

POLICY

PP-058 v.01

POLICY WHISTLEBLOWING DI MERCURY PAYMENT SERVICES
S.P.A.

FRONTESPIZIO

| | |
|----------------------------------|---|
| Titolo | Policy Whistleblowing di Mercury Payment Services S.p.A. |
| Classificazione | Policy |
| Codice documento | PP-058 |
| Approvato da | Consiglio di amministrazione di Mercury Payment Services S.p.A. |
| Data di approvazione | 31-07-2023 |
| Data di entrata in vigore | 31-07-2023 |

AGGIORNAMENTI

| Versione | Data | Codice | Aggiornamenti |
|----------|------------|--------|--|
| 1 | 31-07-2023 | PP-058 | Prima emissione La POG-044 Segnalazioni delle violazioni delle norme whistleblowing è abrogata Le istruzioni operative di dettaglio verranno emesse in sede di rilascio del canale di segnalazione interna |

INDICE

| | | |
|----|--|----|
| 1 | DEFINIZIONI | 4 |
| 2 | INTRODUZIONE | 5 |
| 3 | SCOPO E AMBITO DI APPLICAZIONE | 5 |
| 4 | PRESIDI A TUTELA DELLA RISERVATEZZA E TRATTAMENTO DEI DATI PERSONALI | 6 |
| 5 | PROTEZIONE DALLE RITORSIONI | 7 |
| 6 | SEGNALAZIONE INTERNA | 7 |
| 7 | CANALI DI SEGNALAZIONE ESTERNI | 10 |
| 8 | CONSERVAZIONE | 10 |
| 9 | FORMAZIONE | 11 |
| 10 | CONTROLLI SULL'ADEGUATEZZA DEL SISTEMA WHISTLEBLOWING..... | 11 |
| 11 | AGGIORNAMENTO DELLA POLICY | 11 |
| 12 | FLUSSI INFORMATIVI | 11 |
| 13 | ALLEGATI..... | 12 |

1 DEFINIZIONI

Si definisce:

| | |
|---|--|
| Capogruppo | Nexi S.p.A. o Nexi |
| Comitato Whistleblowing | Organo collegiale composto da: Presidente del Consiglio di Amministrazione e dal Presidente del Collegio Sindacale di Mercury Payment Services S.p.A. |
| Divulgazione pubblica | 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 |
| Facilitatore | Una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata |
| Gruppo | Gruppo Nexi |
| Gruppo di lavoro Whistleblowing (ad oggi non previsto) | Organo collegiale composto da un minimo di due soggetti tra cui preferibilmente il Responsabile della funzione Compliance ed il Responsabile della funzione Audit ove presenti. Altri membri ove presenti: Responsabile della funzione Antiriciclaggio, Responsabile della funzione Legale, Responsabile della funzione Risk Management, Responsabile della funzione Security, Vertici aziendali (es. managing director) individuati sulla base della governance delle società del gruppo |
| Responsabile Whistleblowing | Soggetto esterno che riceve le segnalazioni |
| Segnalazione interna | La comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna |
| Segnalazione esterna | La comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna |
| Società o MePS | Mercury Payment Services S.p.A. |
| Soggetto segnalante o Segnalante | Colui che effettua la segnalazione della violazione o una divulgazione pubblica |
| Soggetto coinvolto/ o segnalato | Colui che è oggetto della segnalazione |
| Violazione/i | Comportamenti, atti od omissioni che ledono l'interesse della Società |

2 INTRODUZIONE

Mercury Payment Services S.p.A. promuove una cultura aziendale basata sul comportamento etico e sulla buona governance, favorendo così un ambiente aziendale che incoraggi la segnalazione di comportamenti inaccettabili.

A tal fine, alla luce di quanto previsto dalla normativa esterna rilevante¹ nonché dalle Linee Guida ANAC, la Società adotta la presente Policy in materia di whistleblowing (di seguito anche "Policy"), applicabile alle segnalazioni circostanziate relative a violazioni inerenti alle attività di Mercury Payment Services S.p.A. e a condotte illecite o violazioni di norme che possano avere un impatto (ad esempio sanzionatorio, patrimoniale, reputazionale, ecc.) sulla Società ed anche sulle altre società del Gruppo Nexi.

In particolare, questo documento si propone di:

- promuovere un ambiente di lavoro che contribuisca a una comunicazione aperta e improntata alla tutela dei soggetti segnalanti (come di seguito identificati);
- definire un insieme di principi per tutelare l'integrità e la reputazione della Società e per prevenire o minimizzare i rischi legati alla segnalazione;
- delineare il quadro dei flussi informativi verso la Capogruppo.

La Policy è redatta in accordo con la normativa emanata dalla Capogruppo in materia, ed è approvata dal Consiglio di Amministrazione di Mercury Payment Services S.p.A. su proposta della Funzione Compliance di Gruppo per il tramite della Funzione Compliance Oversight.

3 SCOPO E AMBITO DI APPLICAZIONE

La presente Policy stabilisce le procedure per la segnalazione e la gestione delle seguenti Violazioni:

- illeciti in materia di: servizi, prodotti e mercati finanziari; prevenzione del riciclaggio e del finanziamento del terrorismo; protezione dei consumatori; tutela della vita privata e protezione dei dati personali; sicurezza delle reti e dei sistemi informativi; tutela dell'ambiente; appalti pubblici;
- frodi ai danni dello Stato o della UE;
- violazioni in materia di concorrenza e di imposta sulle società;
- illeciti rilevanti ai sensi del D.Lgs. 231/2001 e violazioni del Modello di organizzazione e gestione definito e del relativo Codice Etico;
- violazioni del diritto del lavoro (es. molestie, bullismo/ mobbing, ecc.).

Le segnalazioni devono essere riferite solo a Violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nei suddetti ambiti. In particolare, si evidenzia che per effettuare la Segnalazione non è necessario disporre di prove della violazione ma almeno di informazioni sufficientemente circostanziate che facciano ritenere ragionevole l'invio della segnalazione (fondati sospetti).

Inoltre, qualora la persona che effettua la segnalazione abbia un interesse privato o diretto nella segnalazione (es. qualora sia corresponsabile del fatto o parte lesa dalla condotta del soggetto segnalato), deve darne evidenza nella comunicazione.

Si evidenzia che non sono ricomprese tra le informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio).

¹ In particolare: D. Lgs. 24/2023; art. 4-undecies TUF, art. 6 D. Lgs. 231/2001, art. 48 D. Lgs. 231/2007

I destinatari della presente Policy sono:

- dipendenti assunti² con un contratto a tempo indeterminato o determinato, full time o part time, personale in somministrazione lavoro o staff leasing, stagisti, consulenti che prestano la loro attività presso la Società e collaboratori che operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale;
- ex dipendenti, se le informazioni sulle Violazioni sono state acquisite nel corso del rapporto stesso;
- persone il cui rapporto di lavoro non è ancora iniziato, nei casi in cui le informazioni riguardanti una Violazione sono state acquisite durante il processo di selezione o altre fasi delle trattative precontrattuali e contrattuali;
- azionisti e le persone appartenenti all'organo di amministrazione, di direzione o di vigilanza della Società, compresi i membri senza incarichi esecutivi;
- volontari e tirocinanti retribuiti o non retribuiti;
- fornitori, appaltatori e subappaltatori, e qualsiasi persona che lavora sotto la supervisione e la direzione di tali soggetti.

MePS si impegna a promuovere un ambiente di lavoro che contribuisca a una comunicazione aperta riguardo alle proprie pratiche aziendali e a proteggere il Segnalante, Facilitatore, colleghi e familiari del Segnalante e gli enti di proprietà del Segnalante da ritorsioni e discriminazioni per aver correttamente rivelato o segnalato condotte illegali o comportamenti che violano o potenzialmente violano le aree che rientrano nell'ambito della presente Policy.

Le questioni segnalate saranno gestite in modo strettamente confidenziale e trattate con la dovuta diligenza, come meglio descritto nei successivi paragrafi.

4 PRESIDI A TUTELA DELLA RISERVATEZZA E TRATTAMENTO DEI DATI PERSONALI

La Società pone in essere adeguati presidi a tutela del Segnalante, del Facilitatore nonché delle persone del medesimo contesto lavorativo, colleghi, familiari del Segnalante.

In particolare, sono attivi canali di segnalazione interna che garantiscono la riservatezza dell'identità del Segnalante e di tutti i soggetti a vario titolo coinvolti, nonché del contenuto della segnalazione e della relativa documentazione.

La riservatezza è garantita anche quando la segnalazione effettuata ai sensi della presente Policy viene inviata attraverso modalità diverse da quelle istituite dalla Società o a soggetti diversi da quelli autorizzati e competenti a gestire le segnalazioni (si veda paragrafo 6.3). In tal caso, il soggetto che ha ricevuto la segnalazione provvede a trasmetterla tempestivamente al soggetto competente, dandone notizia al Segnalante.

L'identità del Segnalante – e qualsiasi altra informazione da cui possa evincersi – può essere rivelata a persone diverse da quelle competenti a ricevere e a dare seguito alla segnalazione, solo con il consenso espresso del Segnalante oppure quando obbligatorio o legittimo ai sensi della normativa applicabile. In casi eccezionali, qualora la rivelazione dell'identità del Segnalante sia indispensabile (es. nell'ambito di indagini avviate dall'Autorità o di procedimenti giudiziari), sarà comunque fornita una comunicazione scritta al Segnalante sulle ragioni che giustificano la comunicazione.

Si evidenzia che, nel caso in cui le segnalazioni siano oggetto di denuncia alle Autorità, l'obbligo di riservatezza dell'identità delle persone coinvolte o menzionate nella segnalazione potrebbe venire meno alle condizioni e nelle modalità previste dalla normativa rilevante.

Per maggiori informazioni sul trattamento dei dati personali effettuato dalla Società nell'ambito della ricezione e della gestione delle segnalazioni, si prega di prendere visione dell'informativa sul trattamento dei dati personali ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679 ("GDPR") e della normativa nazionale vigente in materia di protezione dei dati personali, pubblicata in una sezione dedicata del sito della Società. Tale informativa si applica al trattamento dei dati personali di tutti i soggetti che possono a vario titolo essere acquisiti da MePS per via di una

² Le tutele delle persone segnalanti si applicano anche durante il periodo di prova

segnalazione (Segnalante, Segnalato, Persone coinvolte, altri soggetti menzionati nella segnalazione).

In ogni caso, il trattamento dei dati personali effettuato dalla Società nell'ambito della ricezione e della gestione delle segnalazioni è svolto in conformità con le disposizioni del GDPR e della normativa nazionale vigente in materia di protezione dei dati personali.

5 PROTEZIONE DALLE RITORSIONI

MePS, nel promuovere un ambiente di lavoro che contribuisca alla diffusione di una comunicazione aperta, assicura la protezione da ritorsioni e discriminazioni.

Si evidenzia che le seguenti tutele valgono per i soggetti che effettuano segnalazioni interne ed esterne, divulgazioni pubbliche e denunce all'Autorità, qualora siano rispettate le condizioni previste dalla normativa applicabile.

In particolare, la Società non tollera ritorsioni o punizioni - anche tentate o minacciate - di alcun tipo nei confronti dei soggetti che segnalano in buona fede o che assistono MePS nelle indagini su qualsiasi violazione segnalata ai sensi della presente Policy. Ciò include qualsiasi rimprovero, rappresaglia, cambiamento di mansioni lavorative, cambiamento di condizioni di impiego, cambiamento delle previsioni di segnalazione, danni relativi alle prospettive di carriera o reputazionali, minacce di fare una delle suddette o omissioni intenzionali che possono danneggiare il dipendente.

Pertanto, qualora il Segnalante, a seguito dell'accertamento della Segnalazione, ritenga di aver subito condotte ritorsive, può inoltrare una nuova segnalazione – non anonima – avente ad oggetto le ritorsioni subite affinché siano adottati i provvedimenti necessari per ripristinare la situazione e/o per rimediare alle conseguenze negative connesse alla discriminazione, nonché avviare tutti i provvedimenti che saranno ritenuti necessari, eventualmente anche disciplinari. In alternativa, il Segnalante può valutare di trasmettere una segnalazione esterna, come meglio descritto nei successivi paragrafi.

Sono protetti dalle ritorsioni anche i Facilitatori, i colleghi e i familiari del Segnalante e gli enti di proprietà del Segnalante.

I soggetti che pongono in essere una falsa segnalazione contro qualcuno con dolo e/o colpa grave, non saranno protetti dalla presente Policy. In particolare, tali soggetti potranno essere destinatari di sanzioni civili, penali e amministrative, nonché azioni disciplinari, compreso il licenziamento.

6 SEGNALE INTERNA

6.1 IL RESPONSABILE WHISTLEBLOWING

La Società individua quale Responsabile Whistleblowing un soggetto esterno, dotato di un livello adeguato di competenze, autorità, imparzialità e indipendenza.

In particolare, il Responsabile Whistleblowing, come meglio descritto al paragrafo 6.3:

- rilascia al Segnalante un avviso di ricevimento della Segnalazione entro sette giorni dalla data di ricezione;
- mantiene le interlocuzioni con il Segnalante;
- dà un corretto seguito alle Segnalazioni ricevute;
- fornisce un riscontro alla persona segnalante, entro tre mesi dalla data di avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Il Responsabile Whistleblowing viene nominato quale responsabile del trattamento dei dati in base ad un accordo appositamente stipulato con la Società e, pertanto, ha accesso a tutte le informazioni e ai dati personali relativi alle segnalazioni ricevute in conformità alle disposizioni della normativa applicabile.

6.2 MODALITÀ DI EFFETTUAZIONE DELLE SEGNALAZIONI

Il soggetto che sa, sospetta o ha ragionevoli motivi per sospettare che sia stata commessa o sia in corso una Violazione può effettuare una Segnalazione attraverso uno o più dei seguenti canali:

- tramite apposita piattaforma elettronica³ adottata dalla Società, che consente di effettuare la Segnalazione sia in forma scritta sia in forma orale (tramite un sistema di messaggistica vocale);
- su richiesta del Segnalante, attraverso un incontro diretto con il Responsabile Whistleblowing, fissato entro 7 giorni da quando è pervenuta la richiesta.

Le Segnalazioni in forma orale, previo consenso del Segnalante, saranno analizzate dal Responsabile Whistleblowing mediante registrazione su dispositivo idoneo alla conservazione e all'ascolto, oppure mediante trascrizione integrale, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali. In caso di trascrizione, il Segnalante può verificare, rettificare o confermare il contenuto della trascrizione con la propria firma. La segnalazione trascritta è adeguatamente protocollata e conservata dal Responsabile Whistleblowing, come meglio descritto nel paragrafo 8.

Ove possibile, può essere utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di Segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Le segnalazioni si auspicano essere nominative; la Società non intende incoraggiare segnalazioni anonime avendo posto in essere tutte le garanzie atte a tutelare il Segnalante. Si precisa che l'anonimato limita la possibilità di investigare efficacemente non essendo possibile instaurare un rapporto diretto con il Segnalante e, per tale motivo, è necessario che tale segnalazione sia il più possibile chiara e dettagliata per facilitare i necessari approfondimenti.

Come descritto in precedenza, MePS ha adottato un canale digitale - supportato da strumenti di crittografia - per la gestione delle Segnalazioni. La piattaforma digitale garantisce che le segnalazioni siano trattate in forma riservata. Inoltre, al Segnalante non viene chiesto di fornire informazioni personali, a meno che non sia lui stesso a scegliere di farlo. La riservatezza dell'identità del Segnalante e di qualsiasi terzo menzionato nella segnalazione è protetta. Il sistema impedisce l'accesso a personale non autorizzato. Tutte le informazioni presenti sulla piattaforma possono essere consultate e trattate solo dal Responsabile Whistleblowing e sono trattate con la massima riservatezza.

La piattaforma elettronica per il whistleblowing genererà un numero identificativo univoco per ciascun Segnalante al fine di utilizzare la piattaforma di Segnalazione in modalità sicura. Tale piattaforma consente al Responsabile Whistleblowing di comunicare con il Segnalante, se sono necessarie ulteriori informazioni, senza rivelare la sua identità. Quando si utilizza la piattaforma di Segnalazione, gli indirizzi IP non possono essere tracciati.

Qualora la Segnalazione interna sia presentata ad un soggetto diverso dal Responsabile Whistleblowing, laddove il Segnalante dichiara espressamente di voler beneficiare delle tutele in materia whistleblowing (es. se una Segnalazione perviene in busta chiusa sulla quale è indicato che si tratta di una segnalazione di whistleblowing) o tale volontà sia desumibile dalla Segnalazione, la stessa deve essere considerata "segnalazione whistleblowing" e va trasmessa, entro sette giorni dal suo ricevimento, al Responsabile Whistleblowing, dando contestuale notizia della trasmissione alla persona segnalante.

6.3 IL PROCESSO DI GESTIONE DELLA SEGNALAZIONE INTERNA

Nei successivi paragrafi viene descritto il processo di gestione delle segnalazioni interne, che presenta limitate differenze sulla base del soggetto segnalato.

Si evidenzia che, secondo quanto previsto dalla normativa rilevante, il Responsabile Whistleblowing è tenuto a fornire un riscontro⁴ al Segnalante entro tre mesi dalla data di avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione.

Il set documentale e informativo relativo alla Segnalazione e alle analisi effettuate è conservato in apposite cartelle di rete ad accesso riservato.

Al momento della ricezione della Segnalazione, il Responsabile Whistleblowing provvede a trasmettere la conferma di ricevimento della Segnalazione al Segnalante entro e non oltre sette giorni dalla ricezione della stessa.

³ Si precisa che le informazioni presenti in tale piattaforma sono accessibili e consultabili unicamente dal Responsabile Whistleblowing]

⁴ Si precisa che per 'riscontro' si intende la comunicazione alla persona segnalante delle informazioni relative al seguito che viene dato o che si intende dare alla Segnalazione

Successivamente, il Responsabile Whistleblowing informa il Comitato Whistleblowing affinché effettui le analisi necessarie.

Si precisa che, nel caso in cui il soggetto segnalato sia un membro del Comitato Whistleblowing, quest'ultimo non verrà informato dal Responsabile Whistleblowing.

Il Comitato Whistleblowing analizza la Segnalazione ricevuta al fine di verificarne l'ammissibilità ai sensi della normativa rilevante (es. se è chiara, sufficientemente circostanziata, rientra nell'ambito di applicazione, ecc.). In particolare, è necessario che nella Segnalazione risultino chiare: (i) le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione; (ii) la descrizione del fatto; (iii) le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Ove quanto segnalato non sia adeguatamente circostanziato, il Responsabile Whistleblowing può chiedere elementi integrativi al Segnalante tramite la piattaforma elettronica o anche di persona, ove il Segnalante abbia richiesto un incontro diretto.

Qualora la Segnalazione sia considerata non ammissibile, il Comitato Whistleblowing ne dispone l'archiviazione, dando informativa a:

- Responsabile Whistleblowing, affinché dia riscontro al Segnalante;
- Consiglio di Amministrazione e Collegio Sindacale della Società, nel caso in cui il soggetto segnalato sia Amministratore Delegato ("AD"), amministratore o sindaco.

Qualora, invece, il Comitato Whistleblowing ritenga che la Segnalazione sia ammissibile, provvede - con il supporto del Responsabile Whistleblowing - a verificarne la rilevanza ai sensi del D.Lgs. 231/01 (es. riguardi uno dei reati presupposto previsti dal citato decreto o una violazione del modello adottato dalla Società) e, nel caso, ne dà tempestiva comunicazione all'Organismo di Vigilanza.

Successivamente, laddove emerga la necessità di effettuare approfondimenti/ indagini interne, il Comitato Whistleblowing dà incarico a un soggetto esterno⁵ affinché svolga gli accertamenti del caso.

Al termine dell'istruttoria, il Comitato Whistleblowing predisponde una nota illustrativa contenente le risultanze degli approfondimenti effettuati nonché una proposta di eventuali azioni da intraprendere (es. archiviazione della segnalazione, avvio di procedimento disciplinare nei confronti del soggetto segnalato (qualora sia un dipendente), avvio di azioni di responsabilità/ legali, individuazione di eventuali presidi volti a evitare per il futuro il ripetersi di tali eventi ecc.) e invia tale nota a (i) Organismo di Vigilanza, qualora la segnalazione sia rilevante ai fini 231/01 e (ii) Consiglio di Amministrazione affinché il consiglio valuti e decida - con l'eventuale coinvolgimento delle funzioni specialistiche di volta in volta identificate sulla base dell'ambito - le azioni da porre in essere.

A seguito della decisione del Consiglio di Amministrazione, il Comitato Whistleblowing provvede a dare indicazione al Responsabile Whistleblowing affinché fornisca un riscontro al Segnalante.

Inoltre, è trasmessa un'informativa all'Organismo di Vigilanza, qualora la segnalazione sia rilevante ai fini 231/01, e ai seguenti soggetti/ organi, sulla base del soggetto segnalato:

Soggetto segnalato: AD, amministratore o sindaco

- Consiglio di Amministrazione, Collegio Sindacale e Comitato Controllo e Rischi della Capogruppo, qualora la Segnalazione risulti fondata e sia stata deliberata un'azione da intraprendere.

Soggetto segnalato: restanti casi

- Amministratore delegato
- Responsabile della funzione HR;
- Collegio Sindacale della Società;
- Consiglio di Amministrazione, Collegio Sindacale e Comitato Controllo e Rischi della Capogruppo, nel caso in cui vengano decise azioni da intraprendere e il Consiglio di Amministrazione della Società deliberi di

⁵ La Società dispone un apposito budget per il ricorso a soggetti esterni

inviare tale informativa.

6.4 GESTIONE DEL CONFLITTO D'INTERESSE

Nel caso in cui la Segnalazione riguardi uno dei membri del Comitato Whistleblowing, il soggetto segnalato non verrà informato della Segnalazione ricevuta e non sarà coinvolto nella gestione della stessa.

In ogni caso, qualora in fase di analisi della Segnalazione emerga che la stessa veda coinvolti soggetti informati a vario titolo nel processo di gestione della segnalazione (es. il responsabile della funzione HR; Presidente o membro dell'OdV; ecc.), tali soggetti dovranno essere esclusi dal processo.

7 CANALI DI SEGNALAZIONE ESTERNI

La normativa rilevante prevede che i Segnalanti possano fornire informazioni sulle Violazioni utilizzando canali esterni, al ricorrere di una delle seguenti condizioni:

1. la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
2. il Segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito (es. potenziale conflitto d'interesse) ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
3. il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Di seguito si riportano i canali di segnalazione attualmente attivati dalle Autorità di vigilanza competenti sull'attività di MePS. È opportuno consultare direttamente i siti internet delle Autorità per verificare eventuali ulteriori condizioni per la segnalazione esterna e aggiornamenti sui canali di segnalazione:

| Autorità | Sito di riferimento |
|----------------|---|
| Anac | Whistleblowing – www.anticorruzione.it |
| Banca d'Italia | https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/index.html |
| Consob | http://www.consob.it/web/area-pubblica/whistleblowing |
| AGCM | https://www.agcm.it/servizi/whistleblowing |

I destinatari della presente policy possono anche scegliere di effettuare 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 persone. La Divulgazione Pubblica delle Violazioni deve avvenire nel rispetto delle condizioni⁶ poste dalla normativa rilevante affinché il Segnalante possa beneficiare delle tutele riconosciute.

8 CONSERVAZIONE

Tutti i documenti relativi alle segnalazioni devono essere conservati in conformità alle leggi e alle normative vigenti e alle politiche e procedure di MePS e del Gruppo Nexi. In particolare, in ottemperanza alle disposizioni di legge

⁶ Una persona che effettua una divulgazione pubblica beneficia della protezione prevista dal decreto whistleblowing se ricorre una delle seguenti condizioni:

- a) La persona segnalante ha prima segnalato internamente ed esternamente, o direttamente esternamente conformemente a quanto disposto dal decreto, ma non è stata intrapresa un'azione appropriata in risposta alla segnalazione entro il termine indicato dalla normativa rilevante; oppure
- b) La persona segnalante aveva fondati motivi di ritenere che: (i) la violazione possa costituire un pericolo imminente o palese per il pubblico interesse, come nel caso in cui sussista una situazione di emergenza o il rischio di danno irreversibile; oppure (ii) In caso di segnalazione esterna, sussista il rischio di ritorsioni o le prospettive che la violazione sia affrontata efficacemente siano scarse per via delle circostanze del caso di specie, come quelle in cui possano essere occultate o distrutte prove oppure in cui un'autorità possa essere collusa con l'autore della violazione o coinvolta nella violazione stessa.

vigenti e applicabile, le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Se i documenti possono essere rilevanti per qualsiasi controversia, inchiesta o indagine in corso o potenziale, le informazioni non devono essere distrutte e devono essere conservate per la durata di tale controversia, inchiesta o indagine e successivamente, se necessario, in conformità alle leggi, ai regolamenti o alle politiche e procedure di MePS.

9 FORMAZIONE

La Funzione People Development & Talent assicura, con la collaborazione del Funzione Compliance di Gruppo per il tramite della Funzione Compliance Oversight, la diffusione e il rafforzamento della conoscenza del sistema whistleblowing attraverso attività di sensibilizzazione, informazione e formazione del personale aziendale.

A tal fine, la Funzione People Development & Talent, per quanto di propria competenza e in coordinamento con il Funzione Compliance di Gruppo, individua i fabbisogni formativi in ambito whistleblowing anche tenuto conto di cambiamenti organizzativi, criticità specifiche riscontrate o requisiti normativi esterni.

Inoltre, sono previsti, ove necessario, corsi di formazione specifici (che prevedano, ad esempio, l'analisi di casi concreti) per i membri del Comitato Whistleblowing.

Con cadenza periodica, la Funzione Compliance di Gruppo per il tramite della Funzione Compliance Oversight monitora la fruizione dei programmi e percorsi di formazione.

10 CONTROLLI SULL'ADEGUATEZZA DEL SISTEMA WHISTLEBLOWING

La funzione Audit della Capogruppo - con il supporto delle strutture competenti/ soggetti esterni, ove necessario - effettua controlli periodici sull'adeguatezza e la tenuta del processo whistleblowing (es. test del tool; audit su

processo di gestione delle segnalazioni interne; verifiche tempistica di evasione; ecc.).

La funzione Compliance della Capogruppo, per il tramite della Funzione Compliance Oversight, assicura nel continuo la conformità del processo (attività ex ante).

11 AGGIORNAMENTO DELLA POLICY

La Funzione Compliance della Capogruppo, per il tramite della Funzione Compliance Oversight periodicamente valuta eventuali modifiche da apportare alla presente Policy e, se del caso, provvede a sottoporla all'approvazione del Consiglio di Amministrazione.

12 FLUSSI INFORMATIVI

Su base annuale, il Comitato Whistleblowing della Società predisponde una relazione contenente i casi⁷, le risultanze delle analisi effettuate e gli andamenti delle segnalazioni ricevute nel periodo di riferimento.

Tale reportistica è trasmessa ai seguenti destinatari:

- Consiglio di Amministrazione;
- Amministratore Delegato;
- Collegio Sindacale;

⁷ Non devono essere fornite informazioni relative all'identità del Segnalante

- Organismo di Vigilanza.

Inoltre, il Comitato Whistleblowing della Società provvede a trasmettere alla funzione Compliance di Capogruppo – per il tramite della Compliance Oversight – un report di sintesi sulla gestione delle segnalazioni, affinché provveda a inviarlo al Consiglio di Amministrazione, Collegio Sindacale e Comitato Controllo e Rischi della Capogruppo.

13 ALLEGATI

Allegato 1 – Flowchart del processo di gestione della segnalazione