; con riguardo all'identità del segnalante non trova pertanto applicazione la disposizione di legge in base alla quale il presunto responsabile ha il diritto di ottenere, tra l'altro, l'indicazione dell'origine dei dati personali.

7. Responsabilità del soggetto segnalante

La presente *Policy* lascia impregiudicata la responsabilità penale e disciplinare del *whistleblower* nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale (artt. 368 e 595) e dell'art. 2043 c.c.
Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso del presente regolamento, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il segnalato e/o altri soggetti, ed ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto del presente documento.

8. Relazione annuale

Come previsto dall'Allegato 4 del Regolamento Attuativo, il Responsabile dei sistemi interni redige annualmente, nel rispetto della tutela dei segnalanti, una relazione sul corretto funzionamento dei sistemi interni di segnalazione contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute.
Tale relazione è approvata dal Consiglio di Amministrazione, sentito il Collegio Sindacale, e viene messa a disposizione del personale.

Allegato 1A: Modello di segnalazione: dati identificativi

Informativa *Privacy* al segnalante sulla gestione del trattamento di *whistleblowing* (ai sensi del Regolamento UE 2016/679 - c.d. GDPR)

La presente informativa viene resa ai sensi del GDPR per illustrare le regole adottate da Euregio Plus SGR S.p.A. (la "Società" nel seguito) per la tutela dei dati nell'ambito del trattamento di gestione del *whistleblowing* di cui al d.lgs. 24/2023 ("decreto *whistleblowing*" nel seguito). In quanto tale essa è parte integrante della procedura operativa predisposta ad uso dei soggetti segnalanti.

Titolarità e contatti

La titolarità del trattamento è in capo alla Società. Per ogni informazione, per contattare titolare, responsabile del trattamento, responsabile della protezione dati (c.d. DPO) nonché per l'esercizio dei diritti riconosciuti dalla normativa vigente l'interessato potrà rivolgersi, in alternativa:

- all'indirizzo di posta elettronica info@euregioplus.com;
- alla sede della Società, mediante RR, all'indirizzo Passaggio Duomo, 15, 39100, Bolzano, all'att.ne del servizio di presidio *privacy*.

Finalità, base giuridica, condizione di liceità del trattamento

Il trattamento ha come finalità la raccolta e la successiva gestione delle segnalazioni necessarie per avviare e, ove applicabile, gestire le pratiche di accertamento dei fatti segnalati con la correlata adozione degli eventuali provvedimenti.
Il trattamento viene svolto con condizione di liceità dovuta ad "obbligo legale del titolare" ed è motivato dalle indicazioni giuridiche provenienti dal GDPR e d.lgs. 196/03 nonché dal citato decreto *whistleblowing*.
Ove il segnalante non sia anonimo, il modulo di segnalazione è integrato con la richiesta di consenso alla comunicazione dei dati dello stesso a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni, inclusi l'autorità disciplinare e i soggetti segnalati coinvolti nella segnalazione nei casi previsti dal decreto *whistleblowing*. In mancanza di consenso la segnalazione verrà trattata come "anonima" e potrebbe generare il non luogo a procedere ove il nominativo del segnalante risulti indispensabile.

Tipologia di dati trattati, misure di sicurezza, periodo di conservazione degli stessi

Il trattamento prevede al momento una gestione con modalità cartacee. Ove il segnalante non sia anonimo, la gestione di dati personali comuni di contatto del segnalante riconducibili principalmente al nominativo, dati di contatto, ruolo e posizione lavorativa. Oltre tali dati verranno gestite le informazioni di natura personale eventualmente facenti parte della segnalazione o allegate alla stessa e conferiti dal segnalante. Detti dati verranno conservati non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione o di definizione dei procedimenti avviati a seguito della segnalazione o, in caso di contestazioni, per il termine prescrizionale previsto dalla normativa vigente.
Ai sensi del decreto *whistleblowing*, i dati personali trasmessi dal segnalante che non siano utili alla elaborazione della segnalazione saranno oggetto di immediata cancellazione. Allo stesso modo non verranno conservate informazioni di tipo elettronico riconducibili a indirizzi IP, cookies e quant'altro atto a individuare uno specifico soggetto segnalante mediante analisi dei tracciati di accesso.
I dati raccolti in forma cartacea verranno conservati in schedari con modalità riservate di accesso strettamente riservate ai soggetti deputati alla loro gestione. Eventuali comunicazioni elettroniche contenenti dati personali del segnalante o della pratica verranno gestiti mediante i più avanzati sistemi di

sicurezza, ivi incluse tecniche crittografiche di tenuta e di comunicazione dati nonché di limitazione di accesso agli stessi, tendenti a contenere i rischi di perdita di riservatezza, integrità e disponibilità degli stessi e ispirate alle indicazioni "best practice" dell'art. 32 del GDPR, delle norme ISO27001 e linee guida ENISA.

Diffusione e comunicazione dei dati

Il trattamento non prevede in nessuna circostanza attività di diffusione o comunicazione indiscriminata dei dati raccolti.
I soggetti che possono avere accesso ai dati del segnalante, ove esso risulti non anonimo e in assenza di consenso ad una maggiore divulgazione del segnalante, sono riconducibili unicamente ai soggetti interni espressamente preposti alla gestione del trattamento e, ove imposto da regolamenti o normativa comunitaria, alle Autorità di vigilanza e ordine pubblico. Queste ultime tratteranno le informazioni in qualità di titolari autonomi.
A detti soggetti, limitatamente ai dati oggetto della segnalazione, potranno aggiungersi in qualità di designati o incaricati soggetti aziendali deputati al controllo societario, ai soggetti interni o esterni deputati all'esecuzione dei provvedimenti legati alla pratica di segnalazione o all'assistenza legale e, in qualità di Titolari autonomi, Autorità di Vigilanza e Ordine Pubblico e, ove nominato, all'Organismo di Vigilanza ai sensi del d.lgs. 231/01.
Infine, limitatamente alle sole attività tecniche legate alla manutenzione degli strumenti software eventualmente resi disponibili al segnalante dalla Società, i dati potranno essere acceduti da personale esterno specificatamente incaricato e impegnato alla riservatezza.

Profilazione

Il trattamento non prevede attività di profilazione così come definita dall'art. 4 punto 4 del GDPR riportata nel seguito: " *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

Trasferimento dati in Paesi terzi

Il trattamento e la conservazione dei dati saranno effettuati in Italia o in Paesi facenti parte dell'Unione Europea. Ove risultasse necessario il loro trasferimento presso altri Paesi, esso potrà avvenire se verranno soddisfatte le condizioni previste allo scopo dalla normativa vigente per il trasferimento dati verso Paesi extra UE stabilite dagli apparati legislativi e dall'Autorità Garante.

Diritti dell'interessato segnalante e condizioni di limitazione degli stessi

L'interessato segnalante, in relazione alle finalità previste, può contattare i soggetti coinvolti sopracitati ed esercitare i diritti a lui riconosciuti dalla normativa vigente. L'interessato ha altresì il diritto di proporre reclamo direttamente all'Autorità Garante per la protezione dei dati personali, o all'Autorità Nazionale Anticorruzione (ANAC) nei termini previsti dalla normativa vigente rilevabili dal sito/contatti delle stesse.
Ai sensi dell'art. 13.3 del decreto *whistleblowing* e dell'art. 2-*undecies* del d.lgs. 196/03, il legislatore ha previsto l'imposizione di una serie di limitazioni all'esercizio dei diritti previsti dal GDPR in funzione dei quali la Società potrà valutare di non ottemperare all'esercizio dei diritti qualora dall'esercizio degli stessi possano derivare pregiudizi effettivi e concreti ad una serie di ambiti (indicati dall'art. 2-*undecies* del d.lgs.

196/2003 a cui si rimanda per maggiore dettaglio) giudicati dal legislatore come meritevoli di particolari forme di tutela. Resta inteso che in tal caso all'interessato verrà inoltrata specifica comunicazione.

Dichiarazioni del segnalante

ATTENZIONE: Qualora il segnalante intenda mantenere l'anonimato, può omettere l'inserimento del presente modello nella busta chiusa da inviare al responsabile dei sistemi di segnalazione interna.

MODELLO PER LA SEGNALAZIONE DELLE VIOLAZIONI: dati identificativi del segnalante	
NOME E COGNOME DEL SEGNALANTE	
INQUADRAMENTO E QUALIFICA PROFESSIONALE	
SEDE DI LAVORO	
TELEFONO/CELLULARE	
E-MAIL	

- Il sottoscritto _____ dichiara l'assenza di qualsiasi interesse privato collegato alla segnalazione.

Oppure

- Il sottoscritto _____ dichiara la sussistenza di un interesse privato collegato alla dichiarazione, di seguito evidenziata *(Descrizione dell'interesse)*

  _____

  _____

- Il sottoscritto:

  ☐ autorizza

  ☐ non autorizza

  la divulgazione dei propri dati personali a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni ai sensi dell'art. 12, comma 2, d.lgs. n. 24/2023, incluse l'autorità disciplinare e il segnalato nei casi previsti dall'art. 12, comma 5, d.lgs. n. 24/2023.

- Il sottoscritto dichiara di aver preso visione dell'informativa *privacy* al segnalante sulla gestione del trattamento di *whistleblowing*.

Luogo, data Firma

Allegato 1B: Modello di segnalazione: oggetto della segnalazione

MODELLO PER LA SEGNALAZIONE DELLE VIOLAZIONI: oggetto della segnalazione	
DATA/PERIODO IN CUI SI È VERIFICATO IL FATTO	
LUOGO FISICO IN CUI SI È VERIFICATO IL FATTO	☐ UFFICIO (Indicare denominazione e indirizzo della struttura) _____ ☐ ALL'ESTERNO DELL'UFFICIO (Indicare luogo e indirizzo) _____
COMPLETA DESCRIZIONE DEGLI ATTI O DEI FATTI	
PRESUNTO/I AUTORE/I DEGLI ATTI O DEI FATTI	
PRESUNTI ALTRI EVENTUALI SOGGETTI A CONOSCENZA DEGLI ATTI O DEI FATTI E/O IN GRADO DI RIFERIRE SUL MEDESIMO	
EVENTUALI ULTERIORI INFORMAZIONI UTILI AI FINI DELLA SUSSISTENZA DEI FATTI/ATTI SEGNALATI	
EVENTUALI ALLEGATI A SOSTEGNO DELLA SEGNALAZIONE	

Allegato 2: Informativa *Privacy* al segnalato

Informativa *Privacy* al segnalato sulla gestione del trattamento di *whistleblowing* (ai sensi del Regolamento UE 2016/679 - c.d. GDPR)

La presente informativa viene resa ai sensi del GDPR per illustrare le regole adottate da Euregio Plus SGR S.p.A. (la "Società" nel seguito) per la tutela dei dati nell'ambito del trattamento di gestione del *whistleblowing* di cui al d.lgs. 24/2023 ("decreto *whistleblowing*" nel seguito).

Titolarità e contatti

La titolarità del trattamento è in capo alla Società. Per ogni informazione, per contattare titolare, responsabile del trattamento, responsabile della protezione dati (c.d. DPO) nonché per l'esercizio dei diritti riconosciuti dalla normativa vigente l'interessato potrà rivolgersi, in alternativa:

- all'indirizzo di posta elettronica info@euregioplus.com;
- alla sede della Società, mediante RR, all'indirizzo Passaggio Duomo, 15, 39100, Bolzano, all'att.ne del servizio di presidio *privacy*.

Finalità, base giuridica, condizione di liceità del trattamento

Il trattamento ha come finalità informare il segnalato per il quale è stata avviato specifico procedimento istruttorio sulla gestione dei dati personali attinenti il segnalato stesso.
Il trattamento viene svolto con condizione di liceità dovuta ad "obbligo legale del titolare" ed è motivato dalle indicazioni giuridiche provenienti dal GDPR e d.lgs. 196/03 nonché dal citato decreto *whistleblowing*.

Tipologia di dati trattati, misure di sicurezza, periodo di conservazione degli stessi

Il trattamento prevede la gestione di dati personali raccolti a seguito della segnalazione pervenuta alla Società riconducibili principalmente al nominativo, fatti segnalati.
Detti dati verranno conservati non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione o di definizione dei procedimenti avviati a seguito della segnalazione o, in caso di contestazioni, per il termine prescrizionale previsto dalla normativa vigente.
Si precisa che ai sensi del decreto *whistleblowing*, i dati personali trasmessi dal segnalante che non siano utili alla elaborazione della segnalazione saranno oggetto di immediata cancellazione.
I dati raccolti in forma cartacea verranno conservati in schedari con modalità riservate di accesso strettamente riservate ai soggetti deputati alla loro gestione. Eventuali comunicazioni elettroniche contenenti dati personali del segnalante o della pratica verranno gestiti mediante i più avanzati sistemi di sicurezza, ivi incluse tecniche crittografiche di tenuta e di comunicazione dati nonché di limitazione di accesso agli stessi, tendenti a contenere i rischi di perdita di riservatezza, integrità e disponibilità degli stessi e ispirate alle indicazioni "best practice" dell'art. 32 del GDPR, delle norme ISO27001 e linee guida ENISA.

Diffusione e comunicazione dei dati

Il trattamento non prevede in nessuna circostanza attività di diffusione o comunicazione indiscriminata dei dati raccolti.
I soggetti che possono avere accesso ai dati sono riconducibili unicamente ai soggetti interni espressamente preposti alla gestione del trattamento e, ove imposto da regolamenti o normativa

comunitaria, alle Autorità di vigilanza e ordine pubblico. Queste ultime tratteranno le informazioni in qualità di titolari autonomi.
A detti soggetti potranno aggiungersi in qualità di designati o incaricati soggetti aziendali deputati al controllo societario, ai soggetti interni o esterni deputati all'esecuzione dei provvedimenti legati alla pratica di segnalazione o all'assistenza legale e, in qualità di Titolari autonomi, Autorità di Vigilanza e Ordine Pubblico e, ove nominato, all'Organismo di Vigilanza ai sensi del d.lgs. 231/01.
Infine, limitatamente alle sole attività tecniche legate alla manutenzione degli strumenti software eventualmente resi disponibili al segnalante dalla Società, i dati potranno essere acceduti da personale esterno specificatamente incaricato e impegnato alla riservatezza.

Profilazione

Il trattamento non prevede attività di profilazione così come definita dall'art. 4 punto 4 del GDPR riportata nel seguito: " qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

Trasferimento dati in Paesi terzi

Il trattamento e la conservazione dei dati saranno effettuati in Italia o in Paesi facenti parte dell'Unione Europea. Ove risultasse necessario il loro trasferimento presso altri Paesi, esso potrà avvenire se verranno soddisfatte le condizioni previste allo scopo dalla normativa vigente per il trasferimento dati verso Paesi extra UE stabilite dagli apparati legislativi e dall'Autorità Garante.

Diritti dell'interessato segnalato e condizioni di limitazione degli stessi

L'interessato segnalato, in relazione alle finalità previste, può contattare i soggetti coinvolti sopracitati ed esercitare i diritti a lui riconosciuti dalla normativa vigente. L'interessato ha altresì il diritto di proporre reclamo direttamente all'Autorità Garante per la protezione dei dati personali, o all'Autorità Nazionale Anticorruzione (ANAC) nei termini previsti dalla normativa vigente rilevabili dal sito/contatti delle stesse.
Ai sensi dell'art. 13.3 del decreto *whistleblowing* e dell'art. 2-*undecies* del d.lgs. 196/03, il legislatore ha previsto l'imposizione di una serie di limitazioni all'esercizio dei diritti previsti dal GDPR in funzione dei quali la Società potrà valutare di non ottemperare all'esercizio dei diritti qualora dall'esercizio degli stessi possano derivare pregiudizi effettivi e concreti ad una serie di ambiti (indicati dall'art. 2-*undecies* del d.lgs. 196/2003 a cui si rimanda per maggiore dettaglio) giudicati dal legislatore come meritevoli di particolari forme di tutela. Resta inteso che in tal caso all'interessato verrà inoltrata specifica comunicazione.