Policy Whistleblowing di Sisal

Approvata dal Consiglio di Amministrazione di Sisal del 24/06/2024

Sommario

PREMESSA

Sisal S.p.A. (“Sisal” o la “Società”) e le relative società controllate si impegnano a condurre le proprie attività di business con onestà e integrità, mantenendo gli standard più alti di condotta e comportamento etico, anche in linea con i principi dettati dalla capogruppo Flutter Entertainment PLC (“Flutter”) e applicabili a tutte le società dalla stessa controllate (il “Gruppo”).

Con l’obiettivo di promuovere e rafforzare tali standard, Sisal ha implementato una Policy Whistleblowing (di seguito anche la “Policy”) per la segnalazione di qualsiasi condotta, anche omissiva, che costituisca o possa costituire una violazione o induzione ad una violazione di leggi, regolamenti, valori e principi sanciti dal proprio Codice Etico e di Comportamento, dal Modello 231, dalle proprie policy e procedure aziendali o dalle policy e procedure di Gruppo, come meglio specificato nel paragrafo “SCOPO E AMBITO DI APPLICAZIONE”. Chiunque è invitato a dare tempestiva comunicazione di tali condotte mediante le modalità di seguito descritte, astenendosi dall’intraprendere iniziative autonome di analisi e/o di approfondimento.

In ragione di ciò, la Società ha implementato specifici canali di comunicazione per la gestione delle Segnalazioni (come di seguito definite) al fine di essere conforme al D.lgs n. 24/2023 che recepisce la Direttiva UE 2019/1937 nonché ai principi in materia di whistleblowing sanciti nella “Whistleblower Policy” di Flutter.

A tal fine, la presente Policy:

- definisce l’ambito di applicazione del processo di Segnalazione;
- identifica i soggetti che possono effettuare Segnalazioni;
- identifica i canali attraverso cui effettuare la Segnalazione, idonei a garantire la

riservatezza del contenuto della stessa;

- identifica e prescrive i principi e le regole generali che governano il processo di Segnalazione, nonché le conseguenze di eventuali abusi nell'utilizzo dei canali istituiti;
- definisce il processo di gestione della Segnalazione nelle sue varie fasi, identificando ruoli, responsabilità, modalità operative e strumenti utilizzati;
- definisce le modalità di trattamento del contenuto della Segnalazione, compresi i dati identificativi del Segnalante e del Segnalato;
- tutela il Segnalante contro condotte ritorsive e/o discriminatorie, dirette o indirette, per motivi collegati alla Segnalazione.

SCOPO E AMBITO DI APPLICAZIONE

La presente Policy descrive il processo e i canali di comunicazione da utilizzare per l'invio, la ricezione, l'analisi e il trattamento delle Segnalazioni di irregolarità o comportamenti illeciti, anche omissivi, commessi o tentati, che costituiscano o possano costituire:

a) una violazione, o induzione ad una violazione, di leggi e regolamenti relativi in particolare ai seguenti ambiti:
   - appalti pubblici;
   - servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e finanziamento del terrorismo;
   - sicurezza e conformità dei prodotti;
   - protezione dei consumatori;
   - tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
   - salute pubblica;
   - tutela dell'ambiente;
   - violazioni delle norme in materia di concorrenza e di aiuti di Stato;
   - violazioni delle norme in materia di imposta sulle società;

b) una violazione, o induzione ad una violazione, di normativa interna, come:
   - valori e principi sanciti nel Codice Etico e di Comportamento di Sisal, nel Codice Etico di Flutter e in ogni altro Codice Etico adottato dalla Divisione International – con tale termine intendendosi la divisione territoriale del Gruppo *UK & Ireland, International, US e Australia* di cui la Società fa parte;
   - valori, principi e controlli individuati nel Modello di Organizzazione, Gestione e Controllo ex. D.lgs. 231/2001 di Sisal;

- policy e procedure interne di Sisal e del Gruppo, ivi inclusa la Policy Anticorruzione di Flutter; o

c) in generale, una violazione della normativa nazionale o europea, ivi inclusa quella relativa alle licenze di gioco o in tema di AML/CFT.

Per una esemplificazione più dettagliata delle condotte che possono costituire oggetto di segnalazione si rinvia all'Appendice A in calce alla presente Policy.

Le Segnalazioni che non rientrano nel campo di applicazione oggettivo come sopra individuato sono indirizzate ai dipartimenti competenti (ad es. segnalazioni di malfunzionamenti, richieste di informazioni sui prodotti, lamentele della clientela, ecc.).

DEFINIZIONI E ABBREVIAZIONI

CANALI PER LA SEGNALAZIONE: Canali di comunicazione individuati da Sisal, quali mezzi, interni o esterni all'organizzazione stessa, per veicolare le segnalazioni.

COMITATO SEGNALAZIONI o COMITATO: comitato composto da Internal Audit Director e Chief Risk & Compliance Officer, che sono stati altresì identificati come Confidential Designee di Sisal, per esprimere le opportune valutazioni in caso di Segnalazioni con Impatto Determinante aventi rilevanza a livello di capogruppo o divisionale (*i.e.* le *Material Impact and Serious Misconduct and Improper Behaviour* di cui alla "Whistleblower Policy" di Flutter).

COMPORTAMENTO ILLECITO: Qualsiasi azione o omissione che costituisce o potrebbe costituire una violazione o induzione ad una violazione relativamente alle condotte tra quelle di cui al paragrafo "SCOPO E AMBITO DI APPLICAZIONE".

CONFIDENTIAL DESIGNEE: secondo quanto previsto dalla "Whistleblower Policy" di Flutter, sono le persone a cui è conferita la responsabilità di gestire il processo di indagine delle segnalazioni.

ODV: Organismo di Vigilanza ex D.lgs. 231/2001, è coinvolto nelle valutazioni relative alle segnalazioni rilevanti ai sensi del D.Lgs. 231/01.

RITORSIONI: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato posto in essere in ragione della Segnalazione e che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto

SEGNALANTE: Soggetto, tra quelli di cui al paragrafo "DESTINATARI DELLA POLICY", che effettua la Segnalazione.

SEGNALAZIONE: Comunicazione del Segnalante avente a oggetto informazioni relative a Comportamenti Illeciti.

SEGNALATO: Soggetto a cui il Segnalante attribuisce il Comportamento illecito oggetto della Segnalazione.

SEGNALAZIONI CON IMPATTO DETERMINANTE: qualsiasi violazione normativa o delle politiche interne che si è verificata o è probabile che si verifichi (con una probabilità ≥50%) entro i prossimi tre anni e che potrebbe comportare un rischio grave, severo o critico per il Gruppo Flutter.

SERIOUS MISCONDUCT AND IMPROPER BEHAVIOUR **o SEGNALAZIONI DI VIOLAZIONI GRAVI E COMPORTAMENTI SCORRETTI**: (i) le Segnalazioni con Impatto Determinante, (ii) le Segnalazioni aventi ad oggetto condotte corruttive, (iii) le Segnalazioni

che possono determinare conseguenze sul piano reputazionale per il Gruppo con coinvolgimento di media, investitori o autorità, (iv) le Segnalazioni attinenti alle condizioni lavorative o a condotte scorrette sul posto di lavoro (ad esempio, minacce di violenza fisica, molestie sessuali, verbali o di altro tipo, discriminazione, ambiente ostile, conflitto di interessi o abuso di sostanze. Questo tipo di segnalazioni richiede lo svolgimento di un'istruttoria più approfondita.

DESTINATARI DELLA POLICY

La presente Policy si applica ai seguenti soggetti (di seguito anche "Destinatari" e/o "Segnalanti"):

a) i lavoratori del Gruppo (dipendenti, lavoratori autonomi, i volontari, i tirocinanti retribuiti e non retribuiti, ex dipendenti[1], candidati al lavoro[2]);
b) gli azionisti e i membri dell'organo di amministrazione, direzione o vigilanza di un'impresa, compresi i membri senza incarichi esecutivi, i volontari e i tirocinanti retribuiti e non retribuiti;
c) qualsiasi persona che lavora sotto la supervisione e la direzione di appaltatori, subappaltatori e fornitori, i clienti, i partner, i consulenti e, più in generale, gli stakeholder del Gruppo.

[1] Qualora segnalino o divulghino informazioni su violazioni acquisite nell'ambito del rapporto di lavoro cessato.

[2] Qualora il loro rapporto di lavoro non sia ancora iniziato e le informazioni riguardanti la violazione siano state acquisite durante il processo di selezione o nelle fasi delle trattative precontrattuali.

PRINCIPI GENERALI

Il sistema di Segnalazione è ispirato ai seguenti principi fondamentali:

- **Tutela dell'identità dei Segnalanti e della riservatezza delle informazioni**: a fronte della Segnalazione è sempre garantita la tutela e la riservatezza dell'identità del Segnalante, trattandone i dati in conformità alla legge e adottando ogni misura utile a prevenire la diffusione dei dati del Segnalante e del contenuto della Segnalazione.

  Sisal garantisce che l'identità del Segnalante non sia divulgata – senza il suo consenso esplicito – a nessuno che non faccia parte del personale autorizzato competente a ricevere e dare seguito alle Segnalazioni, a meno che la divulgazione rappresenti un obbligo necessario e proporzionato imposto dal diritto UE o nazionale.

  In particolare, l'obbligo di riservatezza viene meno nei casi in cui:

  (i) nell'ambito di un procedimento disciplinare, la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato; e

  (ii) la rivelazione dell'identità del Segnalante e delle informazioni da cui possa evincersi, direttamente o indirettamente, tale identità, è indispensabile anche ai fini della difesa della persona coinvolta.

  In tali ipotesi, è dato avviso al Segnalante, mediante comunicazione scritta, delle ragioni della rivelazione dei dati riservati. Inoltre, le Segnalazioni sono sottratte al diritto di accesso previsto, e per quanto applicabile al settore privato, dagli artt. 22 e ss. della L. n. 241/1990, nonchè dagli artt. 5 e ss. del D. Lgs. n. 33/2013. Le misure a tutela della riservatezza del Segnalante sono volte, tra l'altro, a garantire che lo stesso non sia soggetto ad alcuna forma di ritorsione.

Al di fuori dei casi sopra individuati, chiunque non rispetti l'obbligo di riservatezza sarà soggetto a provvedimenti disciplinari, fino al licenziamento, in accordo al sistema disciplinare vigente.

- **Divieto di atti ritorsivi o discriminatori verso i Segnalanti**: la Società proibisce ogni forma di ritorsione o discriminazione, attiva od omissiva, anche solo tentata o minacciata, posta in essere in ragione della Segnalazione e che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto. Tale protezione è garantita qualora la Segnalazione (anche se successivamente valutata infondata) sia stata comunicata in buona fede, in quanto il Segnalante aveva fondati motivi per ritenere che le informazioni sulle violazioni segnalate fossero vere al momento della segnalazione e che le stesse rientrassero nell'ambito di applicazione oggettivo di cui alla presente Policy.

  Per misure discriminatorie si intendono azioni disciplinari ingiustificate, molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili per il Segnalante; una esemplificazione di possibili misure discriminatorie è contenuta alla Appendice B alla presente Policy.

  Sisal garantisce la rimozione degli effetti di qualsiasi forma di ritorsione contro il Segnalante.

  La commissione di atti ritorsivi o discriminatori nei confronti di chiunque abbia effettuato una Segnalazione in conformità a quanto previsto dalla presente Policy comporta l'avvio di un procedimento disciplinare nei confronti dell'autore di tali atti e l'irrogazione delle relative misure disciplinari (che possono comportare il anche il licenziamento), conformemente a quanto previsto dalla normativa giuslavoristica nazionale applicabile, e sarà segnalata alle autorità competenti, secondo quanto

previsto dalla legislazione applicabile, e i relativi responsabili potranno essere soggetti a sanzioni civili e penali.

Si precisa inoltre che le misure sopra elencate a tutela delle persone Segnalanti si applicano altresì, ove opportuno ai soggetti e nelle situazioni di cui alla Appendice C. Pertanto, chiunque ritenga di aver subito una ritorsione/discriminazione per i motivi di cui sopra, deve inoltrare una segnalazione avente ad oggetto le ritorsioni/discriminazioni subite. La Società garantisce in tali casi lo svolgimento tempestivo delle relative indagini.

Il Segnalante non può essere considerato responsabile per diffamazione, violazione del diritto d'autore, degli obblighi di segretezza, delle norme in materia di protezione dei dati e di divulgazione dei segreti commerciali. Nessuna responsabilità può essere addebitata al Segnalante nemmeno in relazione alle condotte adottate per accedere alle informazioni oggetto di Segnalazione. Inoltre, i soggetti interessati hanno il diritto di tutelarsi legalmente qualora siano state riscontrate in capo al Segnalante responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o riportato.

Nel caso in cui, al contrario, le segnalazioni dovessero rivelarsi manifestamente infondate, effettuate con dolo o colpa grave, ovvero fosse accertata la responsabilità del Segnalante per i reati di diffamazione o di calunnia, tale condizione costituirebbe una violazione della presente *Policy*, con conseguente possibile applicazione di misure disciplinari e riconoscimento di responsabilità in capo al Segnalante; in tali casi le tutele nei confronti del Segnalante di cui al presente paragrafo non potrebbero essere garantite.

- **Tutela del Segnalato**: la Società tutela i soggetti segnalati per quanto attiene sia la

confidenzialità delle segnalazioni che li riguardano e delle eventuali indagini svolte, sia la protezione degli stessi da eventuali azioni ritorsive e/o diffamatorie.
A seguito di indagini sulla fondatezza della Segnalazione, il Comitato, qualora si apra un procedimento disciplinare, informa il soggetto cui la Segnalazione si riferisce, lo tiene aggiornato circa gli sviluppi del procedimento, compatibilmente con lo svolgimento delle attività di verifica e di raccolta delle prove necessarie, così da permettergli l'esercizio del diritto di difesa.
I dati personali del Segnalato possono essere trasmessi all'autorità amministrativa o giudiziaria competente e, più in generale, a soggetti pubblici, nel rispetto delle formalità di legge, ovvero per dare seguito a richieste pervenute dagli stessi.

- **Tutela dell'integrità delle segnalazioni**: la piattaforma *web* garantisce che nessuna segnalazione (dalla fase della notifica a quella della decisione) possa essere cancellata e/o alterata.

- **Dovere di indipendenza e professionalità nella gestione e valutazione delle Segnalazioni**: tutti i soggetti coinvolti, a qualsivoglia titolo, nel processo di gestione e valutazione delle Segnalazioni devono svolgere i relativi compiti nel rispetto dei doveri di indipendenza e garantendo l'accurata ed efficiente gestione e valutazione di tutte le segnalazioni. In particolare, l'organo deputato alla gestione delle segnalazioni è autonomo, dedicato e composto da personale specificamente formato per tale attività.

IL SISTEMA DI SEGNALAZIONE

Il sistema di segnalazione delle Società si compone dei seguenti canali:

a) piattaforma web accessibile 24/7 al seguente link [LINK] che garantisce la non tracciabilità e registrazione degli indirizzi IP dei Segnalanti;

b) linea telefonica registrata/sistema di messaggistica vocale registrato accessibile 24/7 al seguente numero di telefono 800761667; e

c) incontro diretto mediante richiesta al Comitato Segnalazioni.

La Società raccomanda l'invio delle Segnalazioni attraverso la piattaforma *web*, in quanto appositamente studiata per garantire al Segnalante facilità di utilizzo, riservatezza e confidenzialità e - in caso di Segnalazione anonima – consentire di chiedere chiarimenti al Segnalante, mantenendo il suo anonimato.

Se per la Segnalazione si utilizza la linea telefonica/sistema di messaggistica vocale registrati o si richiede un incontro diretto, il Comitato Segnalazioni può richiedere, previo consenso del Segnalante, di documentare la Segnalazione (a seconda dei casi tramite trascrizione integrale, registrazione della conversazione, resoconto dettagliato o verbale).

Al Segnalante è offerta la possibilità di verificare, rettificare e approvare, a seconda dei casi, la trascrizione, il resoconto o il verbale dell'incontro.

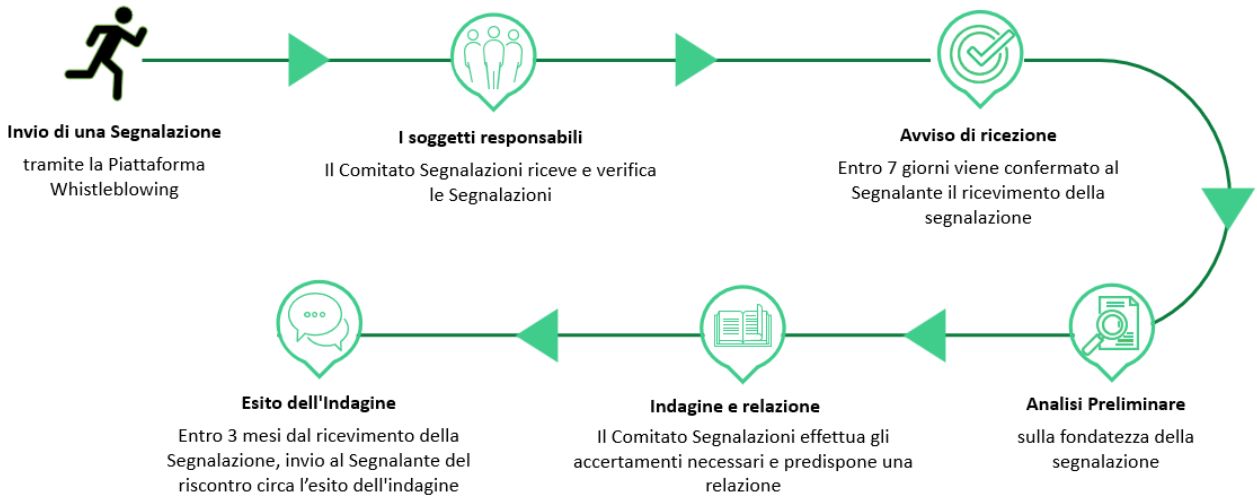
Si precisa che anche le trascrizioni, resoconti o verbali relativi alle Segnalazioni pervenute attraverso canali interni alternativi alla piattaforma *web* sono inseriti nella stessa a cura del Comitato Segnalazioni.

Per le fasi successive dell'*iter* di gestione di tali Segnalazioni, vale quanto descritto nei successivi paragrafi.

In ogni caso, chiunque riceva una Segnalazione attraverso canali diversi da quelli previsti dal sistema di Segnalazione deve prontamente - e non oltre 7 (sette) giorni dalla Segnalazione - inoltrarla in originale con gli eventuali allegati al Comitato Segnalazioni, il quale provvede a immetterla nella piattaforma *web*, con contestuale avviso della trasmissione al Segnalante.

La trasmissione deve avvenire nel rispetto dei criteri di massima riservatezza e con modalità idonee a tutelare il Segnalante e l'identità dei Segnalati, senza pregiudizio per l'efficacia delle successive attività di accertamento. Di tale Segnalazione non deve essere effettuata alcuna copia.

IL PROCESSO DI SEGNALAZIONE



Segnalazione di un comportamento illecito

Sisal incoraggia i soggetti di cui al paragrafo "DESTINATARI DELLA POLICY" a segnalare irregolarità o comportamenti illeciti, anche potenziali, di cui vengono a conoscenza utilizzando i canali previsti dal Sistema di Segnalazione, affinché possano essere oggetto di verifica da parte degli organi preposti.

La consapevolezza o il semplice sospetto di commissione di un comportamento illecito può manifestarsi nello svolgimento delle mansioni di competenza dei lavoratori del Gruppo nei rapporti con il personale interno o esterno, con le forze dell'ordine, con le agenzie di regolamentazione, con i clienti o con altre terze parti.

Le Segnalazioni possono essere effettuate in forma anonima, tuttavia Sisal raccomanda che le stesse siano nominative, al fine di consentire ai soggetti preposti una più efficiente attività di indagine, applicando in ogni caso le tutele previste contro eventuali ritorsioni In

ogni caso, qualora la Segnalazione sia anonima, tutti i soggetti coinvolti nella ricezione e/o valutazione della stessa adotteranno tutti gli accorgimenti necessari a garantire il rispetto dell'anonimato del Segnalante, astenendosi da qualunque tentativo di identificare il Segnalante o rivelarne l'identità, a meno che non sia richiesto dalla legge.

La Segnalazione deve essere effettuata in buona fede. Il Segnalante è invitato a fornire tutti gli elementi a sua conoscenza, utili per procedere alle dovute e appropriate verifiche a riscontro della fondatezza dei fatti oggetto di Segnalazione, allegando la documentazione a supporto del potenziale comportamento illecito oggetto di Segnalazione in possesso del Segnalante.

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

- una descrizione dettagliata dei fatti verificatisi e modalità con cui se ne è venuti a conoscenza;
- data e luogo in cui l'evento è accaduto;
- nominativo e ruolo delle persone coinvolte o elementi che possano consentirne l'identificazione;
- nominativi di eventuali altri soggetti che possano riferire sui fatti oggetto di Segnalazione o elementi che possano consentirne l'identificazione;
- riferimento ad eventuali documenti che possano confermare la fondatezza dei fatti riportati.

Il Segnalante deve avere cura di non riportare informazioni non pertinenti o non necessarie rispetto alla Segnalazione.

Le Segnalazioni prive dei requisiti sopra individuati vengono archiviate per mancanza degli elementi essenziali.

Tutte le Segnalazioni vengono ricevute e gestite dal Comitato Segnalazioni, nominati quali soggetti autorizzati al trattamento e debitamente istruiti in merito al trattamento dei dati personali ai sensi degli artt. 29 e 32 par. 4 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del d.lgs. 196 del 2003.

Il Comitato Segnalazioni informa l'OdV delle Segnalazioni afferenti al Modello ex D.lgs. 231/2001, in modo da garantire il coinvolgimento dell'OdV nella valutazione e decisione relativa a tale tipologia di Segnalazioni. Il Comitato Segnalazioni è responsabile dell'interazione con il Segnalante nel rispetto delle tempistiche di legge.

La Segnalazione volta a denunciare situazioni di natura esclusivamente personale ed estranee al perimetro delle previsioni di legge, non viene presa in considerazione.

Inoltre, se il Segnalante effettua una segnalazione può essere considerato responsabile nei casi in cui la Segnalazione risulti essere, per dolo o colpa grave, falsa, infondata e/o effettuata al solo scopo di danneggiare il Segnalato. Nei casi più gravi (es. dolo nella falsità della segnalazione), la condotta posta in essere può essere oggetto di procedimento disciplinare ai sensi della Legge n. 300/70 o causa di risoluzione del contratto o dell'incarico.

Piattaforma Whistleblowing

La Piattaforma Whistleblowing garantisce la tracciabilità del workflow della Segnalazione.

Tutte le informazioni della Segnalazione sono protette per garantire la massima riservatezza e accessibili solo dal Comitato o da soggetti espressamente autorizzati dallo stesso.

La Piattaforma è resa disponibile ai Destinatari attraverso il sito internet Speak Up! o tramite intranet aziendale. All'atto dell'invio della Segnalazione, previa presa visione dell'informativa sul trattamento dei dati personali, la Piattaforma Whistleblowing rilascia un token (ID Segnalazione), che può essere utilizzato dal Segnalante per avere informazioni circa l'esito della segnalazione e garantire le comunicazioni anche in totale anonimato.

Inoltre, la Piattaforma Whistleblowing prevede la possibilità per il Segnalante di escludere dalla gestione e valutazione della Segnalazione le Funzioni interne, qualora direttamente coinvolte nella Segnalazione. Per approfondimenti sulla gestione dei conflitti di interesse, si rimanda al paragrafo dedicato della presente Policy.

Il Comitato Segnalazioni accede alla Piattaforma per consultare tutte le Segnalazioni pervenute e svolgere le attività di pertinenza. Tutti gli accessi sono tracciati e la Piattaforma è protetta dalle opportune misure di sicurezza tecniche.

Segnalazioni ricevute al di fuori dei canali previsti

La Funzione di Sisal che riceva una Segnalazione transitata al di fuori dei canali previsti deve trasmetterla senza indugio, in originale con gli eventuali allegati, al Comitato Segnalazioni, che avrà cura di inserirla nella Piattaforma. La trasmissione deve avvenire nel rispetto dei criteri di massima riservatezza e con modalità idonee a tutelare il Segnalante e l'identità dei soggetti segnalati, senza pregiudizio per l'efficacia delle successive attività di

accertamento. Non deve essere effettuata alcuna copia, inoltro o stampa della Segnalazione ricevuta.

Analisi preliminare

Le Segnalazioni sono oggetto di analisi preliminare da parte del Comitato Segnalazioni, con l'eventuale coinvolgimento dell'OdV in caso di Segnalazioni rilevanti ex D.lgs. 231/2001. Il Comitato Segnalazioni verifica la presenza di dati e informazioni utili a consentire una prima valutazione della Segnalazione stessa. Entro 7 (sette) giorni dalla ricezione della Segnalazione, il Comitato invia al Segnalante un avviso di ricevimento della Segnalazione, utilizzando le modalità di comunicazione adottate dallo stesso in sede di Segnalazione.

Il Comitato, nell'ambito delle analisi preliminari e dell'esecuzione dell'indagine, tiene in considerazione l'eventuale sussistenza di temi comuni o accuse ripetute relative a un particolare dipartimento o individuo coinvolto in un'indagine.

Il Comitato adotta tutte le misure necessarie per trattare in modo confidenziale le Segnalazioni, anche al fine di tutelare l'identità del Segnalante, del Segnalato e degli altri soggetti menzionati nella Segnalazione.

Nel corso delle verifiche, il Comitato può avvalersi del supporto delle funzioni aziendali di volta in volta competenti (ad es. Funzione HR) e, ove ritenuto opportuno, di consulenti esterni specializzati nell'ambito della Segnalazione ricevuta ed il cui coinvolgimento è funzionale all'accertamento della Segnalazione, assicurando la riservatezza e l'anonimizzazione dei dati personali eventualmente contenuti nella Segnalazione.

Chiunque venga coinvolto nelle attività di verifica relative ad una Segnalazione è tenuto a prestare la massima collaborazione e ad attenersi alle indicazioni ricevute nello svolgimento delle proprie attività.

Tutti i soggetti coinvolti negli accertamenti devono mantenere la massima riservatezza riguardo le informazioni ricevute nel corso delle verifiche.

Al termine dell'analisi preliminare, il Comitato può:

a) archiviare la Segnalazione in quanto non sufficientemente supportata da prove, manifestamente infondata o relativa a comportamenti o fatti non rilevanti in relazione a questa Policy;
b) aprire la fase di indagini di cui al paragrafo successivo, coinvolgendo l'OdV in caso di Segnalazioni rilevanti ex D.lgs. 231/2001; o
c) coinvolgere il Confidential Designee di Flutter (o soggetto diverso qualora lo stesso versi a sua volta in situazione di conflitto di interesse) per le opportune valutazioni in caso di Segnalazioni con Impatto Determinante e/o di Violazioni Gravi e Comportamenti Scorretti o comunque ritenute dal Comitato rilevanti a livello di Gruppo.
   In caso di escalation al Confidential Designee di Flutter si applicheranno le regole previste dagli strumenti normativi Flutter in materia.

Nell'effettuare la valutazione circa la necessità di aprire la fase di indagini il Comitato deve considerare, tra gli altri, i seguenti elementi:

- l'identità del soggetto segnalato: ad esempio Segnalazioni effettuate nei confronti di un membro *senior* del personale del Gruppo potrebbero richiedere una indagine più ampia;
- la natura della violazione oggetto di Segnalazione: a seconda dei casi, potrà essere

opportuno includere nel *team* che prenderà parte all'indagine un membro senior del Dipartimento HR, Finance, a seconda dell'area di competenza; se necessario, consulenti esterni, esperti forensi o altre tipologie di professionisti potranno essere coinvolti nelle indagini da parte del Comitato;

- la circostanza che i fatti oggetto di Segnalazione riguardino una violazione in materia contabile oppure relativa ai controlli interni e internal auditing (in particolare se rilevante secondo il Sarbanes-Oxley Act o le regole imposte dalla SEC): questo tipo di Segnalazioni possono richiedere il coinvolgimento dell'Audit Committee di Flutter laddove necessario;
- la gravità della Segnalazione: più la Segnalazione appare grave, più accurata deve essere la relativa valutazione. Ad esempio, Segnalazioni relative a corruzione, integrità del bilancio o che minaccino la reputazione del Gruppo, che coinvolgano gli investitori o che o che riguardino le condizioni di impiego (violenza fisica, verbale, sessuale o molestie, discriminazioni, trattamenti ostili, conflitti di interessi o abuso di sostanze sul luogo di lavoro) richiederanno verosimilmente una valutazione più accurata.

Il Comitato informa il Segnalante riguardo l'esito degli accertamenti eseguiti entro un termine ragionevole, in ogni caso non superiore a 3 (tre) mesi.

Qualora dalla Segnalazione si desuma il verificarsi di una violazione di norme di legge o regolamento, con la preventiva autorizzazione/consultazione del Responsabile della Funzione Legal o di un consulente legale esterno e, laddove opportuno per le segnalazioni rilevanti a livello di Gruppo, in consultazione con il Board Audit or Risk and Sustainability Committee di Flutter, il Comitato può denunciare all'autorità competente tale circostanza.

Indagine

Con riferimento a ciascuna Segnalazione, laddove, a seguito delle analisi preliminari, emergano o siano comunque desumibili elementi utili e sufficienti ad effettuare una valutazione sulla fondatezza della Segnalazione medesima il Comitato provvede a:

- avviare analisi specifiche, coinvolgendo, ove opportuno, le funzioni aziendali interessate dalla Segnalazione;
- concludere l'istruttoria in qualunque momento, qualora, nel corso della stessa, sia accertata l'infondatezza della Segnalazione;
- verificare le possibili implicazioni legali a carico della Società;
- valutare se vi è un obbligo di informazione alle autorità;
- in caso di permanenza in essere della condotta denunciata, richiedere di assumere provvedimenti cautelari che conseguano la cessazione della condotta in atto.

In tale fase, il Comitato provvede a classificare la segnalazione in base alle opzioni presenti nella piattaforma Speak Up, che verrà poi eventualmente rivista a valle della chiusura dell'indagine.

Inoltre, il Comitato deve:

- assicurare che l'indagine sia accurata, equa, imparziale e tuteli la riservatezza dell'identità del Segnalante e delle persone coinvolte, incluso il soggetto Segnalato;
- garantire l'adozione di misure opportune per la raccolta, il trattamento e la conservazione di informazioni personali ed assicurare che le esigenze dell'indagine siano bilanciate con quella di tutela della privacy. Sul punto, è onere del Comitato

Segnalazioni valutare l'eventualità di informare il Segnalato circa l'indagine. Il Segnalato è, comunque, sempre informato dal Comitato Segnalazioni nel caso di avvio di un procedimento disciplinare;

- garantire che l'attività istruttoria sia svolta con la massima rapidità e diligenza.

Esito dell'indagine

All'esito della fase di verifica, il Comitato predispone una relazione riepilogativa delle indagini effettuate e delle evidenze emerse condividendola, in base agli esiti, con i soggetti di volta in volta competenti, ivi incluso l'OdV in caso di Segnalazioni rilevanti ex D.lgs. 231/2001, al fine di definire gli eventuali piani di intervento da implementare e le azioni da avviare a tutela della Società e del Gruppo, comunicando altresì i risultati degli approfondimenti e delle verifiche svolte relativamente a ciascuna Segnalazione ai responsabili delle strutture aziendali interessate dai contenuti della stessa.

Il Comitato classifica, all'interno della Piattaforma Whistleblowing, la Segnalazione analizzata in:

1. Segnalazione priva di indicazioni sufficienti e rilevanti;
2. Segnalazione non fondata;
3. Segnalazione fondata.

Qualora a conclusione delle analisi dovesse emergere l'assenza di elementi sufficientemente circostanziati o, comunque, l'infondatezza dei fatti richiamati nella Segnalazione, quest'ultima viene archiviata dal Comitato, unitamente alle relative motivazioni.

In caso di Segnalazione fondata, le eventuali azioni rimediali dovranno essere proporzionali all'infrazione commessa e tenere conto di: (i) la gravità della violazione; (ii) l'eventuale recidiva dell'autore della violazione; (iii) l'intento dell'autore della violazione; (iv) l'impatto della violazione sul personale del Gruppo, sulla funzione interessata e sul Gruppo in generale; e (v) le eventuali circostanze aggravanti o attenuanti. Qualsiasi provvedimento disciplinare deve essere adottato in conformità alla legislazione locale applicabile all'autore dell'infrazione.

Resta inteso che, in tutti i casi, al termine della verifica sulla fondatezza della Segnalazione ricevuta, al Segnalante viene fornito un riscontro entro un termine ragionevole, in ogni caso non superiore a 3 (tre) mesi.

CONFLITTO DI INTERESSE

La gestione e la valutazione della Segnalazione devono essere affidate in via esclusiva a soggetti che non si trovano in situazioni di conflitto di interesse. Pertanto:

a) se la situazione di conflitto di interessi si riferisce a uno o più membri del Comitato, tali membri non prendono parte alla gestione del caso ed i restanti membri del Comitato devono individuare altri soggetti idonei a ripristinare l'integrità del Comitato stesso;

b) se la situazione di conflitto di interesse riguarda la totalità dei membri del Comitato, la Segnalazione sarà attribuita alla competenza del Confidential Designee di Flutter. Nel caso in cui ciò non sia possibile, la Segnalazione sarà inoltrata al Group Director of Compliance o al Group Chief People Officer. In ogni caso i membri dell'OdV devono essere tenuti informati sugli sviluppi della gestione della segnalazione;

c) nel caso la Segnalazione si riferisca a uno o più membri dell'OdV, i soggetti in situazioni di conflitto non prendono parte alle valutazioni relative alla segnalazione e l'OdV stesso deve informare il Consiglio di Amministrazione che valuta le modalità operative da seguire e le Funzioni aziendali da coinvolgere nella gestione della Segnalazione.

Tali disposizioni trovano applicazione anche nell'ipotesi in cui il conflitto dovesse insorgere durante lo svolgimento degli accertamenti.

REPORTISTICA

Il Comitato, con periodicità trimestrale, fornisce al CEO, al Confidential Designee di Flutter e all'OdV un apposito report riepilogativo di tutte le segnalazioni gestite (archiviate e oggetto di accertamenti, contenente gli esiti delle analisi, inclusa l'adozione (o la mancata adozione) di provvedimenti disciplinari.

Inoltre, la Funzione Internal Audit fornisce all'OdV una reportistica mensile di dettaglio sull'evoluzione degli accertamenti e delle valutazioni inerenti le Segnalazioni rilevanti ex D.lgs 231/2001.

TRATTAMENTO DEI DATI PERSONALI

Si precisa che i dati personali del Segnalante, del Segnalato e di tutti i soggetti coinvolti nella Segnalazione sono trattati in conformità alla normativa vigente sulla protezione dei dati personali di cui al Regolamento (UE) 2016/679 ("GDPR") e del D.lgs. 196/2003, così come modificato dal D.lgs. 101/2018. In particolare, si evidenza in tale contesto che:

- le attività di trattamento sottese alla gestione della Segnalazione sono svolte nel rispetto dei principi dettati degli artt. 5 e 25 GDPR;
- il soggetto Segnalante riceve, prima di inviare la Segnalazione, un'informativa di cui all'art. 13 GDPR che specifica le finalità e modalità del trattamento dei propri dati personali ed il periodo di conservazione degli stessi, le categorie di destinatari a cui possono essere trasmessi i dati nell'ambito della gestione della Segnalazione e i diritti riconosciuti al Segnalante dal GDPR; al Segnalato è fornita altresì una informativa ex art. 14 GDPR in conformità agli obblighi di segretezza e di riservatezza imposti dal D.lgs. 231/2001, come modificato dalla Legge n. 179/2017, nonché in considerazione del rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento connesse alle segnalazioni nell'ambito del sistema di whistleblowing (cfr. art. 14, par. 5, lettere b) e d) del GDPR);
- come indicato nelle informative privacy rese agli interessati, i dati personali sono trattati per il tempo necessario al raggiungimento delle finalità che ne giustificano la raccolta e il trattamento (es.: valutazione e gestione della Segnalazione) e successivamente cancellati o anonimizzati in base ai tempi di conservazione definiti;
- sono messe in atto le misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali, in conformità alla normativa vigente, sia in fase di trasmissione della

Segnalazione, sia in fase di analisi, gestione e archiviazione della Segnalazione;

- l'esercizio dei diritti da parte del Segnalante o del Segnalato (soggetti "interessati" ai sensi della normativa privacy), in relazione ai propri dati personali trattati nell'ambito del processo di Whistleblowing, possono essere limitati, ai sensi e per gli effetti di cui all'articolo 2-undecies del D.lgs. 196/2003 come novellato dal D.lgs. 101/2018, nel caso in cui da un tale esercizio possa derivarne un pregiudizio effettivo e concreto ad altri interessi tutelati da specifiche disposizioni normative, con la precisazione che in nessuna circostanza può essere permesso al Segnalato di avvalersi dei propri diritti per ottenere informazioni sull'identità del Segnalante;
- l'accesso ai dati personali viene concesso solamente ai soggetti abilitati alla ricezione delle Segnalazioni, limitando la comunicazione a terzi delle informazioni riservate e dei dati personali soltanto quando ciò risulta necessario.

CONSERVAZIONE DELLA DOCUMENTAZIONE

Al fine di garantire la ricostruzione delle diverse fasi del processo, è cura del Comitato assicurare:

1. la tracciabilità delle Segnalazioni e delle relative attività di ricezione, archiviazione, istruttoria e valutazione mediante un sistema di log integrato nella piattaforma digitale, che tenga traccia della data e della modalità di ricezione della segnalazione, della relativa tipologia e dei risultati dell'indagine;
2. la conservazione della documentazione inerente alle Segnalazioni e le relative attività di verifica, nonché gli eventuali provvedimenti decisionali adottati dalle funzioni competenti, in appositi archivi e con gli opportuni livelli di sicurezza/riservatezza;
3. la conservazione della documentazione e delle Segnalazioni per il periodo di tempo prescritto per legge e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Le funzioni coinvolte nelle attività di riscontro della fondatezza della Segnalazione assicurano, ciascuna per quanto di competenza, la tracciabilità dei dati e delle informazioni e provvedono alla conservazione e archiviazione della documentazione prodotta in modo da consentire la ricostruzione delle diverse fasi del processo e in conformità alle regole di Gruppo sulla conservazione delle informazioni documentate.

CONDIZIONI PER L'EFFETTUAZIONE DELLA SEGNALAZIONE ESTERNA

Premesso che, come illustrato nella presente Policy, la Società ha predisposto idonei canali di segnalazione interna, conformi a quanto previsto dal D.Lgs. 24/2023, la segnalazione è consentita tramite il canale esterno attivato dall'Autorità Nazionale Anticorruzione ("ANAC"), solo nel caso in cui il Segnalante abbia:

a) già effettuato una segnalazione interna e la stessa non abbia avuto seguito;

b) fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero la stessa segnalazione possa determinare il rischio di ritorsione;

c) fondati motivi di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

In assenza dei presupposti sopra indicati, la segnalazione non viene gestita da ANAC e il soggetto non beneficia delle tutele di cui al D.lgs. 24/2023.

Il canale di segnalazione esterno attivato da ANAC è disponibile al seguente link: https://whistleblowing.anticorruzione.it/#/.

RESPONSABILE AGGIORNAMENTO DELLA POLICY

Responsabile della presente Policy è la Funzione Compliance & Safety, che provvede a un suo periodico aggiornamento, annualmente o ad evento per recepire eventuali modifiche organizzative e/o normative.

DIFFUSIONE E COMUNICAZIONE DELLA POLICY

La Società provvede a informare tutti i Destinatari della Policy della sua esistenza e del suo contenuto, pubblicandola sulla Intranet e sul sito internet di Sisal.

FORMAZIONE

La Funzione Risorse Umane, su input o di concerto con la Funzione Compliance & Safety, ha il compito di pianificare ed erogare attività formative relativa alla Policy e di garantire la disponibilità e la comunicazione della stessa.

APPENDICE A – OGGETTO DELLE SEGNALAZIONI

La Segnalazione può riguardare:

- violazioni effettive o sospette di normative o regolamenti applicabili, per esempio diritti dei dipendenti, requisiti in materia di licenze, ecc;
- violazioni effettive o sospette delle policy di Sisal, della Divisione e/o di Flutter;
- condotte penalmente rilevanti o che costituiscono illeciti civili, amministrativi o violazioni contabili;
- violazioni che coinvolgono legali rappresentanti, amministratori, dirigenti e/o dipendenti della Società [o società controllate, società non controllate nelle quali la Società detiene partecipazioni rilevanti], *joint venture* o - in ogni caso - chiunque agisca per conto della Società (es. consulenti, fornitori, ecc.);
- condotte che configurino potenziali conflitti di interessi;
- violazioni relative all'elusione dei controlli contabili interni o delle politiche contabili di Sisal, di Flutter e/o della Divisione International di appartenenza; ivi incluse a titolo esemplificativo e non esaustivo:
  - frodi o errori intenzionali nella preparazione, valutazione, revisione, audit o rendicontazione di qualsiasi bilancio e/o rendiconto finanziario della Società, della Divisione e/o di Flutter;
  - frodi o errori intenzionali nella registrazione e nella conservazione dei documenti finanziari della Società, della Divisione e/o di Flutter;
  - carenze o non conformità con i controlli contabili interni della Società, della Divisione e/o di Flutter;
  - mancata osservanza della legislazione o degli obblighi fiscali.

- dichiarazioni errate, incomplete o false in merito a al bilancio e/o contenuta nei registri finanziari, nelle relazioni finanziarie, nelle relazioni di revisione o nei rapporti sui rischi della Società, della Divisione e/o di Flutter; o
- problematiche che incidono sull'indipendenza della società di revisione contabile della Società, della Divisione e/o di Flutter;
- falsificazione, occultamento o distruzione di documenti aziendali o finanziari della Società, della Divisione e/o di Flutter;

- violazioni effettive o sospette delle leggi anticorruzione o delle Politiche anticorruzione della Società, della Divisione e/o di Flutter, ivi incluse le violazioni effettive o percepite delle regole relative alla erogazione e ricezione degli omaggi e ospitalità;
- potenziale o effettiva inosservanza delle norme antiriciclaggio e di lotta al finanziamento del terrorismo ("AML/CFT") e tutte le relative politiche e procedure della Società, della Divisione e/o di Flutter;
- presunte ritorsioni nei confronti di un Segnalante appartenente al personale della Società, della Divisione e/o di Flutter che abbia segnalato una questione segnalabile ai sensi della presente Policy;
- questioni che implicano una minaccia significativa per la salute e la sicurezza del Personale della Società, della Divisione, di Flutter e/o del pubblico (ad es. minacce di violenza fisica, molestie, discriminazione, bullismo, ambiente ostile comportamenti offensivi o abuso di sostanze che hanno un impatto sulla luogo di lavoro);
- condotte suscettibili di arrecare un pregiudizio patrimoniale o di immagine alla Società (ad es. frode, appropriazione indebita di beni o manipolazione di giochi/prodotti o sistemi interni per trarne un beneficio o un vantaggio indebito);

- danneggiamento di beni di Flutter, ad esempio causando intenzionalmente un danno o per grave negligenza;
- furti, incluso il furto di attrezzature o di denaro o di effetti personali dei dipendenti;
- qualsiasi questione che possa ricevere un’attenzione negativa da parte dei media o dell’opinione pubblica;
- questioni che possono essere giudicate significative o sensibili per altri motivi, come ad esempio un rischio o un incidente di cybersicurezza;
- qualsiasi altra situazione che possa destare preoccupazione e che sia stata comunicata al personale nell'ambito dei programmi di sensibilizzazione.

APPENDICE B – MISURE DISCRIMINATORIE

Possono costituire misure discriminatorie:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il demansionamento, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione;
- note di demerito o referenze negative;
- l'imposizione o amministrazione di misure disciplinari, la nota di biasimo o altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione, il trattamento svantaggioso o iniquo;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro permanente, laddove il lavoratore avesse legittime aspettative di vedersi offrire un impiego permanente;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- danni, anche alla reputazione della persona, in particolare sui social media, o la perdita finanziaria, comprese la perdita di opportunità economiche e la perdita di reddito;
- l'inserimento nelle liste nere sulla base di un accordo settoriale o industriale formale o informale, che possono comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto per beni o servizi;

- l’annullamento di una licenza o di un permesso;
- la sottoposizione ad accertamenti psichiatrici o medici.

APPENDICE C – TUTELE

Le tutele previste per il Segnalante di cui al § PRINCIPI GENERALI si applicano anche:

a) ai facilitatori (ossia coloro che prestano assistenza al Segnalante nel processo di Segnalazione);

b) a terzi connessi con il Segnalante e che potrebbero rischiare ritorsioni in un contesto lavorativo, quali colleghi o parenti del Segnalante;

c) ai soggetti giuridici di cui il Segnalante è proprietario, per cui lavora o a cui sono altrimenti connessi in un contesto lavorativo.

d) a chi abbia chiesto legittimamente pareri in relazione alla condivisione di informazioni in suo possesso, abbia espresso l'intenzione di fornire tali informazioni o abbia fornito informazioni o assistenza in merito a qualsiasi comportamento che possa ragionevolmente costituire una violazione di legge in ambito finanziario, anticorruzione o antifrode;

e) a chi abbia collaborato, archiviato, fatto archiviare, testimoniato, partecipato o altrimenti prestato assistenza in relazione a un'indagine o a un procedimento relativo a una violazione di legge in ambito finanziario, anticorruzione o antifrode, o abbia espresso l'intenzione di farlo;

f) a chi abbia fornito alle forze dell'ordine informazioni veritiere in merito alla possibile od effettiva commissione di un reato o di un'altra violazione di legge, a meno che tali soggetti non siano i responsabili di tali violazioni; oppure

g) a chi abbia collaborato, partecipato o fornito assistenza nelle fasi di indagine delle segnalazioni ai soggetti a ciò deputati.

Inoltre, le tutele di cui sopra si applicano anche qualora la segnalazione avvenga:

(i) quando il rapporto di lavoro non è ancora iniziato se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;

(ii) durante il periodo di prova; o

(iii) successivamente allo scioglimento del rapporto giuridico, se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.