

WHISTLEBLOWING – IL SISTEMA INTERNO DI SEGNALAZIONE DELLE VIOLAZIONI

Prima versione approvata dal Consiglio d'Amministrazione in data 26/03/2020
Aggiornamento del 30/10/2023

Indice

Riferimenti normativi e disposizioni interne	3
- Regolamento (UE) del 16 aprile 2014 n. 596 del Parlamento europeo e del Consiglio, relativo agli abusi di mercato (“ Regolamento MAR ”);	3
Acronimi	3
1. CONTENUTO	5
1.1 Ambito di applicazione	5
1.2 Soggetti segnalanti	5
1.3 Responsabili dei sistemi interni di segnalazione	6
1.3.1 <i>Responsabile Whistleblowing primario</i>	6
1.3.2 <i>Responsabile Whistleblowing alternativo</i>	6
1.4. Oggetto della segnalazione	7
1.5 Contenuto della segnalazione e modalità di inoltro	8
1.5.1 <i>Contenuto della segnalazione</i>	8
1.5.2 <i>Canali di segnalazione</i>	9
1.5.3 <i>Canale di segnalazione interna</i>	9
1.5.4 <i>Segnalazioni esterne all’Autorità di Vigilanza</i>	11
1.5.5 <i>Segnalazioni esterne all’ANAC</i>	12
1.5.6 <i>Divulgazione Pubblica</i>	13
1.6 Analisi e valutazione delle segnalazioni	13
1.7 Comunicazione agli organi aziendali	14
1.8 Comunicazione al soggetto Segnalante (per segnalazioni diverse da quelle in forma anonima)	15
1.9 Comunicazione al soggetto segnalato	15
1.10 Misure di tutela del soggetto Segnalante	16
1.11 Reporting	17
1.12 Conservazione e archiviazione	17
1.13 Formazione	17
1.14 Informativa a Banca d’Italia e Consob	17

Riferimenti normativi e disposizioni interne

- Regolamento (UE) del 16 aprile 2014 n. 596 del Parlamento europeo e del Consiglio, relativo agli abusi di mercato (“**Regolamento MAR**”);
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (“**Regolamento GDPR**”).
- D.Lgs. 8 giugno 2001, n. 231 e s.m.i. (“**Decreto 231**”), art. 6;
- D. Lgs. 30 giugno 2003, n. 196 e s.m.i. – “Codice in materia di protezione dei dati personali” (“**Codice GDPR**”);
- Legge 30 novembre 2017, n. 179, contenente le 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 (“**Legge WB**”);
- D.Lgs. 24 febbraio 1998 n. 58 (“**TUF**”), artt. 4-*undecies* e 4-*duodecies*;
- D.Lgs. 21 novembre 2007, n. 231 e s.m.i. (“**Decreto Antiriciclaggio**”), art. 48, Capo VII;
- Regolamento di attuazione degli articoli 4-*undecies* e 6, comma 1, lettere b) e c-bis) “Sistemi interni di segnalazione delle violazioni” e 4-*duodecies* “Procedure di segnalazione alle Autorità di Vigilanza” del TUF, artt. 39, 9 e Allegato 4;
- Modello di Organizzazione, Gestione e Controllo - Parte Generale Paragrafo 7;
- Regolamento Banca d'Italia del 5 dicembre 2019 “Regolamento di attuazione degli articoli 4-*undecies* e 6, comma 1, lettere b) e c-bis) del TUF”;
- D.Lgs. 10 marzo 2023 n. 24 – “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 (“**Decreto**”).

Acronimi

SOCIETÀ O SGR	AcomeA SGR S.p.A.
AD	Amministratore Delegato
CDA	Consiglio di Amministrazione
CS	Collegio Sindacale
RWP	Responsabile Whistleblowing Primario
RWA	Responsabile Whistleblowing Alternativo
ODV	Organismo di Vigilanza

Scopo

La presente *policy* unitamente al Modello di Organizzazione, Gestione e Controllo definiscono, in ottemperanza al dettato normativo, i canali di comunicazione adeguati per la ricezione, l’analisi e la gestione delle segnalazioni delle violazioni della normativa disciplinante l’attività svolta, garantendo la riservatezza dei dati personali del soggetto che effettua la segnalazione (il “Segnalante”) e l’adeguata tutela di quest’ultimo.

Infatti, con il termine “**whistleblowing**” si indica un sistema attraverso il quale un soggetto (il “Segnalante”), venuto a conoscenza di atti o fatti illeciti nell’ambito dello svolgimento della propria attività lavorativa, possa denunciare gli avvenimenti di cui sia venuto a conoscenza e possa farlo attraverso appositi canali interni previsti all’interno di tale procedura, senza timore di eventuali condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione.

Resta fermo che le segnalazioni aventi ad oggetto l’avvenuta o presunta violazione delle procedure e/o delle prescrizioni del Modello, ovvero la commissione o ragionevole pericolo di commissione dei reati di cui al Decreto,

seguono l'iter previsto al paragrafo 7 "whistleblowing" parte generale del Modello di Organizzazione, Gestione e Controllo.

Il presente documento contribuisce a diffondere la cultura della legalità e a mettere il personale nelle condizioni di svolgere il proprio lavoro in un ambiente sicuro e dotato dei dovuti presidi di sicurezza.

Il sistema è strutturato al fine di permettere la trasmissione di segnalazioni in forma anonima ove prevista dalla normativa vigente.

1. CONTENUTO

1.1 Ambito di applicazione

Il Decreto Legislativo n.24 del 2023, in attuazione della Direttiva (UE) 2019/1937, abroga la disciplina nazionale previgente in materia di whistleblowing e racchiude in un unico testo normativo – per il settore pubblico e per il settore privato – il regime di protezione dei soggetti che segnalano condotte illecite di cui siano venuti a conoscenza in un contesto lavorativo. Il fine è quello di incentivare le segnalazioni di illeciti che pregiudichino l'interesse pubblico o l'integrità dell'ente.

Tuttavia, il Decreto non trova applicazione *tout court*; infatti, lo stesso esclude le segnalazioni delle violazioni che risultino già disciplinate in via obbligatoria *i)* dagli atti dell'unione europea o nazionali, indicati nella parte II dell'allegato al decreto stesso, *ii)* dagli atti 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. Nei succitati casi prevarrà la disciplina di settore.

Per quanto applicabile alla SGR, in materia di:

- antiriciclaggio troveranno applicazione il D. Lgs. 231/2007 e s.m.i. (in particolare, il D.lgs. 90/2017 che, al Capo VII, ne ha introdotto l'art 48 in materia di sistemi interni di segnalazione delle violazioni) e le direttive (UE) 847/17 e 849/17;
- servizi finanziari troveranno applicazione il D. Lgs 58/98 ed il Regolamento (UE) 596/2014 sugli abusi di mercato.

Escludendo dal proprio perimetro applicativo tutte quelle segnalazioni di violazioni che sono già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali riguardanti servizi, prodotti e mercati finanziari e prevenzione del riciclaggio del finanziamento del terrorismo, il Decreto lascia ferma l'applicazione rispettivamente degli articoli 4-undecies e 4-duodecies del TUF in ambito finanziario. Tali disposizioni contemplano, oltre a specifici canali di comunicazione interni, anche un canale esterno, avente come destinatario la Banca d'Italia o la Consob, a seconda del reparto di vigilanza.

Pertanto, la segnalazione di presunte violazioni all'interno della SGR può avvenire sulla base di due distinti presupposti normativi:

- il **decreto n. 24/2023 di recepimento della Direttiva 2019/1937** qualora la segnalazione abbia ad oggetto violazioni delle disposizioni normative coperte dal Decreto stesso ed applicabili alla SGR. L'ambito di applicazione oggettivo del Decreto è contenuto all'art.2 dello stesso; per quanto rilevante per le attività della SGR, tale ambito comprende i prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo.
- le **norme speciali** sopra richiamate qualora la segnalazione abbia ad oggetto violazioni di disposizioni normative disciplinate specificamente da queste (per quanto applicabile alla SGR: disposizioni del TUF e antiriciclaggio).

In ragione del fatto che le segnalazioni di violazioni siano effettuate ai sensi delle previsioni contenute nel Decreto ovvero nella disciplina speciale, occorre tenere conto delle peculiarità in prosieguo evidenziate.

1.2 Soggetti segnalanti

La normativa di settore, all'art.4-duodecies TUF, individua l'informatore come una persona appartenente al personale dei soggetti indicati dall'articolo 4-undecies (soggetti vigilati) che riferiscono di violazioni delle norme di settore disciplinanti l'attività da questi svolta, nonché del Regolamento (UE) n. 596/2014.L'art. 1, c. 1, lett. I-ter,

TUF, poi, definisce genericamente il “personale” come “*i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l’inserimento nell’organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato*”¹.

La disciplina generale, invece, amplia e specifica il novero dei soggetti che posso effettuare la segnalazione; infatti, l’articolo 2 del D. Lgs 231/2023 definisce la “persona segnalante” come “*la persona fisica che effettua la segnalazione o divulgazione pubblica di informazioni sulle violazioni acquisite nell’ambito del proprio contesto lavorativo*”.

Il successivo articolo 3 del Decreto dettaglia i soggetti che possono effettuare le segnalazioni e, in costanza di rapporto di lavoro o in ragione di un rapporto terminato, identifica i seguenti:

- a. lavoratori subordinati di soggetti del settore privato;
- b. lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
- c. collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- d. volontari e i tirocinanti, retribuiti e non retribuiti;
- e. azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.

1.3 Responsabili dei sistemi interni di segnalazione

1.3.1 Responsabile Whistleblowing primario

Il CdA, in linea con il principio di proporzionalità, ha individuato il Responsabile dell’ufficio *Compliance* quale “**Responsabile Whistleblowing primario**”, ovvero il soggetto responsabile dei sistemi interni di segnalazione delle violazioni, a cui è attribuito il compito di assicurare il corretto svolgimento della procedura.

In particolare, il **RWP**:

- presidia l’intero processo di segnalazione;
- riceve, analizza e valuta le segnalazioni provenienti dai canali di segnalazione (come descritti al § 1.5);
- trasmette in ogni caso e tempestivamente tutte le segnalazioni all’organismo di vigilanza al fine di prenderle in carico per le opportune valutazioni secondo quanto previsto nel Modello 231 adottato dalla SGR;
- decide riguardo all’archiviazione ovvero alla trasmissione alle fasi successive della segnalazione;
- informa, ove opportuno, il Segnalante se si è voluto palesare e qualora sia ritenuto necessario, il segnalato, sugli sviluppi del procedimento, fermo restando quanto previsto nei §§ 1.8 e 1.9;
- riferisce direttamente al **CdA** e al **CS** le informazioni oggetto di segnalazione, ove ritenute rilevanti; relaziona periodicamente al **CdA**, al **CS** e, per quanto di competenza, all’**OdV**, in relazione all’attività svolta, fornendo indicazioni di sintesi circa le evidenze emergenti dal sistema interno di segnalazione, in conformità con quanto definito al §1.11 (“*Reporting*”).

1.3.2 Responsabile Whistleblowing alternativo

Al fine di assicurare canali alternativi a disposizione del Segnalante, il **CdA** individua il “**Responsabile Whistleblowing alternativo**” nel Consigliere indipendente Ivonne Forno.

Tale soggetto sostituisce il Responsabile primario esclusivamente nei casi in cui il **RWP**:

- coincida con il soggetto segnalato o comunque sia implicato nei fatti;

¹ L’art. 1 D. Lgs 231/2007 riprende la medesima definizione.

- sia responsabile diretto (gerarchicamente o funzionalmente) del soggetto segnalato o, comunque abbia un potenziale interesse correlato alla segnalazione, tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

La segnalazione viene altresì inoltrata dal Segnalante al **RWA** nell'ipotesi di negligenza o eccessivo ritardo nella risposta da parte del **RWP**.

Nei predetti casi, il **RWA**, autonomo ed indipendente rispetto al **RWP**, svolge tutte le fasi del processo assegnate a quest'ultimo secondo le regole ordinarie.

Ove il **RWA** riceva una segnalazione non rientrante nelle ipotesi di cui sopra, la rimette al **RWP**, dandone comunicazione al Segnalante.

Ove la segnalazione venga rivolta al **RWP**, lo stesso, ove ritenga di avere un potenziale interesse nella segnalazione, la rimette al **RWA**, dandone comunicazione al Segnalante.

Il **RWA** contribuisce, per quanto di competenza, alla predisposizione della relazione annuale sul corretto funzionamento della procedura di *whistleblowing* e sulla corretta tenuta del sistema interno di segnalazione.

1.4. Oggetto della segnalazione

Il Decreto, in via generale, prevede che possono essere oggetto di segnalazione le informazioni sulle violazioni di normative nazionali e dell'Unione Europea. In particolare, in via esemplificativa, possono indicarsi:

- violazioni del diritto nazionale, illeciti civili, amministrativi, penali e contabili;
- condotte illecite, violazione dei modelli di organizzazione e gestione previsti nel D.Lgs. 231/2001;
- violazioni del diritto dell'Unione Europea;
- illeciti commessi in violazione della normativa dell'Unione indicata all'allegato I del Decreto;
- atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Sono ricomprese le violazioni delle norme dell'Unione in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto e la finalità della normativa applicabile in materia di imposta sulle società (art. 2, co.1, lett. a) n.5);
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni delle disposizioni dell'Unione Europea.

Nella disciplina speciale non esiste una lista tassativa ed esaustiva di reati o irregolarità che possono costituire oggetto di segnalazione di violazioni. Sono tuttavia considerate rilevanti, come indicato dalla normativa, le segnalazioni che possono costituire una violazione delle norme disciplinanti l'attività della SGR² e pertanto, a titolo esemplificativo e non esaustivo, le condotte o omissioni verificatesi nello svolgimento dell'attività lavorativa che possano essere pregiudizievoli per la SGR o per i suoi dipendenti, quali:

- violazioni in materia di gestione dei fondi comuni al fine di danneggiare gli investitori, i fondi gestiti ovvero la SGR medesima;
- violazioni in materia di servizi di investimento al fine di danneggiare i clienti ovvero la SGR medesima;
- utilizzo improprio di informazioni privilegiate o comunque confidenziali acquisite nell'ambito dell'attività lavorativa;
- manipolazioni del mercato in violazione della normativa;
- falsificazione/occultamento/distruzione di registrazioni a contenuto finanziario, contabile e altre false rappresentazioni, soppressione e/o occultamento di informazioni finanziarie;
- omesse comunicazioni al soggetto incaricato della revisione legale dei conti;

² Cfr. art. 4-undecies del TUF.

- frode, furto e appropriazione indebita;
- pagamenti e liquidazioni non giustificati, in tutto o in parte;
- attività poste in essere in conflitto di interesse, violazioni della regolamentazione sul governo societario o sulle politiche di remunerazione;
- false comunicazioni e dichiarazioni fornite alla SGR nell'ambito della prestazione dell'attività lavorativa tali da compromettere il corretto svolgimento dei servizi forniti dalla SGR;
- violazioni alle disposizioni in materia di trasparenza e protezione degli investitori;
- accesso illegittimo ai sistemi informativi e/o illegittimo trattamento dati, anche tramite utilizzo di credenziali di altri colleghi;
- utilizzo inappropriato dei poteri e delle deleghe concesse;
- induzione della clientela a fornire dati e/o informazioni non corrette nell'ambito della profilatura Mifid;
- abuso di comportamenti legati al c.d. *misselling*, vale a dire la vendita o la distribuzione dei fondi gestiti in modo non corretto e trasparente;
- falsa sottoscrizione della documentazione contrattuale o di altri documenti rilevanti.

In materia di antiriciclaggio, si riportano di seguito alcune esemplificazioni di condotte che potrebbero costituire oggetto di segnalazione:

- compilazione del questionario di adeguata verifica della clientela ad opera di un dipendente, anziché del cliente, con informazioni che non rappresentano le effettive dichiarazioni fornite dal medesimo cliente;
- ricezione di denaro contante o titoli al portatore da parte della clientela;
- suggerimenti al cliente su come compilare il questionario antiriciclaggio al fine di ridurre artificialmente il profilo di rischio;
- mancata attivazione dell'iter di segnalazione di operazione sospetta in presenza di evidenti indici di anomalia;
- mancata o non corretta modalità del monitoraggio costante della clientela in violazione palese delle norme previste dalla SGR (violazioni volontarie ripetute e sistematiche per avvantaggiare un soggetto);
- violazione dell'obbligo di riservatezza nei confronti dell'interessato e/o comunicazione a terzi dell'avvenuta segnalazione di operazione sospetta;
- violazione dell'obbligo di riservatezza del soggetto segnalante nell'ambito di segnalazioni di operazioni sospette (SOS);
- mancata richiesta delle autorizzazioni previste per l'apertura di rapporti e/o esecuzione di operazioni;
- mancato rispetto degli obblighi di astensione previsti dalla normativa;
- esecuzione di istruzioni dei clienti oggetto di precedenti segnalazioni di operazioni sospette (SOS) con modalità tali da aggirare i previsti blocchi procedurali.

Resta fermo l'obbligo di segnalazioni riguardanti la commissione, o il ragionevole pericolo di commissione, di reati presupposto ai sensi del D. Lgs. 231/01 o di violazioni del Modello di organizzazione, gestione e controllo adottato dalla Società (Modello 231) rilevanti ai sensi della normativa in materia di responsabilità amministrativa degli enti in quanto seguono l'iter di segnalazione previsto al paragrafo 7 parte generale del Modello 231 adottato dalla Società.

1.5 Contenuto della segnalazione e modalità di inoltro

1.5.1 Contenuto della segnalazione

Per effettuare la segnalazione, non è necessario che il Segnalante disponga di prove della violazione; tuttavia, deve disporre di informazioni sufficientemente circostanziate che ne facciano ritenere ragionevole l'invio. Pertanto, nella segnalazione dovranno essere indicati i seguenti elementi:

- le generalità del Segnalante, con indicazione della posizione o funzione svolta nell'ambito della Società
- le modalità con le quali è venuto a conoscenza degli atti o fatti oggetto di segnalazione;

- una descrizione chiara e completa degli atti o fatti oggetto della segnalazione;
- se conosciute, le generalità, la qualifica e/o il ruolo che permettano di identificare il/i soggetto/i che avrebbe/avrebbero posto in essere i fatti oggetto della segnalazione;
- l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- le circostanze di luogo e di tempo in cui sono state commesse le violazioni oggetto di segnalazione, ove note;
- l'inoltro di eventuali documenti di qualsiasi genere (ivi inclusi foto, *screenshot*, etc.) che possano ulteriormente circoscrivere e/o confermare la fondatezza dei fatti segnalati;
- qualsiasi altra informazione o documento che possa fornire un utile riscontro circa la fondatezza dei fatti segnalati;
- dichiarazione del Segnalante in merito all'assenza o alla sussistenza di un interesse privato collegato alla segnalazione.

Resta inteso che il *whistleblowing* **non riguarda doglianze di carattere personale** del Segnalante o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro o rapporti con superiore gerarchico o colleghi. Pertanto, non verranno verificate dal **RWP (RWA)**, le segnalazioni aventi ad oggetto rimostranze di carattere personale del Segnalante o richieste che attengono alla disciplina del rapporto di lavoro, ai rapporti interpersonali con superiori gerarchici o colleghi e che attengono, in generale, all'osservanza dei doveri di diligenza nell'ambito dell'esecuzione della prestazione lavorativa.

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare del Segnalante, nell'ipotesi di segnalazione calunniosa e diffamatoria ai sensi del codice penale o ai sensi dell'articolo 2043 del Codice Civile.

I lavoratori hanno diritto di effettuare segnalazioni anonime, tuttavia l'impossibilità per il **RWP/RWA** di chiedere informazioni o dare riscontro al Segnalante potrebbe compromettere l'indagine.

1.5.2 Canali di segnalazione

La Direttiva europea pone in capo agli Stati membri il compito di assicurare che vengano apprestati canali di segnalazione interna.

Coerentemente, il Decreto – per quanto applicabile – individua tre canali di segnalazione (interno, esterno e tramite divulgazione pubblica) che, al verificarsi di talune condizioni, devono essere attivati in via alternativa e sussidiaria in ragione della natura e della struttura dell'ente.

I canali individuati dalla normativa speciale e di settore consentono segnalazioni in forma scritta od orale. Le segnalazioni orali sono possibili attraverso linee telefoniche o attraverso altri sistemi di messaggistica vocale e, su soggetto segnalante, mediante un incontro diretto entro un termine ragionevole.

Tanto premesso, la SGR applica le previsioni di cui ai seguenti paragrafi.

1.5.3 Canale di segnalazione interna

Al fine di perseguire la miglior tutela della riservatezza del Segnalante, nonché, ove richiesto dalla normativa, garantire la forma anonima delle segnalazioni³, le stesse sono effettuate attraverso canali specifici, autonomi e indipendenti, che differiscono dalle ordinarie linee di reporting della Società.

³ Cfr. art. 48, comma 2, lett. c) del Decreto Antiriciclaggio.

Le modalità attraverso cui può essere inoltrata una segnalazione sono le seguenti:

- lettera in busta chiusa inviata a mezzo posta ordinaria
 - o all'indirizzo, AcomeA SGR Spa, Largo Guido Donegani 2, 20121 Milano all'attenzione del "Responsabile Whistleblowing primario" ("Riservata Personale", senza indicazione del Mittente); in tal caso l'addetto della reception consegnerà la busta a RWP in modo confidenziale senza aprirla e la comunicazione non verrà successivamente protocollata, ma conservata da RWP (cfr. § 1.12);
- e-mail all'indirizzo di posta elettronica "segnalazioni.RWP@acomea.it" – per le comunicazioni al **RWP**;
- e-mail all'indirizzo di posta elettronica "segnalazioni.RWA@acomea.it" – per le comunicazioni al **RWA**.

A tal fine la SGR ha predisposto anche un'apposita casella di posta elettronica a cui poter inviare le mail in forma anonima garantendo la riservatezza sull'identità del segnalante. Le istruzioni operative per l'accesso a tale servizio saranno portate a conoscenza di tutti i dipendenti tramite apposita comunicazione.

In tal modo, l'identità del Segnalante (ove la segnalazione non sia trasmessa in forma anonima) sarà conosciuta solo dal **RWP** (o **RWA**), che ne garantirà la riservatezza, fatti salvi i casi in cui la stessa non sia opponibile per legge.

Al ricevimento della comunicazione, il soggetto destinatario:

- a) rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
- b) mantiene le interlocuzioni con la persona segnalante richiedendo a quest'ultima, se necessario, integrazioni;
- c) fornisce diligente seguito alle segnalazioni ricevute;
- d) fornisce riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Avvertenza: l'identità del Segnalante è sottratta all'applicazione dell'articolo 15 del GDPR comma 1⁴, e non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

Deve essere altresì garantita la tutela adeguata del Segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione.

⁴ Art. 15, comma 1 GDPR: "Diritto di accesso dell'interessato": "L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato."

RWP (o **RWA**) non partecipano all'adozione degli eventuali provvedimenti decisionali, che sono rimessi al **CdA**, **CS**, **OdV**, ciascuno per quanto di competenza.

1.5.4 Segnalazioni esterne all'Autorità di Vigilanza

Dal 3 gennaio 2018, a norma dell'art. 4-*duodecies* TUF, il personale dei soggetti indicati dall'art. 4-*undecies* del TUF può trasmettere le Segnalazioni anche direttamente alle Autorità di Vigilanza in conformità a regole operative da loro definite, consentendo in tal modo al personale degli intermediari di segnalare all'Autorità violazioni delle norme del TUF e delle norme UE direttamente applicabili di cui sia venuto a conoscenza durante lo svolgimento della propria attività lavorativa.

A questo riguardo, Banca d'Italia e Consob:

- a) ciascuna per quanto di propria competenza, ricevono, da parte del personale dei soggetti indicati all'articolo 1.2 del presente Regolamento, Segnalazioni che si riferiscono a violazioni delle norme del Decreto Legislativo 24 febbraio 1998, n. 58 (TUF), nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie. Tra queste, Consob riceve le Segnalazioni riferite a violazioni delle disposizioni in tema di abusi di mercato di cui al regolamento (UE) n. 596/2014, in conformità alle procedure adottate da Consob ai sensi della Direttiva di esecuzione (UE) 2015/2392;
- b) possono stabilire condizioni, limiti e procedure per la ricezione delle Segnalazioni, tenendo conto:
 - della riservatezza dei dati personali del Segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della Segnalazione; l'identità del Segnalante è sottratta all'applicazione dell'articolo 7, comma 2, lettera g) del Regolamento (UE) 2016/679, e non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del Segnalato;
 - della tutela adeguata del soggetto Segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la Segnalazione;
- c) si avvalgono delle informazioni contenute nelle Segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza;
- d) prevedono, mediante protocollo d'intesa, le opportune misure di coordinamento nello svolgimento delle attività di rispettiva competenza, ivi compresa l'applicazione delle relative sanzioni, in modo da coordinare l'esercizio delle funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti vigilati. Gli atti relativi alle Segnalazioni sono sottratti all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

Sul sito della Consob è possibile consultare la sezione dedicata, al seguente indirizzo: <http://www.consob.it/web/area-pubblica/whistleblowing>.

In tale sezione sono indicate le modalità operative che tutto il personale della SGR deve seguire per trasmettere direttamente alla Consob Segnalazioni riferite a presunti illeciti o violazioni delle norme del TUF nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie.

Parimenti, la Banca d'Italia ha provveduto, in attuazione del già citato art. 4-*duodecies* del TUF, alla predisposizione del c.d. *modulo whistleblowing* a disposizione di dipendenti e collaboratori degli intermediari vigilati (c.d. Segnalazioni whistleblowing) sia di altri soggetti non dipendenti o collaboratori (c.d. Segnalazioni aziendali). Al seguente indirizzo si possono consultare le istruzioni utili per l'inoltro di segnalazioni di violazioni: https://www.bancaditalia.it/ricerca/site-search.html?tutte_le_parole=segnalazioni+whistleblowing. I moduli possono essere inviati tramite casella di posta elettronica alla casella di posta certificata whistleblowing@banca.ditalia.it.

vigilanza@bancaditalia.it ovvero via posta ordinaria, all'indirizzo della Banca d'Italia – Servizio CRE – divisione SRE – a Roma, Via Nazionale n. 91, con busta recante la dicitura “riservato”.

La Banca d'Italia, laddove lo ritenga opportuno, si riserva di contattare il Segnalante per ottenere ulteriori informazioni o chiarimenti, in osservanza al segreto d'ufficio che copre tutti i dati e le informazioni o notizie acquisiti in ragione dell'attività di vigilanza. La Banca d'Italia assicura la riservatezza dei dati personali del Segnalante, anche al fine di assicurare quest'ultimo da possibili ritorsioni.

Il modulo di Segnalazione (per i dipendenti e collaboratori degli intermediari vigilati) ricomprende oltre alle informazioni anagrafiche e di contatto del Segnalante, il ruolo e la qualifica ricoperte all'epoca del fatto segnalato, l'area cui può essere riferito l'illecito (es. area crediti, controllo interno...), la data o l'arco temporale in cui si è consumato l'illecito, una descrizione sintetica dei fatti oggetto della Segnalazione, nonché l'indicazione delle ulteriori autorità cui è stata presentata eventualmente la Segnalazione.

1.5.5 Segnalazioni esterne all'ANAC

Per tutte le violazioni non disciplinate dalle norme speciali sopra individuate, il Decreto ha introdotto e disciplinato (artt. 6 e 7) un nuovo percorso di segnalazione esterna che può essere attivato dal Segnalante al verificarsi delle seguenti condizioni:

- a) se, nello specifico contesto lavorativo, l'attivazione del canale di segnalazione interna non è obbligatoria ovvero il canale non è attivo o non è conforme ai requisiti normativi;
- b) se il whistleblower ha già fatto una segnalazione interna, ma la stessa non ha avuto seguito;
- c) se il whistleblower ha fondato motivo di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- d) se il whistleblower ha fondato motivo di ritenere che la violazione segnalata possa costituire un pericolo imminente o palese per il pubblico interesse.

Il canale di segnalazione esterno è gestito dall'Autorità Nazionale Anticorruzione (ANAC), alla quale il Decreto attribuisce poteri di natura regolatoria, gestoria e sanzionatoria.

L'ANAC offre le medesime garanzie di riservatezza previste per la segnalazione interna (par. 1.5.3).

Sono altresì previsti i medesimi obblighi applicabili alle segnalazioni interne (es. tempi di riscontro); laddove ANAC riceva una segnalazione di competenza di altra Autorità (giudiziaria o amministrativa, anche europea) è tenuta a trasmetterla a quest'ultima dandone avviso al Segnalante.

Il Decreto prevede, in capo all'ANAC, l'onere di indicare – in apposito elenco – gli Enti del Terzo Settore che potrebbero fornire assistenza ai segnalanti nelle fasi prodromiche, contestuali e successive alla segnalazione (artt.18,19). La tutela viene estesa anche a: facilitatori (persone fisiche che assistono i segnalanti nel processo di segnalazione all'interno del medesimo contesto lavorativo), persone legate al Segnalante da uno stabile legame affettivo o di parentela entro il quarto grado, colleghi di lavoro della persona Segnalante che hanno con detta persona un rapporto abituale e corrente e altri enti di proprietà o collegati alla persona Segnalante (art.3, comma 5).

È attribuito all'ANAC il potere di applicare sanzioni amministrative pecuniarie:

- nel caso in cui siano state commesse ritorsioni o la segnalazione è stata ostacolata o è stato violato l'obbligo di riservatezza;

- in caso di mancata istituzione di canali di segnalazione e di mancata o inadeguata adozione di procedure per l'effettuazione e la gestione delle segnalazioni;
- nel caso di accertamento della responsabilità della persona Segnalante per i reati di diffamazione o di calunnia sia sul piano penale, che civile nei casi di dolo o colpa grave.

1.5.6 *Divulgazione Pubblica*

L'art. 15 del Decreto prevede il canale di divulgazione pubblica, anch'esso attivabile solo laddove la segnalazione della violazione non sia già disciplinata in via obbligatoria dalle norme speciali sopra indicate e, in ultima istanza e solo al verificarsi di talune condizioni individuate nel medesimo articolo, quali:

- a) la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna alla quale non è stato dato riscontro entro i termini stabiliti;
- b) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- c) la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

Laddove dovesse verificarsi una delle suindicate circostanze, il Segnalante può rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

1.6 **Analisi e valutazione delle segnalazioni**

Il **RWP** (o **RWA**, nei casi di cui al § 1.3.2) ricevuta la segnalazione svolge le seguenti attività:

- analizza la segnalazione ricevuta per verificarne la "pertinenza" ai sensi della normativa di tempo in tempo vigente;
- attiva, qualora necessario e possibile, un flusso comunicativo con il Segnalante al fine di approfondire le informazioni contenute nella segnalazione;
- effettua le valutazioni di merito riguardo la segnalazione e intraprendere le necessarie azioni di accertamento dei fatti descritti all'interno della segnalazione stessa.

Ai fini dell'analisi, il **RWP** (o **RWA**) potrà richiedere il supporto e la collaborazione delle funzioni aziendali competenti in relazione alla tematica oggetto della segnalazione, nonché avvalersi del supporto di consulenti tecnici (quali ad esempio studi legali esterni o specialisti interni all'azienda) su materie che non rientrano nella propria specifica competenza e potrà chiedere, inoltre, il supporto di tutti i dipendenti. Tutto ciò potrà avvenire solo avendo cura che il coinvolgimento non comprometta l'oggettività dell'analisi né la tutela del soggetto Segnalante.

Il **RWP** (o **RWA**) assicura che l'indagine sia svolta con accuratezza e in tempi ragionevoli e comunque non oltre 60 giorni dalla ricezione della stessa.

Qualora a seguito dell'analisi dei fatti oggetto di segnalazione, emerga l'evidente e manifesta infondatezza di quanto riportato, il **RWP** (o **RWA**) può decidere di archiviare la segnalazione.

Si precisa che le attività del **RWP** (o **RWA**) sono condotte nel rispetto dei principi di imparzialità e riservatezza, nonché nel rispetto della dignità del dipendente, della normativa in tema di protezione dei dati personali, dei

principi di legge in materia del lavoro e della disciplina contrattuale di settore. Tali principi si applicano anche alle funzioni aziendali / altri soggetti che il **RWP** / **RWA** decida di coinvolgere nell'analisi delle segnalazioni.

1.7 Comunicazione agli organi aziendali

A seguito dello svolgimento delle indagini in merito alle segnalazioni ricevute ritenute non infondate, il **RWP** (o **RWA**) informa il Presidente del **CdA** e il Presidente del **CS** (con esclusione del soggetto eventualmente interessato dalla segnalazione), sottoponendo apposita informativa che riassume l'iter dell'indagine, le conclusioni alle quali si sia giunti e che, ove ritenuto necessario, fornisca raccomandazioni e indichi le azioni da porre in essere per sopperire alle violazioni riscontrate e presidiare i rischi che queste si verifichino in futuro. Il Presidente del CdA e il Presidente del CS avranno cura di trasmettere l'informativa così ricevuta agli organi aziendali⁵.

A seguito della trasmissione dell'informativa, gli organi aziendali competenti, con l'esclusione dei soggetti eventualmente interessati, dovranno adottare tempestivamente le azioni disciplinari e/o sanzionatorie ritenute opportune e potranno altresì rendere raccomandazioni di azioni correttive al fine di minimizzare il rischio che le condotte illecite o pratiche scorrette rilevate non si ripetano.

Le delibere degli organi aziendali sono adeguatamente motivate e verbalizzate. Le evidenze delle attività svolte dagli organi aziendali sono conservate con modalità idonee a garantire la riservatezza e la tutela dei soggetti coinvolti.

Nel caso in cui il Segnalante sia corresponsabile delle violazioni, è previsto un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la violazione commessa e con la disciplina applicabile.

⁵ Resta inteso che qualora il Presidente del CdA e il Presidente del CS fossero interessati dalla segnalazione, l'informativa potrà essere trasmessa direttamente agli organi aziendali, con esclusione dei rispettivi Presidenti.

1.8 Comunicazione al soggetto Segnalante (per segnalazioni diverse da quelle in forma anonima)

Il soggetto Segnalante viene informato sugli sviluppi del procedimento che si instaura in relazione ai contenuti della segnalazione.

Le comunicazioni inviate al Segnalante saranno le seguenti:

- la comunicazione di archiviazione senza esito, qualora il **RWP** (o **RWA**) non abbia ritenuto necessario avviare un'indagine per evidente infondatezza della segnalazione;
- la comunicazione di avvio del procedimento, per le segnalazioni ritenute meritevoli di indagine;
- la comunicazione di conclusione del procedimento.

Il Segnalante è tenuto alla più completa riservatezza su tutte le informazioni ricevute; la violazione di tale obbligo può comportare conseguenze disciplinari.

Il canale di comunicazione con il Segnalante sarà il medesimo tramite il quale è pervenuta la segnalazione.

1.9 Comunicazione al soggetto segnalato

Qualora dall'esito della verifica, la segnalazione risulti non infondata, **RWP** (o **RWA**) procede a informare il soggetto segnalato sugli sviluppi del procedimento che si instaura in relazione ai contenuti della segnalazione.

La comunicazione avviene a cura del **RWP** (o **RWA**) ed è resa compatibilmente con la necessità di non compromettere l'attività di analisi e verifica della fondatezza della segnalazione e della relativa raccolta delle prove necessarie al procedimento.

Le comunicazioni inviate al Segnalato saranno le seguenti:

- la comunicazione di avvio del procedimento, per le segnalazioni ritenute meritevoli di indagine;
- la comunicazione di conclusione del procedimento.

1.10 Misure di tutela del soggetto Segnalante

La SGR nel dotarsi di un sistema interno di segnalazione delle violazioni è tenuta:

- a sviluppare uno specifico canale di segnalazione autonomo e indipendente proporzionato alla natura e alle proprie dimensioni;
- a garantire la possibilità di trasmettere una segnalazione anonima nel caso di violazioni di cui al Decreto Antiriciclaggio;
- a tenere indenne il Segnalante da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione stessa (a titolo esemplificativo: licenziamento, demansionamento, mobbing, o altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro in conseguenza della segnalazione, ecc).

Il personale che effettua una segnalazione ai sensi della presente procedura non può essere sanzionato, licenziato o sottoposto ad alcuna misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati, anche solo indirettamente, alla segnalazione. Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili. Il personale che ritiene di aver subito una discriminazione ne dà notizia circostanziata all'RWP/RWA che, accertata la fondatezza, segnala la casistica agli Organi Aziendali competenti, affinché siano adottati i provvedimenti necessari a ripristinare la situazione e/o rimediare agli effetti negativi della discriminazione.

È altresì vietata ogni forma di ritorsione o discriminazione avente effetti sulle condizioni di lavoro di chi collabora alle attività di riscontro della fondatezza della segnalazione.

La SGR è tenuta inoltre a garantire, in ogni caso, la riservatezza dell'identità del Segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'Autorità Giudiziaria, in relazione ai fatti oggetto della segnalazione. La violazione dell'obbligo di riservatezza, inclusa la divulgazione di informazioni in base a cui l'identità del Segnalante si possa dedurre, è considerata una violazione della presente procedura ed è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

L'identità del Segnalante è inoltre sottratta al diritto di accesso previsto dall'art. 15 del GDPR, ad eccezione dei casi in cui:

- il Segnalante esprima il proprio consenso alla divulgazione;
- la sua divulgazione sia necessaria per garantire la difesa del segnalato (ad esempio, nel caso sia necessaria perché richiesta dall'Autorità giudiziaria o risulti indispensabile per garantire la difesa del segnalato).

Si rimanda inoltre al Modello 231 con riferimento alle misure di tutela previste per i soggetti segnalanti con specifico riferimento alle segnalazioni rilevanti ai sensi del Decreto 231.

1.11 Reporting

Il **RWP**, con il supporto del **RWA** per quanto di competenza, redige con cadenza annuale - solo qualora vi siano state segnalazioni - una relazione per il **CdA** ed il **CS**, contenente informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, fornendo indicazioni circa il corretto funzionamento del sistema interno di segnalazione ed evidenziando eventuali criticità emerse. La relazione è trasmessa altresì all'**OdV** in relazione alle segnalazioni rilevanti ai sensi del Decreto 231. La relazione è approvata dal Consiglio di Amministrazione e messa a disposizione del personale sulla rete aziendale in apposita sezione.

1.12 Conservazione e archiviazione

La documentazione raccolta nel corso dell'intera procedura di segnalazione è confidenziale e viene archiviata in sicurezza in formato cartaceo o su supporto informatico, a cura del **RWP** (o **RWA**) in conformità con le norme in vigore sul trattamento dei dati personali per almeno 5 anni.

Possono accedere ai predetti documenti, esclusivamente i soggetti espressamente autorizzati da **RWP** (o **RWA**) e/o i componenti degli organi aziendali – ove non direttamente coinvolti – interessati per le opportune deliberazioni.

Nel caso in cui funzioni di controllo o Autorità esterne abbiano necessità di acquisire dati e informazioni inerenti alle segnalazioni prodotte per le rispettive finalità istituzionali, potrà essere fornito loro l'accesso alla documentazione raccolta e archiviata, garantendo l'anonimato dei soggetti coinvolti, nei limiti in cui l'anonimato e la riservatezza siano opponibili per legge e nel rispetto delle misure di tutela del Segnalante riportate al § 1.10.

1.13 Formazione

Ogni modifica o aggiornamento della presente policy è approvata dal CdA e, in ogni caso, la SGR garantisce a tutti i dipendenti la possibilità di prenderne visione mediante pubblicazione sull'intranet aziendale ed invia una comunicazione ad hoc in caso di variazioni del RWP/RWA o dei canali di segnalazione.

Inoltre, al fine di promuovere una cultura della legalità, la SGR assicura l'erogazione di una formazione annuale a tutti i dipendenti all'interno del modulo di formazione antiriciclaggio circa gli atti o i fatti che possono essere oggetto di segnalazione, le modalità di inoltro della medesima e i presidi posti a garanzia della riservatezza dei dati personali sia del Segnalante, sia del presunto responsabile della violazione.

1.14 Informativa a Banca d'Italia e Consob

Le autorità di vigilanza hanno dedicato le seguenti pagine:

Consob: <http://www.consob.it/web/area-pubblica/whistleblowing> alla disciplina del whistleblowing esterno, per gli aspetti di propria competenza, regolando le modalità operative e i contenuti del processo di segnalazione.

Banca d'Italia: <https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html> alla disciplina del whistleblowing esterno, per gli aspetti di propria competenza, regolando le modalità operative e i contenuti del processo di segnalazione.

1.15 Pubblicazione

La presente policy è portata a conoscenza di tutto il personale della SGR e sempre accessibile sulla intranet aziendale, nella sezione normativa interna.