



Global Policy

Whistleblowing

FB 026_2023

**Funzione
Approvante**

Consiglio di Amministrazione

Data Luglio 2023

**Funzione
Proponente**

Compliance

Indice

1	PREMESSA	3
1.1	Scopo del documento e sintesi dei contenuti	3
1.2	Contesto normativo esterno di riferimento	5
1.3	Glossario e Acronimi.....	5
1.4	Processo Whistleblowing	7
	Gestione delle segnalazioni interne ed esterne di comportamenti illegittimi	7
	Indagine sulla segnalazione interna	11
	Esito dell'indagine sulla segnalazione interna	12
2	MISURE DI PROTEZIONE PREVISTE DAL GRUPPO.....	12
2.1	Protezione delle persone coinvolte nel processo di segnalazione	12
2.2	Protezione dei dati e archiviazione dei documenti	13
2.3	Formazione e Comunicazione	14
2.4	Responsabile del Sistema interno di segnalazione delle violazioni. Controlli e reportistica.....	14

1 PREMESSA

FinecoBank S.p.A., in qualità di Capogruppo – in conformità alle leggi e regolamenti vigenti ed in coerenza con il sistema di coordinamento manageriale di Gruppo definito dalle Group Managerial Golden Rules – emette linee guida, nell'interesse della stabilità del Gruppo, allo scopo di esercitare compiutamente il proprio ruolo di gestione e coordinamento.

Il presente documento integra la normativa di Gruppo, è direttamente applicabile alla Capogruppo ed è indirizzato alle Società del Gruppo destinatarie.

Come previsto dalla Global Policy di Gestione della Normativa di Gruppo, il presente documento sarà adottato in conformità a leggi e regolamentazioni vigenti localmente, che prevalgono in caso di conflitto e requisiti più stringenti.

Dopo l'approvazione da parte degli organi deputati di Fineco, la stessa, in qualità di Capogruppo, trasmette la Global Rule alle Entità per l'approvazione da parte dei rispettivi Organi Societari e ne monitora la corretta e tempestiva implementazione anche avvalendosi delle sue funzioni interne di volta in volta identificate.

Le Società del Gruppo sono pertanto tenute ad avviare tempestivamente – dopo l'opportuna valutazione ed approvazione da parte dei propri Organi competenti – le necessarie attività finalizzate alla corretta applicazione del presente documento.

Nel caso in cui le Società ritenessero:

1. la presente Global Rule (di seguito anche GR) non applicabile, ovvero
2. necessario apportare delle modifiche/deroghe alle previsioni contenute nella presente GR, ai fini della conformità con la normativa locale (se più restrittiva) o in ragione di vincoli di natura organizzativa ed operativa

le Società destinatarie dovranno formulare alla Direzione Compliance di Capogruppo una richiesta di Non Binding Opinion, ai sensi di quanto disposto dalla normativa di Gruppo vigente (Gestione della Normativa di Gruppo).

1.1 Scopo del documento e sintesi dei contenuti

Il Gruppo FinecoBank è impegnato a promuovere una cultura aziendale caratterizzata da comportamenti corretti e da un buon sistema di *corporate governance* e per questa ragione riconosce l'importanza di avere una Rule che disciplini la Segnalazione di Comportamenti Illegittimi da parte dei Dipendenti e di Terze Parti (la "Whistleblowing Global Policy").

Pertanto, la presente Rule definisce canali di comunicazione adeguati per la ricezione, l'analisi e la gestione delle Segnalazioni di Comportamenti Illegittimi all'interno del Gruppo.

Scopo di questa Rule è promuovere un ambiente aziendale in cui i Dipendenti e le Terze Parti si sentano a proprio agio nell'inoltrare una Segnalazione di Comportamenti illegittimi all'interno del

Gruppo, poiché si ritiene che tali Segnalazioni contribuiscano significativamente ad autocorreggersi e a migliorare procedure e comportamenti all'interno del Gruppo.

La presente Global Policy (di seguito anche Policy) va letta congiuntamente alla "Global Policy – Carta di integrità, Codice di Condotta e Compliance Culture" e alla "Global Policy - Lotta alle molestie, ai comportamenti sessualmente inappropriati e al bullismo" così come implementate in ogni Società del Gruppo. Si applica a tutte le Società del Gruppo, comprese le Terze Parti (ad esempio in occasione della formalizzazione di relazioni d'affari e della sottoscrizione di accordi dovrebbe essere inclusa anche una clausola sul Whistleblowing).

Per Comportamento Illegittimo si intende qualsiasi azione o omissione (violazione), avvenuta nello svolgimento dell'attività lavorativa o che abbia un impatto sulla stessa, che arrechi o che possa arrecare danno o pregiudizio al Gruppo e/o ai suoi Dipendenti, o che leda l'interesse pubblico o l'integrità, e che:

- sia illecita, scorretta o immorale;
- violi le disposizioni normative e regolamentari nazionali o dell'Unione Europea; o
- non sia conforme alle normative interne.

La presente Policy si applica agli argomenti trattati nelle Group Rules e in altra normativa interna, quali ad esempio:

- corruzione;
- riciclaggio di denaro;
- violazioni della normativa sulle Sanzioni Finanziarie;
- comportamenti di business non etici o non professionali;
- violazione della normativa anti-trust;
- insider trading e/o manipolazione del mercato;
- molestie;
- comportamenti sessualmente inappropriati;
- bullismo;
- frodi;
- abuso di informazioni e dati dei clienti e della società;
- violazioni di normative e leggi locali;
- non conformità alle normative e procedure di Gruppo;
- violazioni del Codice Etico e/o del Codice di Condotta;

- interazioni aggressive¹;
- altre pratiche o comportamenti illeciti o non corretti.

1.2 Contesto normativo esterno di riferimento

Il Gruppo FinecoBank opera – e lo richiede a tutti i suoi Dipendenti e alle Terze Parti – nel pieno rispetto di tutte le leggi e regolamenti sovranazionali, nazionali e locali applicabili. In alcuni Paesi gli standard e le regole di Gruppo possono essere più restrittivi rispetto ai requisiti di legge locali. Per quanto oggetto della presente Policy, il Gruppo FinecoBank applica i migliori standard, a prescindere dal fatto che i comportamenti segnalati siano o meno vietati dalla normativa di riferimento.

FinecoBank garantisce che la persona che segnala comportamenti inappropriati non sia di conseguenza penalizzata quanto all'incarico lavorativo o ad altre attività connesse al lavoro.

1.3 Glossario e Acronimi

Termine	Definizione
Capogruppo	FinecoBank S.p.A. (di seguito anche "FinecoBank", "Fineco" o "Banca").
Società controllata del Gruppo	Entità direttamente o indirettamente controllata da FinecoBank S.p.A. (di seguito anche "Entità", "Entità del Gruppo", "Entità controllata", "Entità consolidata", "Società controllata" o in breve "LE").
Gruppo	Gruppo FinecoBank, composto da FinecoBank S.p.A. e dalle Società/LE del Gruppo (di seguito anche "Gruppo Fineco").
Società del Gruppo	Società del Gruppo FinecoBank, intendendo la stessa Capogruppo FinecoBank e le sue Società controllate.
Dipendenti	Ai fini di questa Rule e indipendentemente dalla legislazione laburistica vigente si intendono come Dipendenti i dirigenti, funzionari e/o membri di organi strategici, di controllo e/o esecutivi, dipendenti, consulenti finanziari abilitati all'offerta fuori sede e collaboratori anche a titolo temporaneo legati da un contratto a FinecoBank e alle Società del Gruppo.
Terze Parti	Persone fisiche o giuridiche legate al Gruppo da un contratto o un interesse rilevante come, ad esempio, i fornitori, gli appaltatori, gli agenti, i liberi professionisti e consulenti, gli azionisti, i volontari e tirocinanti, retribuiti e non retribuiti, i candidati a un posto di lavoro che sono stati coinvolti nel processo di assunzione o in altre trattative precontrattuali, ex dipendenti ed ex collaboratori.
Segnalazione	Comunicazione scritta o verbale di informazioni sui comportamenti illegittimi.

¹ Tutti gli episodi di aggressività verbale o fisica - ivi compresi episodi riferiti a differenze di genere - o, comunque, un qualsivoglia episodio minaccioso, che possano essere attuati nei luoghi di lavoro a danno del personale di FinecoBank.

Informazioni sui comportamenti illegittimi	Notizie, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.
Segnalazione in malafede	Segnalazione falsa e infondata, con lo scopo di danneggiare o recare pregiudizio a uno o più Dipendenti o al Gruppo.
Segnalazione nominativa	Segnalazione che specifica l'identità del Segnalante.
Segnalazione interna	Comunicazione, scritta o verbale, delle informazioni sui comportamenti illegittimi, presentata tramite il canale di segnalazione interna alla Società.
Segnalazione esterna	Comunicazione, scritta o verbale, delle informazioni sui comportamenti illegittimi, presentata tramite il canale di segnalazione esterna alla Società.
Divulgazione pubblica	Rendere di pubblico dominio informazioni sui comportamenti illegittimi tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.
Segnalante/Whistleblower	La persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sui comportamenti illegittimi acquisite nell'ambito del proprio contesto lavorativo.
Facilitatore	Una persona fisica che assiste il Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.
Persona coinvolta/Segnalato	La persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale il comportamento illegittimo è attribuito o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
Persona designata	Una persona imparziale, competente per il seguito della segnalazione, che può essere la stessa persona o funzione che riceve la segnalazione e che manterrà la comunicazione con il segnalante e, se necessario, chiederà ulteriori informazioni e fornirà un riscontro al segnalante stesso.
Whistleblowing Managerial Forum	Forum, che ogni Società istituisce, composto dai Responsabili di Compliance, CRO, Internal Audit e HR (nel caso di segnalazioni riferite a Dipendenti) o altra Struttura competente per l'assunzione di provvedimenti disciplinari nei confronti di soggetti diversi dai dipendenti. L'Internal Audit è ospite permanente e senza diritto di voto. Si riunisce ad evento.

Ritorsione	Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto. Le ritorsioni e i tentativi di ritorsione comprendono in particolare: a) il licenziamento, la sospensione o misure equivalenti; b) la retrocessione di grado o la mancata promozione; c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro, la limitazione dell'accesso ai dati; d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; e) le note di merito negative o le referenze negative; f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria; g) la coercizione, l'intimidazione, le molestie o l'ostracismo; h) la discriminazione o comunque il trattamento sfavorevole; i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione; l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; m) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi; n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro; o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; p) l'annullamento di una licenza o di un permesso; q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.
Segnalazione Grave	Una segnalazione è classificata come grave quando: (i) la persona accusata di un presunto Comportamento Illegittimo ricopre una posizione di vertice o (ii) si riferisce ad ambiti normativi nei quali il rischio sanzionatorio/reputazionale è elevato (ad es. procedure anticiclaggio) o (iii) è stata indirizzata a un'Autorità di Vigilanza, a un'Autorità Fiscale, a un'Autorità Giudiziaria e ai media.

1.4 Processo Whistleblowing

Il processo di Whistleblowing di ogni Società del Gruppo deve prevedere quanto segue:

- Gestione delle segnalazioni interne ed esterne di comportamenti illegittimi;
- Indagine sulla segnalazione interna;
- Esito dell'indagine sulla segnalazione interna.

Gestione delle segnalazioni interne ed esterne di comportamenti illegittimi Segnalazione interna di comportamenti illegittimi

Le Società attivano propri canali di segnalazione che garantiscano, anche tramite ricorso alla crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché il contenuto della segnalazione e della relativa comunicazione.

Nel caso in cui un Dipendente o una Terza Parte ritenga che si sia verificato o che possa verificarsi un Comportamento Illegittimo, lo stesso può segnalarlo al responsabile di Compliance² della propria Società del Gruppo (oppure, nel caso in cui non esista la funzione di Compliance, al responsabile dell'Internal Audit³). Qualora la Segnalazione riguardi proprio detti soggetti, il Dipendente o la Terza Parte è tenuto a rivolgersi direttamente all'Alta Direzione della propria società.

Se il Dipendente o una Terza parte ha dei dubbi in merito alla classificazione di una condotta quale legittima o meno, ne potrà parlare informalmente con il proprio responsabile ovvero con la Compliance della propria società, che tratterà tale confronto come confidenziale.

Se la Segnalazione è inviata ad una Funzione diversa da Compliance, la stessa dovrà inoltrarla – con la massima urgenza e riservatezza – alla Compliance Locale. Ciò prescinde dal canale *whistleblowing* utilizzato e/o dal tipo di Segnalazione ricevuta (anonima o nominativa).

I Dipendenti o le Terze Parti possono inviare Segnalazioni, sia indicando la loro identità (Segnalazioni Nominative) sia in forma anonima, utilizzando i canali *whistleblowing* messi a disposizione dalla Società. I canali *whistleblowing* garantiscono la riservatezza dell'identità del segnalante, salvo che quest'ultimo ne autorizzi la divulgazione.

Il Gruppo preferisce Segnalazioni nominative in quanto:

- è più difficile indagare se sono necessarie ulteriori informazioni dal segnalante;
- è più difficile proteggere il segnalante;
- è più difficile fornire al segnalante risposte sui risultati dell'indagine.

La Segnalazione deve contenere informazioni sufficientemente dettagliate, tali da consentire di avviare le analisi e le indagini.

I canali dedicati *whistleblowing*, istituiti per trasmettere Segnalazioni, anche se anonime, e comunque in grado di garantire l'anonimato del segnalante, sono uno o più dei seguenti:

- telefono⁴
- sito web dedicato⁵
- indirizzo e-mail dedicato
- lettera cartacea da trasmettere ad un indirizzo dedicato

² Per le Persone giuridiche italiane, se la Segnalazione riguarda violazioni del Modello Organizzativo adottato ai sensi del D. Lgs. 231/2001 o ipotesi di reato tra quelle contemplate da tale Decreto, la stessa può essere inviata anche direttamente all'Organismo di Vigilanza.

³ Nel caso in cui non esistano la funzione di Compliance e/o quella di Internal Audit, la Segnalazione dovrà essere indirizzata ad altra funzione/persona avente indipendenza/livello gerarchico e autonomia tale da garantire la correttezza del processo definito nella presente Global Policy.

⁴ In caso di linea telefonica non registrata, ogni LE deve garantire, con il consenso del segnalante, un verbale completo e accurato della telefonata che deve essere sottoposto all'approvazione del segnalante.

⁵ Il sito web può consentire di scrivere un messaggio o registrarlo.

incontro di persona⁶.

Non è obbligatorio mettere a disposizione tutti i canali di cui sopra contemporaneamente, ma in ogni caso è necessario consentire la segnalazione sia in forma scritta che verbale.

Una volta ricevuta la Segnalazione, il responsabile della gestione del canale (il responsabile di Compliance o la persona designata a gestire le segnalazioni *whistleblowing*, nel seguito la “persona designata”), informerà tempestivamente, se del caso/a seconda degli argomenti, una o più delle seguenti persone all’interno della propria Società del Gruppo, applicando le misure di riservatezza⁷:

il Responsabile delle Risorse Umane/altra Struttura competente per l’assunzione di provvedimenti disciplinari nei confronti di soggetti diversi dai dipendenti;

il Responsabile Anti-Corruption;

il Responsabile dell’AML;

il Responsabile di Legal;

il Responsabile di Security (per competenza);

il Presidente dell’Organismo di Vigilanza, nel caso in cui la società sia soggetta al D.Lgs. 231/ 2001 e la Segnalazione riguardi violazioni del Modello Organizzativo adottato ai sensi di tale Decreto oppure un reato tra quelli contemplati dal citato Decreto⁸.

Il responsabile della Compliance Locale (o dell’Internal Audit, se il segnalato è il responsabile di Compliance), o la persona “designata”, effettuerà una valutazione preliminare della Segnalazione pervenuta e, qualora dovesse ritenere che vi siano evidenze sufficienti di un Comportamento Illegittimo tali da consentire l’inizio di una indagine, incaricherà una persona/funzione di svolgere l’indagine stessa in base all’argomento di volta in volta segnalato (di seguito “persona incaricata a svolgere l’indagine”). Le Segnalazioni “gravi”, anche se anonime, devono essere gestite e segnalate tempestivamente e in modo riservato, rispettando lo specifico processo di Gruppo che garantisce il coinvolgimento dell’Alta Direzione della Società del Gruppo nelle fasi di analisi, di definizione del piano di attività e nei risultati dell’indagine, nelle raccomandazioni e nel monitoraggio.

Di conseguenza il Responsabile di Compliance o la persona designata informerà delle Segnalazioni gravi sia l’Amministratore Delegato sia il Whistleblowing Managerial Forum (WMF). Nel caso di Società

⁶ In caso di incontro fisico non registrato, ogni LE deve garantire, con il consenso del segnalante, un verbale completo e accurato dell’incontro che deve essere sottoposto all’approvazione del segnalante.

⁷ Per le misure di protezione e riservatezza si rimanda ai paragrafi 2.1 e 2.2.

⁸ Per le Persone giuridiche italiane, se la Segnalazione riguarda violazioni del Modello Organizzativo adottato ai sensi del D. Lgs. 231/2001 o ipotesi di reato tra quelle contemplate da tale decreto, la stessa può essere inviata anche direttamente all’Organismo di Vigilanza.

controllata inoltre il Responsabile di Compliance della LE informerà il Chief Compliance Officer di Capogruppo, garantendo che i nominativi delle persone coinvolte non compaiano nel processo di escalation, al fine di assicurare la completa riservatezza dei dati personali. Il Chief Compliance Officer di Capogruppo attiverà la procedura di escalation; il WMF della Capogruppo fornirà indicazioni sulle azioni da intraprendere, che saranno comunicate attraverso il Chief Compliance Officer di Capogruppo. Al WMF delle singole Società controllate compete la decisione delle azioni da intraprendere, motivandole, se del caso, in relazione alle indicazioni ricevute dal WMF di Capogruppo.

Tutte le Segnalazioni, sia verbali sia scritte, sono gestite dal Gruppo con la massima attenzione e la funzione di Compliance Locale, o il soggetto incaricato della gestione delle segnalazioni, deve trasmettere al segnalante, ove possibile (quando cioè sia disponibile un riferimento o un canale per comunicare con il segnalante), la conferma di ricezione della Segnalazione **entro e non oltre sette giorni** dal ricevimento.

Nel caso in cui non vi siano prove sufficienti del Comportamento illegittimo, ne sarà data informativa al Segnalante.

Nel caso in cui un Dipendente o una Terza Parte ritenesse che una Segnalazione non sia stata considerata seriamente all'interno della Società controllata, potrà rivolgersi al Responsabile di Compliance o alla "persona designata" della Capogruppo.

Le Segnalazioni sono accettate in lingua italiana o nella lingua locale.

Se una Segnalazione rientra nell'ambito di applicazione della Global Policy Reclami e non è esplicitamente contrassegnata come Segnalazione *wistleblowing*, la stessa dovrà essere gestita in base ai processi di gestione dei reclami.

Nel caso in cui si valuti che un Dipendente o una Terza parte effettui una Segnalazione in malafede, detto comportamento verrà seriamente considerato e potrà dar luogo ad un provvedimento disciplinare e/o ad azioni legali nei suoi confronti.

FinecoBank assicura la riservatezza, tutela della privacy e protezione dei dati e garantisce la protezione del segnalante da qualsiasi ritorsione (che, se accertata, determinerà un procedimento disciplinare a carico del responsabile) diretta o indiretta, connessa alla Segnalazione effettuata.

Segnalazione esterna di comportamenti illegittimi

In ogni Paese le Autorità competenti locali possono attivare canali dedicati alle segnalazioni *wistleblowing*. La Direttiva Europea 2019/1937 (recepita in Italia con il D.Lgs. 24 del 10 marzo 2023) prevede che i Segnalanti possano fornire informazioni sulle violazioni utilizzando i canali esterni, dopo

aver utilizzato i canali di segnalazione interni o segnalando direttamente attraverso i canali di segnalazione esterni, purché siano soddisfatte le condizioni previste dalle leggi locali. Il Segnalante può contattare anche l'Autorità locale competente, soprattutto qualora ritenga che una segnalazione non sia stata tenuta nel giusto conto all'interno del Gruppo. Tuttavia, i Dipendenti e le Terze Parti sono invitati ad utilizzare in via prioritaria i canali di Segnalazione interni del Gruppo FinecoBank.

I Dipendenti e le Terze Parti possono anche scegliere di fare una "divulgazione pubblica", rendendo le informazioni sulle violazioni disponibili al pubblico attraverso la stampa o i media o comunque attraverso mezzi di diffusione in grado di raggiungere un gran numero di persone⁹.

Indagine sulla segnalazione interna

La persona/funzione incaricata di svolgere l'indagine:

- deve assicurare che la stessa si svolga in maniera equa ed imparziale. Ciò comporta che, ove richiesto dalla normativa locale, ogni persona coinvolta nell'indagine possa essere informata in merito alle dichiarazioni rese ed alle prove acquisite a suo carico e che sia messa in condizione di poter controbattere alle stesse;
- può decidere, per l'esecuzione delle opportune verifiche/controlli, di proporre l'incarico alla funzione di Internal Audit o a un'altra funzione di controllo¹⁰;
- può avvalersi del supporto di consulenti tecnici (quali, ad esempio, studi legali esterni o specialisti interni al Gruppo) su materie che non rientrano nella propria specifica competenza e può chiedere, inoltre, il supporto di tutti i Dipendenti;
- assicura che l'indagine sia accurata, che abbia una durata ragionevole e che rispetti l'anonimato del segnalante e delle persone coinvolte, incluso il soggetto eventualmente segnalato (persona fisica o giuridica citata nella Segnalazione o notificata quale persona che ha compiuto o che è associata all'irregolarità).

⁹ Una persona che effettua una divulgazione pubblica beneficia della protezione prevista dalla legge se ricorre una delle seguenti condizioni: a) la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna, alle condizioni e con le modalità previste e non è stato dato riscontro nei termini previsti in merito alle misure previste o adottate per dare seguito alle segnalazioni; 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.

¹⁰ La funzione di Internal Audit si riserva la facoltà - in caso di disaccordo o mancanza di risorse - di non accettare l'incarico. In tal caso la persona/funzione incaricata di svolgere l'indagine, valuterà se portare la tematica all'attenzione degli organi aziendali competenti. Qualora accettato l'incarico, la funzione di Internal Audit opererà in maniera indipendente e secondo propri approcci e modalità standard, condivisi con il Responsabile di Compliance.

Le Società del Gruppo, ove consentito dalla normativa locale, devono tenere informati sia il soggetto segnalato sia il segnalante sugli sviluppi dell'indagine.

Esito dell'indagine sulla segnalazione interna

Terminata l'indagine, la persona/funzione incaricata di svolgerla redige una relazione per il Compliance Officer Locale (o per il Responsabile Internal Audit nel caso di conflitti d'interesse in capo al Compliance Officer).

La relazione sarà classificata come "strictly confidential" ovvero con livello massimo di riservatezza, conformemente alle disposizioni interne di Gruppo sulla classificazione delle informazioni.

Tale relazione deve:

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

Il Compliance Officer, sulla base della relazione, predispone una proposta di decisione (eventualmente suggerendo la necessità o meno di comminare provvedimenti disciplinari), che sottopone a tutti i componenti del WMF. La decisione finale è assunta a maggioranza dei membri con diritto di voto del WMF. Spetta in ogni caso alla funzione Risorse Umane/altra Struttura competente la decisione finale circa l'irrogazione degli eventuali provvedimenti disciplinari.

Il Dipendente che abbia commesso o sia stato coinvolto in un Comportamento Illegittimo non sarà immune da eventuali provvedimenti disciplinari per il solo fatto di aver segnalato un proprio o altrui Comportamento Illegittimo, ai sensi della presente Rule; tuttavia, tale circostanza potrà essere presa in considerazione nella valutazione del provvedimento disciplinare da adottare.

Il Segnalante dovrà ricevere un riscontro sul seguito dato alla Segnalazione entro tre mesi dalla conferma di ricezione della stessa o, se non è stato inviato alcun avviso di ricevimento al Segnalante, entro tre mesi dalla scadenza del periodo di sette giorni dalla segnalazione.

2 MISURE DI PROTEZIONE PREVISTE DAL GRUPPO

2.1 Protezione delle persone coinvolte nel processo di segnalazione

Ogni società del Gruppo protegge il Segnalante contro qualsiasi forma di ritorsione, discriminazione o penalizzazione per aver effettuato una Segnalazione in buona fede.

Qualsiasi atto di ritorsione o di discriminazione nei confronti del segnalante è vietato e, qualora accertato, può determinare un procedimento disciplinare a carico del responsabile e a sanzioni e procedimenti penali da parte delle Autorità secondo le leggi locali.

Il Dipendente che segnala o assiste ad un Comportamento illegittimo ha diritto a richiedere che la Società lo trasferisca in un altro dipartimento e, laddove necessaria, gli fornisca una consulenza psicologica indipendente in caso di stress derivante dalla Segnalazione. Il Gruppo ottempera a tali richieste quando perseguibili e giustificate.

Il Gruppo assicura la riservatezza dei dati personali del segnalante del segnalato e di altri soggetti definiti dalla legge, in tutte le fasi della procedura di segnalazione.

Il Gruppo garantisce l'anonimato del Segnalante, fatta eccezione per i casi in cui:

- il segnalante esprima il proprio consenso alla divulgazione;
- la divulgazione sia richiesta dalla normativa locale (ad esempio, se è necessario coinvolgere la polizia o le Autorità, o se è indispensabile per la difesa del segnalato); oppure
- la divulgazione sia necessaria per prevenire o ridurre minacce serie a danno della salute o della sicurezza delle persone.

La divulgazione non autorizzata dell'identità del Segnalante oppure di informazioni in base alle quali la stessa si possa dedurre è considerata una violazione della presente Rule e saranno comminate sanzioni nei confronti di chi viola le misure di protezione del Whistleblower.

Qualsiasi azione finalizzata a svelare illegalmente l'identità del Segnalante è considerata una violazione di questa Policy, è soggetta ai relativi procedimenti disciplinari e potrebbe essere sanzionata dalle Autorità.

Le misure di protezione si applicano anche, ove pertinente, ad altri soggetti collegati al segnalante, quali i facilitatori, i parenti, i colleghi e le persone giuridiche in relazione con il whistleblower.

2.2 Protezione dei dati e archiviazione dei documenti

La documentazione concernente le Segnalazioni è confidenziale. Tale documentazione deve essere archiviata in maniera sicura e nel rispetto delle norme vigenti all'interno del Gruppo sulla classificazione e trattamento delle informazioni confidenziali ed in conformità con la normativa e regolamentazione locale.

Tale documentazione sarà archiviata da Compliance e dalle altre funzioni coinvolte nell'indagine, e deve essere accessibile solo ai Dipendenti autorizzati in virtù del proprio ruolo e di apposita nomina a persona autorizzata al trattamento dei dati personali per finalità *Whistleblowing*.

Saranno archiviate solo le informazioni per le quali la normativa locale o quella interna alla Società del Gruppo ne impongono la conservazione. Per i dati personali che manifestamente non sono utili al

trattamento di una specifica segnalazione, questi non saranno raccolti o, se raccolti accidentalmente, saranno cancellati immediatamente.

In conformità alla normativa locale o interna, il segnalante, il segnalato e qualsiasi altro soggetto coinvolto hanno il diritto di avere conferma dell'esistenza di un trattamento dei dati personali che lo riguardano; ricevono pertanto apposita informativa sulle finalità e modalità di tale trattamento e possono conseguentemente richiedere modifiche, integrazioni, aggiornamenti o cancellazione quando i dati personali non sono più necessari in relazione allo scopo per il quale erano stati raccolti o altrimenti trattati; per il segnalato è tuttavia precluso, in ottemperanza della normativa tempo e per tempo vigente nei limiti di quanto previsto dalla stessa, l'esercizio di alcuni dei diritti di cui agli articolo 15 – 22 GDPR, quali ad esempio il diritto di accesso sulla segnalazione, se atto ad identificare l'identità del segnalante, al fine di garantire la riservatezza di quest'ultimo.

I dati personali trattati in seguito alle segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque (5) anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza in ottemperanza del principio di cui agli articoli 5, paragrafo 1, lettera e), del Regolamento (UE) 2016/679 e 3, comma 1, lettera e).

2.3 Formazione e Comunicazione

La formazione è un elemento fondamentale per l'implementazione e per l'applicazione di questa Policy e, a tal fine, il Gruppo si impegna a fornire ed aggiornare la formazione obbligatoria sul *whistleblowing* a favore di tutti i Dipendenti, così da evidenziare le specifiche procedure da seguire e le possibili conseguenze nel caso si verificano comportamenti inappropriati.

Il Gruppo è impegnato inoltre a promuovere la comunicazione sull'argomento; ogni LE mette a disposizione dei Dipendenti e delle Terze Parti informazioni chiare e facilmente accessibili sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne, anche sul proprio sito internet, ove presente, e l'implementazione ed applicazione della presente Policy all'interno di tutto il Gruppo, includendo le Terze Parti (ad esempio in occasione della formalizzazione di relazioni d'affari e della sottoscrizione di accordi con Terze Parti, dovrebbe essere inclusa anche una clausola sul *Whistleblowing*).

2.4 Responsabile del Sistema interno di segnalazione delle violazioni. Controlli e reportistica

Ciascuna Società del Gruppo deve nominare il *Responsabile del sistema interno di segnalazione delle violazioni*, attribuendogli la responsabilità di assicurare e controllare l'integrità, l'indipendenza e

l'efficacia dei processi e delle procedure di whistleblowing della Società. Ha un adeguato livello di autorevolezza ed indipendenza all'interno della Società e può avere accesso a tutte le informazioni e ai dati personali riferiti alle Segnalazioni ricevute. Egli predispose la Relazione Annuale sul corretto funzionamento del sistema interno per la segnalazione delle violazioni contenente informazioni aggregate sugli esiti delle attività e dei controlli relativi al rispetto dei principi di riservatezza e di divieto di atti ritorsivi.

La Relazione Annuale sul Whistleblowing deve essere approvata dagli Organi Societari e resa disponibile al Personale di ciascuna Società.

Le Società controllate dovranno trasmettere alla funzione Compliance di Capogruppo la Relazione annuale, nonché una reportistica periodica contenente, con dati anonimi, casi, parametri ed andamenti delle Segnalazioni ricevute nel periodo di riferimento.