

REAL MONEY EUROPE

Banco Metalli

PROCEDURA WHISTLEBLOWING

Sistema di Segnalazione delle Violazioni

ai sensi del Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, e della Direttiva (UE) 2019/1937

1. Cos'è il Whistleblowing e Perché è Importante

Il whistleblowing è la segnalazione, da parte di una persona — lavoratore, collaboratore, cliente o altro soggetto — di comportamenti illeciti, irregolari o non conformi alla normativa di cui sia venuta a conoscenza nell'ambito di un contesto lavorativo o di una relazione professionale o commerciale.

Real Money Europe LIMITED (di seguito "Real Money Europe" o "la Società"), in qualità di Banco Metalli, ha adottato il presente Sistema di Whistleblowing convinta che la segnalazione tempestiva di eventuali violazioni sia uno strumento fondamentale per:

- Prevenire condotte illecite o non conformi prima che producano danni;
- Proteggere i clienti, i lavoratori e l'integrità dell'attività di compravendita di metalli preziosi;
- Promuovere una cultura aziendale basata su legalità, correttezza e trasparenza;
- Adempiere agli obblighi previsti dal Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, e dalla Direttiva (UE) 2019/1937, nonché adottare le best practice internazionali in materia di governance.

Il Sistema di Whistleblowing della società è adottato in conformità Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, e alla Direttiva (UE) 2019/1937 e costituisce, per un Banco Metalli per Real Money Europe LIMITED, in qualità di Banco Metalli, una scelta volontaria di best practice in materia di governance, legalità e trasparenza, coerente con gli standard più elevati del settore dei metalli preziosi e con gli obblighi AML/CFT previsti dalla normativa vigente.

Il Sistema adottato dalla Società si basa su strumenti che garantiscono la massima riservatezza dell'identità del segnalante, la protezione dei dati personali e il divieto assoluto di ritorsioni di qualsiasi natura nei confronti di chi effettua una segnalazione in buona fede.

1.2 Obiettivi del sistema di whistleblowing

Il Sistema di Whistleblowing della società persegue i seguenti obiettivi fondamentali:

- Prevenzione: individuare tempestivamente condotte non conformi o potenzialmente lesive dell'integrità aziendale;
- Protezione: tutelare i segnalanti da qualsiasi forma di ritorsione o discriminazione;
- Trasparenza: garantire un processo chiaro, definito e accessibile ai soggetti legittimati;
- Miglioramento continuo: utilizzare le segnalazioni come strumento di rafforzamento dei presidi di conformità;
- Conformità normativa: assicurare il rispetto della normativa vigente.

1.3 Ambito di applicazione

Il presente documento disciplina il sistema di whistleblowing della Società e, in particolare:

- a) definisce il sistema di gestione delle segnalazioni ai sensi della normativa applicabile;

- b) stabilisce i ruoli e le responsabilità organizzative in materia di gestione delle segnalazioni;
- c) disciplina le attività di formazione e sensibilizzazione del personale;
- d) implementa un sistema di whistleblowing conforme alla Direttiva (UE) 2019/1937 e al Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022;
- e) garantisce la protezione dei segnalanti e la corretta gestione delle segnalazioni di violazioni normative.

1.4 Principi guida

Il Sistema di Whistleblowing di Real Money Europe si fonda sui seguenti principi:

- riservatezza dell'identità del segnalante;
- divieto di ritorsioni di qualsiasi natura;
- accesso al sistema tramite canale interno unico (piattaforma MITWhistle);
- tempestività nella gestione e riscontro delle segnalazioni;
- proporzionalità delle azioni rispetto alla gravità delle violazioni;
- tracciabilità delle segnalazioni e delle attività di gestione.

1.5 Definizioni

Ai sensi del Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, si intende per:

Termine	Definizione
Segnalante	La persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo
Segnalazione interna	La comunicazione scritta od orale di informazioni sulle violazioni, effettuata tramite il canale di segnalazione interno attivato dalla Società ai sensi della normativa applicabile
Segnalazione esterna	La comunicazione di informazioni sulle violazioni effettuata attraverso i canali esterni previsti dal Protected Disclosures Act 2014, inclusi, ove applicabile, i soggetti designati (<i>prescribed persons</i>) e il Protected Disclosures Commissioner
Segnalazione protetta	La segnalazione di informazioni che, secondo il ragionevole convincimento del segnalante, tendono a dimostrare una violazione rilevante e che sono state acquisite nell'ambito di un contesto lavorativo, effettuata secondo le modalità previste dal Protected Disclosures Act 2014, come modificato
Divulgazione pubblica	Il rendere di pubblico dominio informazioni sulle violazioni tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone, nei casi e nelle condizioni previsti dalla normativa applicabile
Violazioni	Le azioni od omissioni, commesse o che potrebbero essere commesse, che rientrano nella nozione di violazione rilevante ai sensi del Protected Disclosures Act 2014, come modificato, tra cui, in particolare, la commissione di reati, l'inosservanza di obblighi di legge, errori giudiziari, pericoli per la salute o la sicurezza, danni all'ambiente, determinate violazioni del diritto dell'Unione europea e l'occultamento o la distruzione di informazioni relative a tali violazioni
Informazioni sulle violazioni	Informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che potrebbero essere commesse nell'organizzazione con cui il segnalante si interfaccia nell'ambito del proprio contesto lavorativo
Contesto lavorativo	Le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di lavoro con la Società, attraverso le quali le persone acquisiscono informazioni sulle violazioni
Persona coinvolta	La persona fisica o giuridica menzionata nella segnalazione come persona a cui la violazione è attribuita o come persona comunque implicata nella violazione segnalata
Facilitatore	La persona fisica che assiste il segnalante nel processo di segnalazione, operante

	nel medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata
Ritorsioni	Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e che provoca o può provocare alla persona segnalante un danno ingiusto
Misure di protezione	Le misure volte a tutelare da ritorsioni il segnalante, il facilitatore e i soggetti collegati al segnalante
Gestore della segnalazione	Il soggetto designato dalla Società, dotato di autonomia e indipendenza, responsabile della gestione del canale di segnalazione interno, identificato nel Compliance Officer della società.
Segnalazione anonima	La segnalazione effettuata senza indicare l'identità del segnalante; le segnalazioni anonime sono gestite secondo quanto previsto dalla normativa applicabile
Soggetto designato	Il soggetto individuato dalla normativa irlandese quale destinatario competente per determinate categorie di segnalazioni esterne.

2. Riferimenti Normativi

La presente Procedura è adottata in conformità al quadro normativo europeo e nazionale in materia di whistleblowing, compliance, protezione dei dati personali e prevenzione dei rischi aziendali. In particolare, il sistema di segnalazione della società è disciplinato dalle seguenti principali fonti normative:

- Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022 — disciplina irlandese in materia di segnalazioni protette e attuazione della Direttiva (UE) 2019/1937;
- Direttiva (UE) 2019/1937 — protezione delle persone che segnalano violazioni del diritto dell'Unione Europea;
- Regolamento (UE) 2016/679 (GDPR) e normativa irlandese applicabile in materia di protezione dei dati personali;
- Data Protection Act 2018 — normativa irlandese in materia di protezione dei dati personali;
- Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, come modificato — normativa irlandese in materia di prevenzione del riciclaggio e del finanziamento del terrorismo;
- Eventuali ulteriori disposizioni e provvedimenti delle autorità irlandesi competenti applicabili alla Società in materia di governance, compliance e AML/CFT.

3. Chi Può Effettuare una Segnalazione

Il Sistema di Whistleblowing di Real Money Europe è accessibile a tutti i soggetti che, nell'ambito di un contesto lavorativo o professionale, vengono a conoscenza di violazioni ai sensi della normativa applicabile. Le segnalazioni possono essere effettuate sia da soggetti interni sia da soggetti esterni, nei limiti e alle condizioni previste dalla normativa applicabile.

3.1 Segnalanti interni — lavoratori e collaboratori

Sono legittimati a effettuare segnalazioni tutti i soggetti che lavorano o hanno lavorato per la Società in qualsiasi veste:

- Dipendenti a tempo indeterminato e determinato;
- Collaboratori, consulenti e liberi professionisti;
- Stagisti e tirocinanti;
- Lavoratori in somministrazione;
- Directors e membri degli organi societari;
- Agenti e rappresentanti della rete commerciale;

- Ex dipendenti o collaboratori, per fatti di cui sono venuti a conoscenza durante il rapporto;
- Candidati in fase di selezione, per fatti appresi durante il processo di assunzione.

3.2 Segnalanti esterni — soggetti terzi

Sono altresì legittimati a effettuare segnalazioni i soggetti esterni che intrattengono o hanno intrattenuto rapporti professionali o commerciali con la Società, tra cui:

- Fornitori, partner commerciali e terze parti che operano o hanno operato per conto della Società;
- Altri soggetti che, nell'ambito di relazioni professionali o commerciali, abbiano acquisito conoscenza di violazioni rilevanti.

Le tutele previste dal Protected Disclosures Act 2014, come modificato, si applicano ai soggetti che rientrano nell'ambito soggettivo previsto dalla normativa medesima.

3.3 Condizioni per la protezione del segnalante

Le tutele previste dalla presente Procedura si applicano ai segnalanti che effettuano segnalazioni ai sensi del Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, purché, al momento della segnalazione, abbiano fondati motivi di ritenere che le informazioni comunicate siano vere e rientrino nell'ambito delle violazioni rilevanti ai sensi della normativa applicabile. In particolare, la segnalazione deve essere effettuata:

- sulla base di informazioni apprese nel contesto lavorativo e professionale;
- con un ragionevole convincimento circa la veridicità dei fatti segnalati;
- senza abuso dello strumento di segnalazione.

Restano escluse dalle tutele le segnalazioni contenenti informazioni che il segnalante sa essere false. Tali condotte possono comportare responsabilità disciplinari per i lavoratori, nonché responsabilità civili o penali ai sensi della normativa irlandese applicabile.

4. Cosa Si Può Segnalare

Possono essere oggetto di segnalazione le violazioni, o le ragionevoli ipotesi di violazione, previste dalla normativa applicabile, tra cui, a titolo esemplificativo e non esaustivo, le seguenti categorie di norme e procedure interne applicabili alla Società:

4.1 Violazioni della normativa antiriciclaggio (AML/CFT)

Ai sensi del Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, come modificato:

- Omessa identificazione dei clienti o violazioni degli obblighi di adeguata verifica della clientela;
- Mancate segnalazioni di operazioni sospette alla FIU Ireland e ai Revenue Commissioners, secondo quanto previsto dalla normativa irlandese applicabile;
- Violazioni delle procedure KYC interne di Real Money Europe;
- Carenze nei presidi di prevenzione del riciclaggio e del finanziamento del terrorismo.

Le segnalazioni di operazioni sospette (SOS) devono essere effettuate tramite i canali AML dedicati e non attraverso il sistema di whistleblowing.

4.2 Violazioni della normativa applicabile al Banco Metalli

Ai sensi della normativa irlandese applicabile:

- Irregolarità nella compravendita di oro da investimento o metalli preziosi;
- Carenze nei presidi di tracciabilità e registrazione delle operazioni in metalli preziosi;

- Violazioni degli obblighi di comunicazione alle autorità irlandesi competenti;
- Comportamenti scorretti nei confronti dei clienti nella compravendita di oro da investimento.

4.3 Violazioni in materia di governance e controlli interni

Ai sensi della normativa irlandese applicabile e delle procedure interne:

- Carenze nella governance aziendale, nei controlli interni o nella gestione dei conflitti di interesse;
- Comportamenti non conformi al Codice Etico aziendale e ai principi di integrità della Società;
- Condotte rilevanti ai sensi della normativa applicabile in materia di responsabilità della Società;
- Violazioni delle politiche di sicurezza informatica e dei presidi di protezione dei dati aziendali.

4.4 Violazioni in materia di protezione dei dati personali

Ai sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa irlandese applicabile:

- Trattamenti di dati personali effettuati in assenza di una base giuridica valida o in violazione dei principi del GDPR;
- Mancata adozione di misure di sicurezza adeguate, inclusi accessi non autorizzati o perdita di dati;
- Mancata gestione degli obblighi relativi alla violazione dei dati personali, inclusa la mancata notifica alla Data Protection Commission Irlandese;
- Violazioni dei diritti degli interessati.

4.5 Cosa NON si può segnalare tramite questo canale

Non rientrano nell'ambito del presente sistema di whistleblowing:

- Reclami personali relativi a rapporti di lavoro o commerciali, da gestire tramite i canali ordinari;
- Divergenze di opinione su scelte gestionali o strategiche;
- Segnalazioni consapevolmente false;
- Segnalazioni di operazioni sospette di riciclaggio, da inviare tramite l'apposito canale AML dedicato;
- Reclami relativi a prodotti o servizi, da gestire tramite la procedura reclami aziendale.

Il sistema di segnalazione non sostituisce i canali ordinari di assistenza o reclamo.

5. Come Effettuare una Segnalazione — I Tre Canali

Real Money Europe mette a disposizione dei segnalanti un sistema di segnalazione conforme alla normativa vigente, progettato per garantire riservatezza, sicurezza e tutela del segnalante. Le segnalazioni possono essere effettuate anche in forma anonima. Tuttavia, l'indicazione di un recapito personale può facilitare eventuali richieste di chiarimento o aggiornamenti.

La Società rilascia un avviso di ricevimento della segnalazione entro 7 giorni, ai sensi del Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022. La normativa irlandese prevede inoltre un diligente seguito della segnalazione e, in via generale, un riscontro entro 3 mesi.

5.1 Canale interno ufficiale — Piattaforma MITWhistle

Il canale interno ufficiale per l'invio delle segnalazioni è la piattaforma digitale dedicata:

(INSERIRE LINK MITWHISTLE — da completare)

La piattaforma consente:

- segnalazioni scritte e anonime;
- comunicazione riservata con il gestore della segnalazione;
- protezione dei dati mediante sistemi crittografati;
- separazione tra identità del segnalante e contenuto della segnalazione.

Il sistema è erogato da un provider esterno specializzato. Il trattamento dei dati personali avviene nel rispetto della normativa vigente, e i ruoli privacy sono definiti in conformità al GDPR.

5.2 Canale alternativo residuale

In alternativa alla piattaforma, il segnalante può richiedere un colloquio diretto e riservato con il Compliance Officer o inviare una comunicazione riservata scritta.

Tali canali garantiscono comunque la riservatezza del segnalante e sono gestiti secondo le medesime tutele previste dalla normativa.

5.3 Canale esterno

In presenza delle condizioni previste dalla normativa applicabile, il segnalante può effettuare una segnalazione attraverso i canali esterni previsti dal Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, rivolgendosi al soggetto designato competente per materia o al Protected Disclosures Commissioner.

Il ricorso al canale esterno è consentito, in particolare, quando:

- il segnalante ritiene ragionevolmente che la violazione rientri nell'ambito di competenza del soggetto designato cui viene effettuata la segnalazione;
- il segnalante ritiene ragionevolmente che le informazioni comunicate e le eventuali contestazioni in esse contenute siano sostanzialmente veritiere;
- la segnalazione può essere presentata al Protected Disclosures Commissioner, che provvede, ove possibile, a trasmetterla al soggetto competente per il relativo seguito.

5.4 Divulgazione pubblica

Nei casi previsti dal Protected Disclosures Act 2014, come modificato, il segnalante può rendere pubbliche le informazioni relative a una violazione, ad esempio tramite stampa o altri mezzi di comunicazione.

La divulgazione pubblica beneficia delle tutele previste dalla normativa qualora il segnalante abbia ragionevoli motivi di ritenere che le informazioni comunicate e le eventuali contestazioni in esse contenute siano sostanzialmente veritiere e ricorra almeno una delle seguenti condizioni:

- il segnalante abbia già effettuato una segnalazione interna o esterna avente sostanzialmente ad oggetto le medesime informazioni e non siano state adottate misure appropriate entro i termini previsti dalla normativa;
- il segnalante abbia ragionevoli motivi di ritenere che la violazione possa costituire un pericolo imminente o evidente per l'interesse pubblico, ad esempio in presenza di una situazione di emergenza o di un rischio di danno irreversibile;
- il segnalante abbia ragionevoli motivi di ritenere che, effettuando una segnalazione esterna, possa essere esposto a ritorsioni;
- il segnalante abbia ragionevoli motivi di ritenere che vi siano scarse possibilità che la violazione venga efficacemente affrontata, tenuto conto delle specifiche circostanze del caso, ad esempio quando vi sia il rischio che le prove vengano occultate o distrutte oppure che il soggetto competente sia coinvolto nella violazione o colluda con il responsabile.

6. Contenuto della Segnalazione

Per consentire una gestione efficace della segnalazione, è utile — ma non obbligatorio — fornire le seguenti informazioni:

- descrizione dei fatti segnalati (cosa è accaduto, in quale contesto e con quale eventuale frequenza);
- date o periodo in cui si sono verificati i fatti;
- luogo in cui si sono verificati i fatti;
- soggetti coinvolti, se noti;
- eventuale documentazione a supporto (email, contratti, screenshot, altro);
- modalità con cui si è venuti a conoscenza dei fatti.

Non è necessario che il segnalante abbia la certezza assoluta che la violazione si sia verificata: è sufficiente avere ragionevoli motivi per ritenere che le informazioni segnalate tendano a dimostrare una violazione rilevante. Le tutele previste dalla normativa si applicano in presenza delle condizioni stabilite dal Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, indipendentemente dall'esito finale delle verifiche sulla violazione segnalata.

7. Misure di Protezione del Segnalante

La Società garantisce la massima protezione ai segnalanti, in conformità al Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022, e alla Direttiva (UE) 2019/1937.

7.1 Riservatezza dell'identità

L'identità del segnalante è trattata con la massima riservatezza. Essa è conosciuta esclusivamente dai soggetti autorizzati alla gestione della segnalazione e non viene divulgata a terzi senza il consenso esplicito del segnalante, salvo nei casi previsti dalla normativa applicabile.

Tutti i report e i documenti relativi alla segnalazione sono predisposti in modo da non contenere riferimenti che possano permettere l'identificazione del segnalante.

L'identità del segnalante, o le informazioni dalle quali essa possa essere direttamente o indirettamente desunta, può essere comunicata esclusivamente nei seguenti casi:

- quando la comunicazione costituisce un obbligo necessario e proporzionato previsto dalla legge nell'ambito di indagini o procedimenti giudiziari, anche al fine di garantire i diritti di difesa della persona coinvolta;
- quando il soggetto che gestisce la segnalazione dimostri di aver adottato tutte le misure ragionevoli per evitare la divulgazione dell'identità del segnalante;
- quando vi siano ragionevoli motivi per ritenere che la comunicazione dell'identità sia necessaria per prevenire un grave rischio per la sicurezza dello Stato, la salute pubblica, la sicurezza pubblica o l'ambiente;
- quando la comunicazione dell'identità sia altrimenti richiesta dalla legge.

Nei casi in cui l'identità del segnalante debba essere comunicata senza il suo consenso, il segnalante è informato per iscritto e preventivamente, con indicazione delle ragioni della comunicazione, salvo che tale informazione possa compromettere:

- l'efficace svolgimento delle indagini sulla violazione segnalata;
- la prevenzione di un grave rischio per la sicurezza dello Stato, la salute pubblica, la sicurezza pubblica o l'ambiente;
- la prevenzione di un reato o il perseguimento di un illecito penale.

7.2 Divieto assoluto di ritorsioni

La Società vieta qualsiasi forma di ritorsione, discriminazione o comportamento pregiudizievole nei confronti del segnalante, dei suoi colleghi o dei suoi familiari, in conseguenza della segnalazione. Sono considerate ritorsioni, a titolo esemplificativo:

- licenziamento, sospensione o mancato rinnovo del contratto;
- demansionamento, trasferimenti o modifiche peggiorative delle condizioni di lavoro;
- riduzione della retribuzione o dei benefit;
- valutazioni negative non giustificate da criteri oggettivi;
- mancata promozione o avanzamento;
- atti di mobbing, isolamento o pressione indebita;
- interruzione o peggioramento del rapporto commerciale (per soggetti esterni).

La normativa irlandese vieta espressamente al datore di lavoro di adottare o minacciare misure pregiudizievoli nei confronti del lavoratore per aver effettuato una segnalazione protetta.

Il segnalante che ritenga di aver subito una ritorsione può utilizzare il canale interno tramite la piattaforma dedicata oppure, nei casi previsti dalla normativa, rivolgersi ai canali esterni competenti, incluso il Protected Disclosures Commissioner, nonché avvalersi dei rimedi previsti dalla normativa irlandese applicabile.

7.3 Protezione estesa

Le tutele previste dalla presente Procedura si estendono anche a:

- facilitatori: persone che assistono il segnalante nel processo di segnalazione (legale, rappresentante sindacale);
- colleghi e familiari del segnalante che potrebbero subire ritorsioni per connessione con la segnalazione;
- enti o persone giuridiche di proprietà del segnalante, presso cui il segnalante lavora o con cui è altrimenti connesso nell'ambito lavorativo.

7.4 Trattamento dei dati personali del segnalante

I dati personali del segnalante sono trattati nel rispetto del Regolamento (UE) 2016/679 (GDPR) e del Data Protection Act 2018 irlandese. Il trattamento avviene esclusivamente per finalità connesse alla gestione della segnalazione e nel rispetto delle basi giuridiche previste dalla normativa applicabile.

I dati e la documentazione relativi alle segnalazioni sono conservati per il periodo necessario e proporzionato ai fini della gestione della segnalazione e dell'adempimento degli obblighi previsti dalla normativa applicabile. La legge irlandese impone la tenuta di una registrazione delle segnalazioni, comprese quelle anonime.

Per ulteriori informazioni si rimanda all'informativa privacy disponibile sul sito aziendale.

8. Come Gestiamo le Segnalazioni

La Società adotta un processo strutturato di gestione delle segnalazioni articolato in sei fasi, con tempistiche definite nel rispetto dei termini previsti dal Protected Disclosures Act 2014, come modificato dal Protected Disclosures (Amendment) Act 2022:

Fase	Tempistica	Attività	Responsabile
1. Ricezione	Giorno 0	Ricezione tramite piattaforma MITWhistle, protocollazione automatica e registrazione nel registro riservato, con segregazione delle informazioni identificative del segnalante	Compliance Officer / Sistema MITWhistle
2. Conferma	Entro 7 giorni	Invio avviso di ricevimento al segnalante tramite piattaforma, con codice pratica e indicazione delle tempistiche	Compliance Officer
3. Valutazione	Entro 30 giorni	Analisi dell'ammissibilità, valutazione della gravità e urgenza, eventuale richiesta di integrazioni al segnalante	Compliance Officer
4. Istruttoria	Entro 90 giorni	Raccolta documentazione, audizioni delle persone coinvolte, verifiche tecniche, analisi normativa. Eventuali consulenti esterni possono essere coinvolti nel rispetto della riservatezza	Compliance Officer + eventuali consulenti
5. Deliberazione	Entro 90 giorni	Presentazione report al Board of Directors, delibera sulle azioni correttive e/o disciplinari	Board of directors su proposta del Compliance Officer
6. Feedback	Entro 90 giorni	Comunicazione dell'esito al segnalante (nei limiti della riservatezza), avvio delle azioni correttive deliberate	Compliance Officer

Tutte le fasi del processo sono condotte con la massima riservatezza dal gestore della segnalazione. Il vincolo di riservatezza sull'identità del segnalante è esteso a tutti i soggetti coinvolti. Il Registro Segnalazioni è conservato in forma riservata e segregata, accessibile esclusivamente al Compliance Officer e agli ulteriori soggetti espressamente autorizzati dalla Società, ove necessario.

9. Gestione dei Conflitti di Interesse

La Società ha previsto specifiche misure per garantire la gestione indipendente delle segnalazioni nei casi in cui possano emergere conflitti di interesse.

9.1 Segnalazione riguardante il Compliance Officer

Qualora una segnalazione riguardi il Compliance Officer, essa viene gestita tramite la piattaforma MITWhistle e assegnata direttamente al Board of directors, che ne assume la gestione istruttoria. Il Compliance Officer è escluso da qualsiasi accesso o attività relativa alla segnalazione.

9.2 Segnalazione riguardante uno o più Directors

Qualora la segnalazione riguardi uno o più Directors della Società, la gestione è affidata al Company Secretary, purché non coinvolto nei fatti oggetto della segnalazione e in assenza di conflitti di interesse. In caso contrario, la segnalazione è affidata a un soggetto esterno indipendente appositamente designato dalla Società.

10. Rapporti con le Autorità competenti

La Società collabora pienamente con le seguenti autorità competenti:

Protected Disclosures Commissioner	Ricezione e gestione delle segnalazioni esterne nei casi previsti dalla normativa e inoltre, ove necessario, al soggetto competente
Soggetti designati dalla normativa	Ricezione delle segnalazioni esterne nelle materie di rispettiva competenza
Data Protection Commission	Questioni relative al trattamento e alla protezione dei dati personali
Autorità giudiziaria e di polizia irlandesi	Segnalazioni aventi ad oggetto possibili reati, secondo la normativa applicabile

Real Money garantisce che l'utilizzo del canale interno non pregiudica in alcun modo il diritto del segnalante di ricorrere ai canali esterni previsti dal Protected Disclosures Act 2014, come modificato, nei casi e alle condizioni previste dalla normativa applicabile.

11. Formazione e Comunicazione

Real Money Europe si impegna a garantire che tutti i soggetti destinatari della presente Procedura siano adeguatamente informati e formati sul Sistema di Whistleblowing:

- formazione obbligatoria per tutto il personale all'assunzione e con aggiornamento annuale;
- comunicazione della presente Procedura a tutti i collaboratori e agenti della rete societaria;
- pubblicazione della Procedura sul sito aziendale nella sezione dedicata;
- messa a disposizione del canale di segnalazione.

12. Aggiornamenti della Procedura

La presente Procedura è soggetta a revisione annuale da parte del Compliance Officer e Board of directors, ovvero al verificarsi di modifiche normative rilevanti. Ogni modifica è approvata dal Board of Directors e comunicata tempestivamente a tutto il personale. La versione aggiornata è sempre disponibile sul sito aziendale nella sezione dedicata al Whistleblowing.