

PROCEDURA
GESTIONE REPORTING ODV
E WHISTLEBLOWING



ai sensi del Decreto Legislativo 10 marzo 2023 n. 24

SOMMARIO:

1.	SCOPO E AMBITO DI APPLICAZIONE	3
2.	RIFERIMENTI	4
3.	DESTINATARI E OGGETTO DELLA SEGNALAZIONE	5
3.1.	Chi riceve le segnalazioni (“Soggetto ricevente”)	5
3.2.	Chi può segnalare (“ <i>whistleblower</i> ”)	5
3.3.	Cosa si può segnalare (oggetto della segnalazione)	6
3.4.	Esclusioni	7
3.5.	Canale alternativo	9
4.	DESCRIZIONE DEL PROCESSO	10
4.1.	Oggetto del reporting all’OdV	10
4.2.	La segnalazione di illeciti ex D. Lgs. 24/2023 (Decreto <i>Whistleblowing</i>)	11
4.2.1.	Tipologia di canali – Canale interno ed esterni	12
4.3.	Modalità di inoltro della segnalazione – Canale interno	13
4.4.	Modalità di accesso al sistema	14
4.5.	Misure a tutela dell’identità del segnalante	15
4.6.	Istruttoria	16
4.7.	Conservazione	17
4.8.	Relazione annuale	18
5.	INFORMAZIONE E FORMAZIONE	18

N° rev.	Data	Descrizione della modifica	Par. modificati
1	12/11/2021	Prima emissione	N/A
2	26/05/2022	Aggiunti alcuni riferimenti normativi e integrato marginalmente il processo di valutazione di una segnalazione	2.3
3	31/03/2023	Integrazione a seguito del Provvedimento del 23 dicembre 2022 emanato da Banca d’Italia che prevede il 1° aggiornamento recante modifiche al Regolamento d’attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis) del TUF.	2
4	15/12/2023	Integrazione a seguito dell’entrata in vigore del Decreto 24/2023 e istituzione dell’Organismo di Vigilanza.	Revisione integrale
5	23/02/2024	Introduzione dell’uso della piattaforma ISWEB per il canale alternativo, eliminazione del canale “analogico”. Espliciti richiami all’Allegato 4 del Regolamento Banca d’Italia del 5 dicembre 2019.	N/A

1. SCOPO E AMBITO DI APPLICAZIONE

Un adeguato sistema di reporting interno nei confronti dell'Organismo di Vigilanza (di seguito anche "OdV"), corroborato da un canale di ricezione delle segnalazioni (riservate o anonime) relative alla commissione di reati e/o al mancato rispetto del MOGC, gestito sempre dal medesimo Organismo, costituiscono uno strumento necessario per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello di Organizzazione, Gestione e Controllo, per l'eventuale accertamento delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto.

ACP (di seguito anche la "Società" o la "SGR"), attraverso la predisposizione di tale procedura si pone, dunque, l'obiettivo di disciplinare due distinti sistemi di controllo:

- i c.d. "flussi informativi 231", ossia le comunicazioni interne volte a dare evidenza delle attività a presidio del rischio di uno o più reati presupposto ex D. Lgs. 231/01 e le segnalazioni di anomalie e violazioni del Modello da effettuarsi nei confronti dell'OdV (v. **cap. 4.1.**).

Il sistema di reporting nei confronti dell'OdV si applica a tutti i processi e le procedure individuate nel Modello Organizzativo;

- le segnalazioni di illeciti tramite il sistema c.d. *whistleblowing*, ossia attraverso la messa disposizione di specifici canali atti a riceverle e gestirle, garantendo un sistema improntato alla tutela del soggetto che effettua la segnalazione (il "Segnalante") contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurandone inoltre la riservatezza circa l'identità e l'oggetto della segnalazione. La "persona segnalante" (o "whistleblower"), è, ai sensi dell'art. 2 del Decreto 24/2023, la "persona fisica che effettua la segnalazione o divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo" attraverso i canali messi a disposizione dalla Società.

La finalità della procedura di cui si è dotata ACP, risulta così quella di diffondere, coerentemente con i valori del proprio Codice Etico, nonché in aderenza al Decreto 24/2023, una cultura societaria improntata sul rispetto della legalità e dei valori etici a cui si ispira la SGR nella conduzione della propria attività aziendale.

2. RIFERIMENTI

- D. Lgs. 24 febbraio 1998 n. 58 (“TUF”), artt. 4-undecies e 4-duodecies, *aggiornato con le modifiche apportate dai D.lgs. 29, 30, 31 del 10 marzo 2023*;
- D. Lgs. 231/2001 – “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell’art. 11 della L. 29 settembre 2000 n. 300*” - e successivi aggiornamenti;
- D. Lgs. 30 giugno 2003, n. 196 e s.m.i. – “*Codice in materia di protezione dei dati personali*” (“Codice Privacy”);
- D. Lgs. 231/2007 e s.m.i. – “*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*”;
- Regolamento della Banca d’Italia del 5/12/2019 e s.m.i., di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis), del TUF (di seguito anche “Regolamento di Banca d’Italia”);
- Reg. (UE) 16 aprile 2014 n. 596 del Parlamento europeo e del Consiglio, relativo agli abusi di mercato;
- Legge 30 novembre 2017, 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*”;
- Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 “*Regolamento generale sulla protezione dei dati*” (“GDPR”);
- Provvedimento del 23 dicembre 2022 emanato da Banca d’Italia che prevede il 1° aggiornamento recante modifiche al Regolamento d’attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis) del TUF;
- D. Lgs. 24 del 10 marzo 2023 – “*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*” – c.d. “**Decreto Whistleblowing**”;
- Linee guida in materia di Whistleblowing: Delibera ANAC n. 311 del 12 luglio 2023;
- Modello di Organizzazione, Gestione e Controllo di ACP SGR S.p.A.;
- Codice Etico della Società.

3. DESTINATARI E OGGETTO DELLA SEGNALAZIONE

3.1. Chi riceve le segnalazioni (“Soggetto ricevente”)

L’OdV, per sua natura già dotato delle necessarie competenze richieste dal D. Lgs. 24/2023, è addetto all’applicazione - sia per quanto riguarda i flussi informativi 231 che per quanto concerne le segnalazioni di illeciti tramite il sistema di *whistleblowing* - di questa procedura e il Consiglio di Amministrazione ne è investito del controllo applicativo. L’OdV potrà avvalersi della collaborazione di altri soggetti, interni ed esterni all’Ente, nel rispetto delle tutele previste dal Decreto e della normativa sulla protezione dei dati personali.

Questa procedura attiene tanto alla comunicazione, da parte dei soggetti interni alla Società, di flussi informativi nei confronti dell’OdV per garantire la tracciabilità e la documentabilità dei processi aziendali, in coerenza con il MOGC 231, quanto alla possibilità di segnalare illeciti (c.d. *whistleblowing*) per i soggetti di seguito indicati, a prescindere dal fatto che siano effettivi Destinatari del MOGC 231 e anche se il rapporto è in fase di avvio o se è concluso.

3.2. Chi può segnalare (“whistleblower”)

Il Decreto 24/2023, rispetto alla normativa di settore¹, che limita la facoltà di effettuare segnalazioni ai soli dipendenti e circoscrivevano l’oggetto delle stesse a specifici illeciti afferenti alla singola normativa di riferimento, amplia il novero dei soggetti a cui è riservata la facoltà di effettuare la segnalazione di illeciti ravvisati nell’ambito del proprio contesto lavorativo, come di seguito indicati:

- dipendenti delle amministrazioni pubbliche e degli enti pubblici economici che abbiano contatti con la Società;
- lavoratori subordinati;
- lavoratori autonomi;
- liberi professionisti e consulenti;
- volontari e tirocinanti, retribuiti e non retribuiti;

¹ TUF, art.4-*duodecies* e art. 1, c. 1, lett. I-*ter*”

- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

Inoltre, l'art. 3, comma V, lettere a), b), c) e d) del D. Lgs. 24/2023 estende l'ambito soggettivo di applicazione delle tutele predisposte in favore del soggetto che effettua segnalazioni, denunce, divulgazioni pubbliche:

- al facilitatore, ossia colui che assiste il segnalante nel processo di segnalazione - in quanto operante all'interno del medesimo contesto lavorativo - e la cui assistenza deve essere mantenuta riservata;
- 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;
- 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;
- 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.

3.3. Cosa si può segnalare (oggetto della segnalazione)

Il Decreto prevede, in via generale, le seguenti ipotesi:

➔ Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente privato e che consistono in:

a) Violazioni di disposizioni normative nazionali:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del D.lgs. 231/01, in materia di responsabilità amministrativa dell'Ente (a titolo esemplificativo: indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche, frode nelle pubbliche forniture), o violazioni dei Modelli di Organizzazione, gestione e controllo ivi previsti.

b) Violazioni di disposizioni normative europee, 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 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 (a titolo esemplificativo: violazioni in materia di concorrenza e di aiuti di Stato);
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'UE.

➔ 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, nonché i fondati sospetti.

3.4. Esclusioni

In base all'art. 1, comma 2, le disposizioni del presente Decreto non si applicano:

- a) alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;

- b) alle segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea;
- c) alle 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.

N.B. In quest'ultimo caso (lett. c), il Decreto non trova applicazione esclusivamente in ragione del fatto che prevale la disciplina di settore e, nello specifico, il D. Lgs. 231/2007², in materia di **prevenzione del riciclaggio e del finanziamento del terrorismo**, il TUF³ e il Reg. (UE) 596/2014 in materia di **servizi, prodotti e mercati finanziari (“market abuse”)**, che già disciplinano l'istituzione di canali interni ed esterni di segnalazione.

Perciò, oltre ai casi tassativamente previsti dal Decreto 24/2023 (nei quali rientrano, come detto, anche le violazioni di disposizioni normative europee, in materia di mercati finanziari, antiriciclaggio e terrorismo), l'oggetto delle segnalazioni si estenderà inoltre a quelle condotte ascrivibili a violazioni delle suddette norme speciali (TUF, D. Lgs. 231/07 e Reg. Ue 596/2014), disciplinanti l'attività della SGR.

Posto che gran parte delle condotte illecite derivanti dal mancato rispetto delle normative di settore è già ricompresa nel novero dei reati 231 (es. art. 184 e 185 TUF), all'interno delle procedure e dei protocolli di prevenzione del Modello 231 ed inoltre nel perimetro di applicazione del Decreto 24/2023, si riportano di seguito, a mero titolo esemplificativo, alcune ipotesi di violazioni che possono costituire oggetto di segnalazione nell'ambito delle normative speciali:

- eventuali condotte che diano luogo a conflitti di interesse;
- illeciti nell'ambito della gestione dei fondi comuni di investimento o nell'erogazione dei servizi di investimento con l'intento di danneggiare gli investitori, i fondi gestiti o la stessa SGR;
- mancato rispetto delle procedure e dei protocolli interni in tema di informativa, trasparenza e protezione degli investitori;

² D.lgs. 231/2007 - Capo III - Obblighi di segnalazione;

³ D. Lgs. 24 febbraio 1998 n. 58 (“TUF”), artt. 4-undecies – “Sistemi interni di segnalazione delle violazioni” e 4-duodecies – “Procedura di segnalazione alle Autorità di Vigilanza”.

- illeciti riscontrati nella compilazione dei questionari di valutazione del profilo del cliente;
- illecita influenza da parte di un dipendente nella compilazione del questionario antiriciclaggio al fine di ridurne il profilo di rischio;
- omesso monitoraggio della clientela per avvantaggiare uno o più soggetti;
- omessa attivazione dei presidi antifrode da parte dei soggetti deputati;
- mancato rispetto degli obblighi di astensione previsti dalla normativa.

Non rientrano inoltre all'interno delle possibili segnalazioni quelle afferenti alla materia HR (es. molestie, bullismo, pari opportunità), che verranno gestite attraverso i canali tradizionali.

3.5. Canale alternativo

È previsto un canale di segnalazione alternativo qualora la segnalazione riguardi l'Organismo di Vigilanza nella sua totalità ovvero una persona tra i membri dell'Organismo di Vigilanza stesso.

In dettaglio il segnalante potrà rivolgersi al Presidente del Collegio Sindacale, tramite un canale informatico interno di segnalazione (la piattaforma "Segnalazione Illeciti - Whistleblowing").

Il canale è raggiungibile tramite il seguente sito/link: <https://segnalazioni.alternativecapital.partners/#/>
Per le modalità di accesso si rimanda al paragrafo 4.4 della presente procedura.

La piattaforma, attraverso apposito questionario, permetterà al segnalante di attivare il "canale alternativo" di segnalazione esplicitando, nella compilazione del questionario *online*, se la segnalazione riguardi l'Organismo di Vigilanza nella sua totalità ovvero una persona tra i membri dell'Organismo di Vigilanza stesso. In tal caso, tale segnalazione verrà automaticamente inoltrata all'utenza personale riservata del Presidente del Collegio Sindacale, il quale provvederà ad analizzare la segnalazione e gestire la stessa tramite la piattaforma, nel rispetto delle previsioni della presente procedura.

In caso contrario, la segnalazione verrà inoltrata automaticamente all'Organismo di Vigilanza, il quale provvederà ad analizzare la segnalazione e gestirla nel rispetto di quanto descritto al successivo paragrafo 4.3.

4. DESCRIZIONE DEL PROCESSO

4.1. Oggetto del reporting all'OdV

I flussi informativi indirizzati all'OdV mirano a tutelare l'integrità della Società e a migliorare le attività di pianificazione dei controlli da parte dell'Organismo medesimo e dovranno avere ad oggetto l'aggiornamento del Modello di organizzazione, gestione e controllo, la sua applicazione, la sua violazione, nonché l'adeguatezza dei principi del Codice Etico e delle procedure operative rispetto alle finalità cui essi sono preordinati.

Resta impregiudicato che l'OdV possa predisporre un'apposita matrice che disciplini i destinatari e l'oggetto dei flussi informativi periodici o ad evento che ritiene opportuno visionare.

In particolare, ogni Destinatario del Modello 231 deve poter tempestivamente trasmettere all'OdV flussi informativi concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti, che coinvolgano la Società;
- ogni violazione del Modello e dei suoi elementi costitutivi e ogni altro aspetto potenzialmente rilevante ai fini dell'applicazione del D. Lgs. n. 231/2001;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati di cui al Decreto.

I responsabili di funzione, come individuati nel documento Matrice indicativa delle attività a rischio di reato (c.d. "MIARR"), in base alla propria area di pertinenza, devono tempestivamente trasmettere all'OdV:

- i rapporti predisposti nell'ambito delle attività di controllo svolte, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto;
- i rapporti predisposti da ogni soggetto pubblico deputato al controllo o all'applicazione di normative regolatorie, di cui siano venuti in possesso;

- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, evidenzianti i procedimenti disciplinari svolti e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nei confronti dei dipendenti), oppure i provvedimenti motivati di archiviazione dei procedimenti disciplinari;
- i flussi informativi di cui all'Allegato 3 (tre) della Parte Generale del Modello di Organizzazione, Gestione e Controllo.

Il Consiglio di Amministrazione, eventualmente tramite il Consigliere Delegato, deve tempestivamente trasmettere all'OdV:

- ogni eventuale modifica e/o integrazione al sistema di deleghe e procure;
- verbale della riunione del riesame prevista dal Manuale del sistema di gestione qualità, se presente;
- report dei certificatori esterni in occasione degli audit di terza parte;
- relazione relativa agli eventuali infortuni sul luogo di lavoro;
- relazione sullo stato di attuazione del sistema di gestione;
- ogni eventuale emanazione, modifica e/o integrazione effettuata o ritenuta necessaria alle procedure ed al Codice Etico.

Tutte le comunicazioni nei confronti dell'OdV possono essere effettuate attraverso i seguenti canali informativi dedicati:

- E-mail all'indirizzo: odv@alternativecapital.partners
- Lettera indirizzata a Organismo di Vigilanza di ACP SGR S.p.A. – Corso Venezia 16, 20121 Milano (MI)

4.2. La segnalazione di illeciti ex D. Lgs. 24/2023 (Decreto *Whistleblowing*)

Oltre ai flussi informativi 231, di cui al paragrafo che precede, chiunque, nell'ambito del proprio contesto lavorativo, venga in possesso di notizie relative alla violazione di norme, come in precedenza esplicitato, può fare una segnalazione (intesa come informazione, compresi i fondati sospetti, su violazioni già

commesse nonché su condotte volte ad occultarle), o in forma scritta o in forma orale, nelle modalità di seguito riportate.

Preme inoltre sottolineare come non sia necessario che il *Whistleblower* disponga delle prove dell'illecito che intende segnalare, ma le segnalazioni dovranno essere il più possibile chiare e circostanziate, al fine di consentire la valutazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni.

4.2.1. Tipologia di canali – Canale interno ed esterni

Sono previsti 2 (due) diversi canali:

1. **Canale interno** all'Ente (v. 4.3.);
2. **Canale esterno**, che consente al personale degli intermediari (fra cui le SGR) di segnalare direttamente all'Autorità violazioni delle norme del TUF e delle norme UE direttamente applicabili di cui siano venuti a conoscenza durante lo svolgimento della propria attività lavorativa fornendo così un ulteriore strumento di controllo e supervisione utile ad intercettare qualunque comportamento posto in essere in violazione della normativa in materia di servizi d'investimento. In conformità all'art. 4-*duodecies* del TUF, la Consob ha attivato tre nuovi canali (i.e. telefonico, posta elettronica, posta cartacea) dedicati alla ricezione immediata, anche in forma anonima, da parte del personale dei soggetti vigilati (tra cui le SGR) di tali segnalazioni. Per maggiori informazioni cfr. <http://www.consob.it/web/area-pubblica/wistleblowing-ricezione-segnalazioni>

Un altro canale esterno è poi messo a disposizione da Banca d'Italia <https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html>

Da ultimo, per le segnalazioni che esulano dal perimetro delle materie speciali (e per cui è possibile utilizzare i 2 canali summenzionati) è possibile usufruire del canale esterno messo a disposizione dall'ANAC al seguenti link <https://www.anticorruzione.it/-/whistleblowing> (“accedi al servizio”)

Preme sottolineare come tale canale sia utilizzabile solo al ricorrere di determinate circostanze:

- a) se il canale interno risulta essere inattivo o non conforme ai requisiti normativi;
- b) se il *whistleblower* che ha effettuato una segnalazione tramite il canale interno non ricevuto risposta, spirati i termini normativamente previsti;

- c) se il soggetto abbia il fondato motivo di ritenere che il canale interno, anche in considerazione della tipologia di segnalazione, non offra tutte le garanzie previste dalla normativa;
- d) se il *whistleblower* ha fondato motivo di ritenere che la violazione che intende segnalare possa costituire un pericolo imminente o palese per il pubblico interesse.

4.3. Modalità di inoltro della segnalazione – Canale interno

Forma scritta:

a) Modalità digitale

A tutela del segnalante, le segnalazioni possono essere inviate tramite un canale informatico interno di segnalazione (la piattaforma “Segnalazione Illeciti - Whistleblowing”) la cui gestione è affidata all’OdV, ovvero, in alternativa, al Presidente del Collegio Sindacale per le eventuali segnalazioni che dovessero riguardare l’Organismo di Vigilanza.

Il canale è raggiungibile tramite il seguente sito/link: <https://segnalazioni.alternativecapital.partners/#/>

In merito alla possibilità di realizzare una segnalazione anche in **forma orale** può farsi riferimento alla funzione, prevista dal software succitato, di distorsione della voce per rendere non riconoscibile il soggetto da cui la segnalazione perviene.

La Società si impegna ad effettuare annualmente – ad opera di personale interno o all’uopo incaricato - una formazione specifica riferibile alle modalità di utilizzo della piattaforma “Segnalazione Illeciti - Whistleblowing”, così da garantire che eventuali nuovi dipendenti e collaboratori siano posti nella condizione di poter utilizzare, in tutte le sue potenzialità, il mezzo messo loro a disposizione.

Forma orale:

In merito alla possibilità di realizzare una segnalazione anche in forma orale, si prevede la facoltà per il segnalante e l’obbligo per l’OdV di ricevere, mediante apposito incontro, la segnalazione orale e di verbalizzarla, sottoponendo il verbale al segnalante prima della sua formalizzazione, per sua sottoscrizione.

L'OdV potrà avvalersi della collaborazione di altri soggetti, appositamente autorizzati, interni ed esterni all'Ente, nel rispetto delle tutele previste dal Decreto 24/2023 e della normativa sulla protezione dei dati personali.

Le segnalazioni **anonime** o **inammissibili** saranno gestite come segnalazioni generiche, senza le tutele del Decreto, se consentiranno comunque di accertare i fatti. In ogni caso, la segnalazione anonima, per essere presa in considerazione dal soggetto ricevente, dovrà essere il più possibile precisa e circostanziata di elementi che rendano possibile la comprensione della fattispecie e il conseguente avvio di una indagine. Se successivamente venisse identificato il segnalante di una segnalazione anonima, verranno ripristinate le tutele del Decreto.

Per entrambe le modalità, si sottolinea come sussista l'obbligo per il soggetto segnalante di dichiarare se vanta un interesse privato collegato alla segnalazione e sia inoltre previsto un trattamento privilegiato per il segnalante nel caso in cui lo stesso sia corresponsabile delle violazioni oggetto di segnalazione.

4.4. Modalità di accesso al sistema

Il Segnalante può accedere al sistema in:

- Modalità Riservata: la riservatezza si concretizza nella protezione delle informazioni anche attraverso strumenti di crittografia, come richiesto dalla norma. Il segnalante non deve mai registrarsi per sottoporre una segnalazione - per non far venir meno la caratteristica di "spersonalizzazione" garantita dalla piattaforma - ma può procedere senza l'utilizzo di credenziali e, al termine della segnalazione, la piattaforma rilascia al *whistleblower* un codice di 16 (sedici) numeri, generato in maniera automatica dal sistema, per permettergli di tornare nella sua area personale, ancora una volta in maniera totalmente spersonalizzata. Qualora il segnalante voglia fornire le proprie generalità, queste saranno gestite dalla piattaforma in maniera disaccoppiata rispetto alle risposte al questionario; si tratta di una separazione di tipo logico-applicativo con lo scopo di evitare che un eventuale intruso possa accedere contemporaneamente a identità del segnalante e contenuto della segnalazione;
- Modalità Anonima: il segnalante effettua una segnalazione in modalità anonima semplicemente evitando di fornire le sue generalità, nella sezione in cui queste sono richieste. Il sistema, ad ogni modo, permetterà

al segnalante di rivelare la propria identità in un secondo momento, al fine di permettergli di godere delle tutele previste dal *whistleblowing*.

4.5. Misure a tutela dell'identità del segnalante

Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi del codice penale o dell'art. 2043 c.c. e delle ipotesi in cui la riservatezza non è opponibile per legge (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del *whistleblower* viene protetta in ogni contesto successivo alla segnalazione.

Pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata senza il suo espresso consenso e coloro che ricevono o che sono coinvolti nella gestione della segnalazione sono tenuti alla tutela della riservatezza di tale informazione. La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

Qualora la contestazione disciplinare rivolta al segnalato sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

Si precisa che se l'OdV, a seguito della segnalazione, richieda al segnalante, entro un congruo termine, delucidazioni o integrazioni che siano strettamente necessarie al compimento della sua istruttoria, l'istanza sarà archiviata qualora il segnalante medesimo non ottemperi a tale richiesta entro il termine stabilito.

L'OdV, al contrario, rilascerà al segnalante l'avviso di ricevimento della segnalazione entro 7 (sette) giorni dalla presentazione della medesima e fornirà riscontri al segnalante circa le attività compiute quanto prima e comunque non oltre il termine massimo di 3 (tre) mesi, salvo che la segnalazione comporti accertamenti di particolare difficoltà.

L'OdV, inoltre, agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza della loro identità, fatti salvi gli obblighi

di legge e la tutela dei diritti della Società o delle persone coinvolte, nonché la reputazione della/e persona/e segnalata/e.

Ad integrazione di quanto sopra esposto per i dettagli circa le misure di protezione in capo al segnalante, si rimanda al Capo III del **Decreto Whistleblowing**.

In particolare, sono:

- vietati atti di ritorsione o discriminatori, diretti o indiretti nei confronti del segnalante, per motivi collegati, direttamente o indirettamente, alla segnalazione. Sono nulli il licenziamento ritorsivo e le misure organizzative aventi effetti negativi diretti o indiretti sulle condizioni di lavoro, se non sia dimostrato che non abbiano natura ritorsiva e che si fondino su ragioni estranee alla segnalazione;
- l'adozione di misure discriminatorie può essere denunciata all'Ispettorato nazionale del lavoro.

La tutela del segnalante si applica anche qualora la segnalazione o la divulgazione pubblica sia avvenuta quando il rapporto giuridico non è ancora iniziato oppure successivamente allo scioglimento dello stesso. Beneficiano delle predette tutele anche i facilitatori e i soggetti operanti nel medesimo contesto lavorativo che hanno un rapporto abituale o di parentela con il segnalante.

4.6. Istruttoria

- **Esame preliminare:** ricevuta la segnalazione, l'OdV verifica la **procedibilità** della stessa, ossia la sussistenza dei presupposti soggettivi ed oggettivi. Se procedibile, verifica l'**ammissibilità** della stessa, mediante controllo di:
 - corretta descrizione delle circostanze di tempo e luogo;
 - fondatezza della segnalazione, da evincere anche mediante la documentazione eventualmente allegata.

Se la segnalazione fosse improcedibile o inammissibile, l'OdV dovrà procedere all'archiviazione senza ulteriori analisi, dandone motivazione al segnalante.

- **Accertamento della segnalazione:** se la segnalazione risulta procedibile e ammissibile, l'OdV effettua l'istruttoria interna per verificarne la veridicità e potrà:
 - archivarla, se infondata;

- ritenuta fondata e darne comunicazione ai soggetti interni o esterni che dovranno adottare gli atti conseguenti.

Nel caso in cui - successivamente agli approfondimenti istruttori svolti - venga riscontrata una violazione, l'OdV o il Presidente del Collegio Sindacale, rispettivamente per le proprie competenze, riferiscono direttamente e senza indugio, alla prima occasione utile, agli organi aziendali le informazioni oggetto di segnalazione, anche al fine di individuare ed applicare le misure più adeguate, in conformità con quanto previsto all'interno del Sistema sanzionatorio, tempo per tempo in vigore presso la Società e di informare le Autorità qualora vi sia un obbligo giuridico in tal senso. Parimenti, gli stessi riferiscono agli organi aziendali anche quando richiesto dal segnalante.

Resta inteso che qualora la segnalazione riguardi una o più persone del Consiglio di Amministrazione o del Collegio Sindacale, gli stessi non saranno destinatari della suddetta informativa.

In entrambe le ipotesi, sia di archiviazione della segnalazione che di gestione della stessa, al termine del procedimento, il segnalante viene informato della chiusura del procedimento stesso.

Degli esiti dell'istruttoria, l'OdV darà notizia al segnalante per il tramite della piattaforma nel caso in cui la segnalazione sia pervenuta tramite detto canale, in alternativa, nel caso di segnalazione in forma orale, con una comunicazione scritta trasmessa a mezzo mail all'indirizzo indicato dal segnalante nel corso dell'incontro avanti l'OdV.

4.7. Conservazione

Le segnalazioni vengono conservate nella apposita piattaforma digitale cui non hanno accesso altri soggetti oppure, laddove trasmesse in modalità differenti rispetto a quella offerta dalla summenzionata piattaforma digitale, in apposito archivio analogico ad accesso controllato e consentito unicamente all'OdV.

Inoltre, nel rispetto del principio della minimizzazione dei dati di cui al Reg. Ue 679/2016 ("GDPR"), le segnalazioni saranno conservate per un periodo massimo di 5 anni, salvo che sia necessario un periodo di tempo superiore per far valere un diritto in sede giudiziaria.

4.8. Relazione annuale

L'OdV ovvero il Presidente del Collegio Sindacale, laddove la segnalazione abbia riguardato l'OdV stesso, relazionano annualmente in CdA in merito al corretto funzionamento dei sistemi interni di segnalazione, specificando le informazioni aggregate sulle risultanze delle attività svolte a seguito delle segnalazioni ricevute (a titolo esemplificativo, la relazione riferirà quante segnalazioni sono pervenute nell'anno, quante archiviate perché non ammissibili e/o infondate; etc.). La relazione è approvata dal CdA e messa a disposizione del personale.

5. INFORMAZIONE E FORMAZIONE

La Società si impegna ad effettuare annualmente - ad opera di personale interno o esterno incaricato - una formazione specifica riferibile alle modalità di utilizzo della piattaforma "Segnalazione Illeciti - Whistleblowing", così da garantire che eventuali nuovi dipendenti e collaboratori siano posti nella condizione di poter utilizzare, in tutte le sue potenzialità, il mezzo messo loro a disposizione.

Si impegna, inoltre, ad eseguire formazione continua sul sistema di segnalazione, anche in vista di eventuali aggiornamenti normativi o procedurali. In conformità all'Allegato 4 del Regolamento Banca d'Italia, sono illustrati al personale in maniera chiara, precisa e completa il procedimento di segnalazione interno, i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione

In particolare, la Società fornirà:

- attraverso l'affissione in bacheca e la pubblicazione nel sito web, documenti informativi chiari al segnalante e, comunque, a tutti i soggetti coinvolti, circa i canali di segnalazione, le procedure da seguire e i presupposti per fare le segnalazioni;
- documenti informativi chiari sulle tutele previste per i soggetti tutelati;
- informazioni sul sistema sanzionatorio, sia in caso di illecito utilizzo delle segnalazioni, sia in caso di ritorsioni nei confronti dei soggetti tutelati;
- una costante attività formativa in materia di trattamento dei dati personali.