

Conio Srl	Predisposta da: Funzione di controllo
	Versione di: Aprile 2026
Stato	Approvata dal Consiglio di Amministrazione in data 27 /04 /26

POLITICA PER IL CONTRASTO DEGLI ABUSI DI MERCATO E LA COMUNICAZIONE AL PUBBLICO DELLE INFORMAZIONI PRIVILEGIATE

Sommario

1. Premessa	4
2. Aspetti generali del documento	4
2.1 Scopo della policy	4
2.2 Destinatari del documento e suo aggiornamento	5
2.3 Responsabile manutenzione e invio segnalazioni	6
2.4 Normativa di riferimento	6
3. PRINCIPALI FATTISPECIE DI ABUSI DI MERCATO	6
3.1 Premessa	6
3.2 Informazioni privilegiate e relativi abusi	7
3.2.1 Definizione	7
3.2.2 Abuso di informazioni privilegiate	8
3.3 Divulgazione illecita di informazioni privilegiate	9
3.4 Manipolazione di mercato	9
2.4 Operazioni personali	11
4. ADEMPIMENTI VOLTI AD INTERCETTARE E SEGNALARE FENOMENI DI MARKET ABUSE	11
4.1 Identificazione abusi di mercato ed obblighi segnalatori	11
4.2 Monitoraggio informatico	12
4.3 Formazione	12
4.4 Controlli di II livello	13
4.5 Modalità di controllo delle segnalazioni e invio dello STOR	14
5. LA COMUNICAZIONE AL PUBBLICO DI INFORMAZIONI PRIVILEGIATE	15
5.1 Premessa	15
5.2 La comunicazione al pubblico	15
5.3 Pubblicazione delle informazioni privilegiate	17
5.4 Notifica di divulgazione tardiva di informazioni privilegiate	18

1. Premessa

Conio S.r.l. (di seguito, “**Conio**” o la “**Società**”) nel rispetto della normativa e delle *best practice* di settore adotta politiche e prassi a presidio dei principali rischi a cui può essere esposta, anche in materia di abusi di mercato.

2. Aspetti generali del documento

2.1 Scopo della policy

La presente Policy è finalizzata a definire le procedure, i criteri e le modalità da adottare per gestire, monitorare e prevenire in modo efficiente il rischio di (i) abuso di informazioni privilegiate, (ii) divulgazione illecita di informazioni privilegiate e (iii) manipolazione del mercato (c.d. **Abusi di Mercato**).

Nello specifico, la Società ha istituito dispositivi, sistemi e procedure per:

- a) monitorare efficacemente e su base continuativa tutti gli ordini ricevuti e tutte le operazioni in crypto-attività eseguite, al fine di prevenire, rilevare e individuare gli ordini e le operazioni qualora vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso;
- b) monitorare efficacemente e su base continuativa aspetti del funzionamento della DLT, al fine di rilevare e individuare altri aspetti del funzionamento della tecnologia a registro distribuito, compreso il meccanismo di consenso, qualora vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso;
- c) trasmettere alla Consob le segnalazioni di ordini o operazioni sospetti (c.d. **STOR**) - secondo le modalità previste dalla normativa di settore - che sono suscettibili di costituire un abuso di mercato.

Alla luce dei servizi offerti dalla Società le crypto-attività che rientrano nella disciplina degli Abusi di Mercato sono:

- le crypto-attività c.d. *other than*,

- EMT (E-Money Token) e
- ART (Asset Referenced Token).

Inoltre, tali disposizioni si applicano a qualsiasi operazione, ordine di scambio di cripto-attività (con altre cripto-attività o con fondi) o di esecuzione di ordini per conto della clientela o condotta che si riferisca alle cripto-attività di cui sopra offerte da Conio alla clientela.

La Policy è redatta nel rispetto del principio di proporzionalità e considerato che Conio NON svolge l'attività di di piattaforma di negoziazione di cripto-attività .

La normativa sugli Abusi di Mercato è finalizzata a:

- tutelare l'integrità e l'efficienza del mercato delle cripto-attività;
- garantire la trasparenza degli operatori attraverso l'imposizione di obblighi comportamentali ed organizzativi ai soggetti che hanno potenzialmente accesso alle informazioni rilevanti.

Gli operatori CASP, tra cui Conio, in particolare, hanno l'obbligo di segnalare senza indugio all'Autorità competente gli ordini e le operazioni che, in base a ragionevoli motivi, possono ritenersi configurare una violazione delle norme sull'abuso di Informazioni Privilegiate (come di seguito definite) e sulla manipolazione del mercato.

Le operazioni relative alle cripto-attività, sopra elencate, vanno considerate sia se compiute da clienti diretti della Società, sia se compiute da controparti qualificate (i.e. piattaforme di negoziazione) di cui Conio si avvale come *liquidity provider*. Rientrano pertanto nella disciplina tutte le operazioni relative al portafoglio di proprietà di Conio e alle operazioni compiute da e per conto dei clienti.

2.2 Destinatari del documento e suo aggiornamento

La policy è portata a conoscenza degli Organi sociali, dei dipendenti e dei collaboratori di Conio (consulenti esterni, stagisti, ecc.) tramite la sua pubblicazione su tramite la sua pubblicazione Intranet aziendale e sistema di storage on premise con dati criptati.

Stante che le norme in materia di Abusi di Mercato si applicano anche ai clienti della Società, Conio informa i clienti della rilevanza delle richiamate norme e delle conseguenze derivanti dal compimento di Abusi di Mercato attraverso il proprio contratto con il cliente e attraverso la pubblicazione della presente policy sul sito web di Conio ad accesso indiscriminato.

Più in dettaglio, la Policy si applica a qualsiasi destinatario, su indicato, coinvolto in potenziali fattispecie di Abusi di Mercato (*infra* definite nel dettaglio *sub* paragrafo 3) e accede ad esempio ad informazioni privilegiate (*infra* definite *sub* paragrafo 3.2.1) perché: a) è anche membro di organi di amministrazione, direzione o vigilanza dell'emittente, dell'offerente o della persona che chiede l'ammissione alla negoziazione di una nuova cripto-attività; b) ha una partecipazione al capitale dell'emittente, dell'offerente, o della persona che richiede ammissione alla negoziazione; c) ha accesso a tali informazioni nell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche esterna alla Società, o in relazione al suo ruolo nella tecnologia a registro distribuito o in una tecnologia analoga; oppure d) è coinvolto in attività criminali.

Quando il destinatario è una persona non fisica, la Policy si applica, conformemente al diritto nazionale, alle persone fisiche che partecipano alla decisione di effettuare l'acquisto, la cessione, la cancellazione o la modifica di un ordine per conto della persona giuridica in questione.

La Policy è sottoposta ad annuale revisione in considerazione anche degli eventuali aggiornamenti di tempo in tempo necessari prendendo in esame anche la necessità di aggiornare i parametri di anomalia e degli indicatori del Sistema di Monitoraggio. È responsabilità degli Organi sociali e delle funzioni aziendali destinatarie della Policy segnalare alla Funzione Unica di Controllo eventuali situazioni non gestibili in base ai principi della Policy e le relative proposte di intervento e modifica.

2.3 Responsabile manutenzione e invio segnalazioni

Il Consiglio di Amministrazione della Società è l'organo responsabile dell'adozione della Policy, nonché della valutazione e del riesame periodico della sua efficacia e della risoluzione di eventuali carenze al riguardo.

In coerenza con il principio di proporzionalità e con la natura, la dimensione, la complessità dell'attività svolta e la gamma di servizi prestati dalla Società, il Consiglio di amministrazione nomina con una specifica delibera nell'ambito della Funzione Unica di Controllo una persona quale responsabile

- della manutenzione e dell'aggiornamento della Policy;
- dell'invio delle STOR nel rispetto della presente Policy;
- della valutazione dell'adeguatezza e della manutenzione del sistema di monitoraggio e sorveglianza dei mercati di Conio

(di seguito il “**Responsabile**”).

Il Responsabile, nell'ambito della definizione, adozione, attuazione e controllo dell'osservazione di un più generale programma di compliance, sostiene e incoraggia un appropriato grado di risk culture che sottolinei l'importanza della corretta gestione degli Abusi di Mercato. Il Responsabile è altresì dotato dell'autorità necessaria per assolvere alle proprie responsabilità in modo appropriato e indipendente, nonché i) delle necessarie competenze per seguire l'evoluzione della normativa e dei regolamenti di settore per garantire che la Società sia sempre aggiornata e conforme alle disposizioni vigenti e ii) delle necessarie competenze di gestione dei conflitti di interesse, anche attraverso una formazione continua.

Le eventuali attività del Responsabile, diverse da quelle attribuite ai sensi della presente Policy, non ne compromettono l'indipendenza e l'obiettività.

La Società prevederà nel corso dello sviluppo della propria attività di business di ampliare le risorse impiegate nella prevenzione degli Abusi di Mercato considerando un aumento direttamente proporzionale delle attività a rischio da monitorare.

2.4 Normativa di riferimento

- Regolamento UE 2023/1114 del Parlamento europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle crypto-attività (“**MiCAR**”);
- Regolamento Delegato (UE) 2025/885 della Commissione del 29 aprile 2025 che integra il regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i dispositivi, i sistemi e le procedure per prevenire, individuare e segnalare gli abusi di mercato, i modelli da utilizzare per segnalare presunti abusi di mercato e le procedure di coordinamento tra le autorità competenti per individuare e sanzionare gli abusi di mercato transfrontalieri;
- Regolamento di Esecuzione (UE) 2024/2861 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2023/1114 per quanto riguarda gli strumenti

tecniche per l'adeguata comunicazione al pubblico delle informazioni privilegiate e la comunicazione al pubblico tardiva di tali informazioni;

- ESMA - **Final Report** "*Draft technical Standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation*" (MiCA)

3. PRINCIPALI FATTISPECIE DI ABUSI DI MERCATO

3.1 Premessa

L'abuso di mercato, ai fini della normativa di settore, è il concetto che comprende le condotte illecite nei mercati di scambio delle crypto-attività, intesi come: a) Abuso di informazioni privilegiate; b) Divulgazione illecita di informazioni privilegiate; c) Manipolazione del mercato.

Tali condotte impediscono una piena ed effettiva trasparenza del mercato, che rappresenta un requisito fondamentale affinché tutti gli operatori siano in grado di operare su mercati delle crypto-attività integrati, come già accade per i mercati finanziari.

3.2 Informazioni privilegiate e relativi abusi

3.2.1 Definizione

L'art. 87 MiCAR, per informazioni privilegiate, intende:

a) informazioni di natura precisa, che non sono state rese pubbliche e che riguardano, direttamente o indirettamente, uno o più emittenti di crypto-attività, offerenti o persone che chiedono l'ammissione alla negoziazione o una o più crypto-attività e che, se rese pubbliche, potrebbero avere un effetto significativo¹ sui prezzi di tali crypto-attività o sul prezzo di una crypto-attività collegata;

¹ Per informazioni che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi delle crypto-attività s'intende le informazioni che un possessore di crypto-attività ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni d'investimento.

b) nel caso di operatori incaricati dell'esecuzione di ordini di cripto-attività per conto di clienti, s'intende anche le informazioni di natura precisa trasmesse da un cliente e connesse agli ordini pendenti in cripto-attività del cliente, concernenti, direttamente o indirettamente, uno o più emittenti, offerenti o persone che chiedono l'ammissione alla negoziazione o una o più cripto-attività e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali cripto-attività o sul prezzo di una cripto-attività collegata.

Si considera che le informazioni sono di natura precisa se esse fanno riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se tali informazioni sono sufficientemente specifiche da permettere di trarre conclusioni sul possibile effetto di detta serie di circostanze o di detto evento sui prezzi delle cripto-attività. A tal riguardo, nel caso di un processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, possono essere considerate come informazioni di natura precisa la futura circostanza o il futuro evento, nonché le tappe intermedie² di detto processo che sono collegate alla concretizzazione o alla determinazione della futura circostanza o del futuro evento.

3.2.2 Abuso di informazioni privilegiate

Ai fini dell'art. 89 MiCAR, si considera che vi sia abuso di informazioni privilegiate quando una persona in possesso di informazioni privilegiate utilizza tali informazioni acquisendo o cedendo, per conto proprio o per conto di terzi, direttamente o indirettamente, le cripto-attività cui tali informazioni si riferiscono. È considerato abuso di informazioni privilegiate anche l'utilizzo di informazioni privilegiate tramite annullamento o modifica di un ordine concernente cripto-attività al quale le informazioni si riferiscono quando tale ordine è stato inoltrato prima che la persona

² Una tappa intermedia in un processo prolungato è considerata un'informazione privilegiata se, di per sé, risponde ai criteri indicati riguardo alle informazioni privilegiate.

interessata entrasse in possesso di dette informazioni privilegiate. L'uso di informazioni privilegiate si configura anche quando una persona presenta, modifica o ritira un'offerta per conto proprio o per conto di terzi.

Nessuno può abusare o tentare di abusare di informazioni privilegiate ovvero utilizzare informazioni privilegiate sulle cripto-attività per acquisire o per cedere tali cripto-attività, direttamente o indirettamente, per conto proprio o per conto di terzi. Nessuno può raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate³.

Nessuno in possesso di informazioni privilegiate sulle cripto-attività raccomanda o induce un'altra persona sulla base di tali informazioni privilegiate: a) ad acquistare o cedere tali cripto-attività; o b) ad annullare o modificare un ordine riguardante tali cripto-attività.

3.3 Divulgazione illecita di informazioni privilegiate

Ai sensi dell'art. 90, MiCAR, nessuno in possesso di informazioni privilegiate può divulgare illecitamente tali informazioni ad altre persone, tranne nel caso in cui tale divulgazione avvenga nell'ambito del normale esercizio di un'attività lavorativa, di una professione o di una funzione.

La divulgazione a terzi delle raccomandazioni o induzioni, si intende come divulgazione illecita di informazioni privilegiate quando la persona che divulga la raccomandazione o l'induzione sa o dovrebbe sapere che essa si basa su informazioni privilegiate.

³ Il ricorso a una raccomandazione o a una induzione è inteso come abuso di informazioni privilegiate quando la persona che ricorre a tale raccomandazione o induzione sa o dovrebbe sapere che esse si basano su informazioni privilegiate.

3.4 Manipolazione di mercato

Ai sensi dell'art. 91, MiCAR, a nessuno è consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato. Per manipolazione del mercato si intendono le attività seguenti:

- a) salvo che per motivi legittimi, concludere un'operazione, collocare un ordine di negoziazione o porre in essere qualsiasi altra condotta che: i) fornisca, o sia suscettibile di fornire, indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di una crypto-attività; ii) fissi, o sia suscettibile di fissare, il prezzo di una o più crypto-attività a un livello anormale o artificiale;
- b) concludere un'operazione, collocare un ordine di negoziazione o porre in essere qualsiasi altra attività o condotta che incida o possa incidere sul prezzo di una o più crypto-attività utilizzando uno strumento fittizio o qualsiasi altro tipo di inganno o espediente;
- c) diffondere informazioni attraverso i media, compreso Internet, o qualsiasi altro mezzo che forniscano, o è probabile che forniscano, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di una o più crypto-attività, o che fissino, o è probabile che fissino, il prezzo di una o più crypto-attività a un livello anormale o artificiale, compresa la diffusione di informazioni non confermate, qualora la persona responsabile della diffusione sapesse, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti.

Sono considerate manipolazione del mercato, tra l'altro, le condotte seguenti:

- a) l'acquisizione di una posizione dominante sull'offerta o sulla domanda di una crypto-attività, che abbia o possa avere l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita oppure crei, o possa creare, altre condizioni commerciali inique;
- b) l'inoltro di ordini a una piattaforma di negoziazione di crypto-attività, compresa qualsiasi cancellazione o modifica degli stessi, mediante qualsiasi mezzo di negoziazione disponibile, e che

produca uno degli effetti di cui al capoverso 2, lettera a), attraverso: i) la compromissione o il ritardo del funzionamento della piattaforma di negoziazione di cripto-attività o l'esecuzione di qualsiasi attività che possa avere tale effetto; ii) l'esecuzione di azioni intese a ostacolare l'individuazione di ordini autentici sulla piattaforma di negoziazione di cripto-attività da parte delle altre persone o qualsiasi attività che possa avere tale effetto, anche mediante l'inserimento di ordini che determinano la destabilizzazione del normale funzionamento della piattaforma di negoziazione di cripto-attività; iii) la creazione di un segnale falso o fuorviante in merito all'offerta, alla domanda o al prezzo di una cripto-attività, in particolare mediante l'inserimento di ordini per avviare o aggravare una tendenza, o l'esecuzione di qualsiasi attività che possa avere tale effetto;

c) l'uso occasionale o abituale dei mezzi di informazione tradizionali o elettronici al fine di esprimere pareri su una cripto-attività, nella quale si sono prese posizioni in precedenza, e di approfittare successivamente degli effetti prodotti da tali pareri sul prezzo di detta cripto-attività, senza avere nel contempo reso pubblico detto conflitto di interesse in modo adeguato ed efficace.

3.5 Operazioni personali

La disciplina delle operazioni personali va letta con rinvio all'apposito paragrafo della Policy sui conflitti di interesse adottata dalla Società.

4. ADEMPIMENTI VOLTI AD INTERCETTARE E SEGNALARE FENOMENI DI MARKET ABUSE

4.1 Identificazione Abusi di Mercato ed obblighi segnalatori

L'articolo 92, MiCAR, prevede, con una formula generale, che *“chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività dispone di dispositivi, sistemi e procedure efficaci per*

prevenire e individuare gli abusi di mercato. Tale persona è soggetta alle norme di notifica dello Stato membro in cui è registrata o ha la sede centrale o, nel caso di una succursale, dello Stato membro in cui è situata la succursale, e comunica senza indugio all'autorità competente di tale Stato membro qualsiasi ragionevole sospetto in merito a un ordine o a un'operazione, comprese eventuali cancellazioni o modifiche degli stessi, e ad altri aspetti del funzionamento della tecnologia a registro distribuito, come il meccanismo di consenso, qualora vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso”.

Conio, con la presente Policy, risponde a tali obblighi.

Essi si applicano

- agli ordini e alle operazioni connessi a qualsiasi cripto-attività (EMT, ART e *other than*) quali che siano: la veste in cui l'ordine è inoltrato o l'operazione è eseguita, la tipologia di clienti interessata, il luogo in cui l'ordine è inoltrato o l'operazione è eseguita, sia esso in una sede di negoziazione o al di fuori di essa;
- a qualsiasi condotta che si riferisca alle cripto-attività di cui sopra offerte da Conio alla clientela.

4.2 Monitoraggio informatico

Conio è tenuta a monitorare efficacemente e su base continuativa tutti gli ordini ricevuti e tutte le operazioni eseguite al fine di rilevare e individuare gli ordini, le operazioni e qualsiasi condotta che si riferisca alle cripto-attività che potrebbero costituire un Abuso di Mercato. Il monitoraggio viene effettuato sia off-chain che on-chain, ove applicabile, includendo anche aspetti ulteriori del funzionamento della tecnologia a registro distribuito (DLT), compreso il meccanismo di consenso, qualora vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso.

A tal fine, Conio ha sviluppato *in-house* un sistema di monitoraggio e sorveglianza dei mercati con sistemi che prevedono controlli automatici e manuali di confronto del prezzo presente in Conio e i prezzi medi delle cripto-attività transate, e su tutta la gamma delle attività quindi anche ordini, transazioni, altre tipologie di cripto-attività, con lo scopo di identificare comportamenti sospetti della clientela e dei propri dipendenti (di seguito il “**Sistema di Monitoraggio Informatico**”).

Il Sistema di Monitoraggio Informatico prevede i pattern di cui all’Allegato 1 volti a generare alert per prevenire e contrastare le singole fattispecie di Abuso di Mercato che possono risultare dalla prestazione di tutti i Servizi che la società è autorizzata a svolgere ad eccezione di quanto previsto per il Servizio di Esecuzione di Ordini per conto dei clienti che rileva, in considerazione delle modalità di svolgimento dello stesso, ai soli fini del tracciamento delle informazioni legate ai singoli ordini e la revoca dei singoli ordini.

-

Il Sistema di Monitoraggio Informatico traccia, inoltre, le operazioni poste in essere anche dai propri dipendenti e salva, in modo immutabile, tutte le informazioni raccolte durante la vita di un’utenza. In caso di compromissione di quest’ultima Conio ha posto in essere un sistema ad autenticazione multifattoriale per mitigare eventuali rischi di esecuzioni di operazioni di tipo dispositivo non autorizzate.

Nello specifico, il Sistema di Monitoraggio Informativo analizza le circostanze dalle quali potrebbe emergere un Abuso di Mercato al verificarsi del pattern e genera l’alert entro i successivi 5 minuti.

Le suddette informazioni sono documentate per iscritto, con eventuali modifiche o aggiornamenti, e sono conservate per un periodo minimo di 5 anni all’interno del Cloud aziendale ad accesso esclusivo del responsabile della Funzione IT.

In caso di tentativi di abusi di mercato, interni ed esterni, la società è dotata di un sistema di rilevamento che opera in via continuativa su tutti i dispositivi in modo tale da bloccare, identificare eventuali minacce.

4.3 Formazione

Conio organizza e impartisce una formazione efficace e completa al personale incaricato della prevenzione, del monitoraggio, del rilevamento e dell'individuazione degli ordini e operazioni e degli altri aspetti del funzionamento della DLT che potrebbero costituire abuso di informazioni privilegiate, manipolazione di mercato ovvero tentato abuso di informazioni privilegiate o tentata manipolazione di mercato, compreso il personale incaricato dell'elaborazione degli ordini e delle operazioni.

La formazione deve essere offerta periodicamente ed è adeguata e proporzionata alla scala, alle dimensioni e alla natura dell'attività professionale svolta.

4.4 Controlli di II livello

La Funzione Unica di Controllo:

- individua, nell'ambito delle verifiche periodiche, eventuali fenomeni di ripetitività di comportamenti potenzialmente abusivi e ne valutano la relativa gravità;
- raccomanda le possibili azioni di mitigazione del rischio, tra cui, a titolo esemplificativo, le seguenti:
 - per gli ordini della Società sul conto di proprietà, si predispone un incontro con gli operatori al fine di precisare loro comportamenti operativi non conformi alla normativa di riferimento;
 - se si tratta di ordini impartiti dai clienti, si predispone un incontro con la funzione di riferimento al fine di precisare comportamenti operativi non conformi alla normativa di riferimento;
 - eventuale segnalazione a Consob.

La Funzione Unica di Controllo valuta l'adeguatezza delle procedure interne e degli applicativi di

supporto, almeno una volta all'anno, proponendo al Consiglio di Amministrazione eventuali variazioni ai processi operativi o alle soglie di allarme previste.

4.5 Modalità di controllo delle segnalazioni e invio dello STOR

L'iter operativo in merito ai controlli e segnalazioni di operazioni sospette si articola a seconda della provenienza della segnalazione, la quale può alternativamente essere effettuata

(i) da un soggetto esterno alla Società;

(ii) da un dipendente o collaboratore della Società;

In tal caso viene informato il Responsabile il quale acquisisce tutte le informazioni ed effettua le dovute valutazioni e controlli in merito alla necessità di procedere con la formulazione di una STOR.

Se ritiene fondata la segnalazione, il Responsabile procede alla eventuale formulazione di una STOR la quale dovrà essere predisposta sulla base del modello allegato alla presente Policy (cfr. Allegato 2 della presente policy) compilando i campi informativi pertinenti agli ordini, alle operazioni o ad altri aspetti del funzionamento della DLT segnalati in un modo chiaro e preciso, compresi i documenti giustificativi e gli allegati.

La STOR deve essere inviata alla CONSOB tramite il mezzo elettronico indicato sul sito Internet della stessa CONSOB immediatamente all'emergere di un ragionevole sospetto di effettivo o tentato Abuso di Mercato.

(iii) dal Sistema di Monitoraggio Informativo

Il Sistema di Monitoraggio Informatico prevede la possibilità di estrarre e valutare - in merito a un ordine, un'operazione o altri aspetti della DLT in merito ai quali sussistono circostanze che indichino che un Abuso di Mercato sia stato commesso, sia in atto o possa essere commesso - la quale deve essere eseguita entro massimo 5 giorni lavorativi successivi all'alert dal Responsabile.

In particolare, il Responsabile esegue il monitoraggio degli alert e procede a una valutazione preliminare.

Successivamente, viene verificata l'assenza di eventuali anomalie riguardanti l'operatività e si procede agli approfondimenti concernenti un ordine, un'operazione o altri aspetti della DLT, coinvolgendo se ritenuto necessario le funzioni aziendali coinvolte nell'operazione.

Effettuate le valutazioni il Responsabile procede alla eventuale formulazione di una STOR la quale dovrà essere predisposta sulla base del modello allegato alla presente Policy (cfr. Allegato 2 della presente policy) compilando i campi informativi pertinenti agli ordini, alle operazioni o ad altri aspetti del funzionamento della DLT segnalati in un modo chiaro e preciso, compresi i documenti giustificativi e gli allegati.

Nei casi che presentano profili di particolare complessità o rilevanza, il Responsabile informa il Consiglio di amministrazione prima dell'eventuale trasmissione della STOR. Rientrano in tale fattispecie anche le seguenti casistiche:

- coinvolgimento di soggetti interni alla Società;
- potenziale impatto reputazionale significativo sulla Società;
- operatività transfrontaliera o elementi di particolare complessità tecnica connessi alla DLT.

Il Consiglio di amministrazione, in seguito ad una approfondita analisi, delibera alternativamente di

- archiviare il caso se viene meno il ragionevole sospetto di effettivo o tentato Abuso di Mercato;
- rafforzare il monitoraggio sul singolo cliente;
- risolvere il contratto con il cliente nel caso in cui l'operazione eseguita sia di un importo rilevante (superiore a 100 mila euro) e/o la sussistenza del ragionevole sospetto di

effettivo o tentato Abuso di Mercato comporti un impatto reputazionale significativo sulla Società.

Resta ferma la responsabilità del Responsabile in ordine alla tempestiva trasmissione della STOR alla CONSOB, ai sensi dell'art. 92 MiCAR.

La STOR deve essere inviata alla CONSOB tramite il mezzo elettronico indicato sul sito Internet della stessa CONSOB immediatamente all'emergere di un ragionevole sospetto di effettivo o tentato Abuso di Mercato.

Conio garantisce

- di preservare la riservatezza delle informazioni contenute nella STOR;
- che né al soggetto nei cui confronti la STOR è creata, né a chiunque a altro non sia tenuto a esserne a conoscenza per la funzione svolta o la posizione occupata presso il segnalante, giungano informazioni relative *(i)* alla generazione degli alert, *(ii)* alla valutazione che può condurre la Funzione Unica di Controllo, *(iii)* al fatto che la risorsa designata della Funzione Unica di Controllo completerà la STOR senza inviare richieste di informazioni alla persona nei cui confronti la STOR può essere creata per completare determinati campi, *(iv)* alla trasmissione di una STOR alla CONSOB o all'intenzione di trasmetterla.

Nel caso in cui sia necessario inviare una STOR relativa a operazioni e ordini o altri aspetti del funzionamento della DLT passati in quanto il sospetto è emerso a causa di eventi verificatisi o informazioni resi disponibili successivamente, sarà necessario spiegare nella relativa STOR inviata a CONSOB i motivi dello sfasamento temporale tra la presunta violazione e la trasmissione della STOR, illustrando le circostanze specifiche del caso.

In ogni caso è fatto obbligo di comunicare a CONSOB tutte le informazioni supplementari di cui si sia venuti a conoscenza dopo la trasmissione originaria della STOR e fornire qualsiasi informazione o documento sia richiesto da CONSOB.

Conio conserva per un periodo di almeno cinque anni le informazioni che documentano le analisi effettuate sugli ordini, le operazioni e gli aspetti del funzionamento della DLT che potrebbero costituire Abuso di Mercato.

4.6. Flussi informativi e supervisione

Il Responsabile trasmette al Consiglio di amministrazione, con periodicità almeno semestrale, un report contenente informazioni aggregate in merito a:

1. il numero di *alert* generati dal Sistema di Monitoraggio Informatico;
2. il numero di casi sottoposti ad approfondimento;
3. il numero di STOR inviate all'Autorità competente;
4. il numero di casi archiviati;
5. le eventuali criticità riscontrate nel Sistema di Monitoraggio Informatico.

Il Consiglio di amministrazione valuta l'efficacia complessiva del sistema adottato dalla Società e, ove necessario, richiede l'adozione di interventi correttivi o migliorativi.

5. LA COMUNICAZIONE AL PUBBLICO DI INFORMAZIONI PRIVILEGIATE

5.1 Premessa

Il presente paragrafo disciplina le ipotesi in cui la Società rivesta il ruolo di “emittente”, “offerente” e “persona che chiede ammissione alla negoziazione di cripto-attività”.

Ad oggi, però, la Società non riveste tale ruolo e quindi trova applicazione solo il par. 5.2.; infatti, non trovano applicazione le previsioni di cui all'art. 88 MiCAR in materia di divulgazione delle informazioni privilegiate.

I paragrafi 5.3 e seguenti forniscono, invece, evidenza degli obblighi che diverranno applicabili solo nel momento in cui la Società dovesse assumere il ruolo di emittente, offerente o persona che chiede ammissione alla negoziazione. Allo stato quindi sono solo indicazioni normative e di best practice, che saranno riviste e aggiornate una volta che Conio ricoprirà il citato ruolo di “emittente”, “offerente” o “persona che chiede ammissione alla negoziazione di crypto-attività”.

-

5.2 Gestione di informazioni sensibili (presidi operativi vigenti)

Nell’ambito dei servizi attualmente prestati, la Società può venire a conoscenza di informazioni potenzialmente sensibili relative ai clienti o alle operazioni. Tali informazioni sono gestite attraverso i seguenti presidi e flussi informativi interni:

- (i) accesso limitato alle informazioni su base need-to-know da parte delle funzioni e delle aree autorizzate;
- (ii) tracciamento e controllo degli accessi ai sistemi informativi;
- (iii) presidi organizzativi e IT a tutela della riservatezza e integrità delle informazioni;
- (iv) presidi contrattuali con i fornitori di servizi.

5.3 La comunicazione al pubblico

Conio comunica quanto prima al pubblico le informazioni privilegiate che lo riguardano direttamente, in modo da consentire al pubblico di accedervi rapidamente e di valutarle in modo

completo, corretto e tempestivo. La Società non coniuga la comunicazione di informazioni privilegiate al pubblico con la commercializzazione delle loro attività. La Società pubblica e conserva sul sito web, per un periodo di almeno cinque anni, tutte le informazioni privilegiate che sono tenuti a comunicare al pubblico.

Conio comunica le informazioni privilegiate in suo possesso utilizzando strumenti tecnici che consentono di diffondere tali informazioni: a) su base non discriminatoria a una platea il più possibile ampia; b) a titolo gratuito; c) simultaneamente in tutta l'UE.

Per garantire una diffusione efficace, la Società comunica le informazioni privilegiate, direttamente o tramite terzi, ai mezzi di informazione sui quali il pubblico fa ragionevole affidamento, tra cui uno o più dei seguenti: a) mezzi di informazione tradizionali; b) social media⁴ che consentono la pubblicazione in forma scritta; c) piattaforme basate sul web⁵ che consentono la pubblicazione di notizie relative a emittenti, offerenti o persone che chiedono l'ammissione alla negoziazione di cripto-attività.

La Società non diffonde informazioni privilegiate attraverso i social media o le piattaforme basate sul web qualora tali canali non garantiscano l'accessibilità delle informazioni privilegiate a tutti i propri utenti o subordinino l'accesso a modalità tali da limitare l'accesso dei propri utenti.

La pubblicazione di informazioni privilegiate sui social media, sulle piattaforme basate sul web o sul sito web di una piattaforma di negoziazione di cripto-attività contiene un link alla dichiarazione scritta pubblicata sul sito della Società.

⁴ Per social media si intende un «servizio di social network online» quale definito all'articolo 2, punto 7), del regolamento (UE) 2022/1925.

⁵ Per piattaforme basate sul web si intendono le piattaforme online che raccolgono e diffondono dati e informazioni relativi alle cripto-attività, accessibili a titolo gratuito e su base non discriminatoria, per promuovere decisioni di investimento informate.

La Società diffonde informazioni privilegiate attraverso i social media o le piattaforme basate sul web utilizzando mezzi elettronici che preservano la completezza, l'integrità e la riservatezza delle informazioni privilegiate in fase di diffusione. Per ogni diffusione di questo tipo si indicano chiaramente: a) la natura privilegiata delle informazioni comunicate; b) l'identità dell'emittente, dell'offerente o della persona che chiede l'ammissione alla negoziazione, compresa la denominazione legale completa, se del caso; c) l'identità del notificante, specificando nome, cognome e posizione di tale persona presso l'emittente, l'offerente o la persona che chiede l'ammissione alla negoziazione; d) l'oggetto delle informazioni privilegiate; e) la data e l'ora in cui le informazioni sono diffuse.

La Società assicura la completezza, l'integrità e la riservatezza delle informazioni privilegiate rimediando prontamente a qualsiasi carenza o disfunzione nella loro diffusione.

5.4 Pubblicazione delle informazioni privilegiate

La Società pubblica sul proprio sito web le informazioni privilegiate di cui all'articolo 87 del MiCAR sotto forma di dichiarazione scritta scaricabile. Il linguaggio utilizzato nella dichiarazione scritta scaricabile per descrivere le informazioni privilegiate è chiaro, preciso e non fuorviante.

Il sito web:

- a) consente agli utenti di accedere, a titolo gratuito e su base non discriminatoria, alle informazioni privilegiate pubblicate sul sito stesso;
- b) colloca le informazioni privilegiate in una sezione facilmente identificabile affinché gli utenti possano reperirle agevolmente;
- c) indica chiaramente la data e l'ora della divulgazione delle informazioni privilegiate;
- d) elenca le divulgazioni delle informazioni privilegiate in ordine cronologico;

- e) fornisce le informazioni privilegiate nella lingua in cui è redatto il White Paper sulla crypto-attività e, ove possibile, in una lingua comunemente utilizzata negli ambienti della finanza internazionale;
- f) offre agli utenti la possibilità di ricevere avvisi tramite e-mail, messaggio o finestra a comparsa che segnalino l'esistenza di pubblicazioni relative a informazioni privilegiate e che favoriscano il rapido accesso a tali pubblicazioni ogni qual volta siano pubblicate informazioni privilegiate.

5.5 Notifica di divulgazione tardiva di informazioni privilegiate

La Società sotto la propria responsabilità, ritarda la divulgazione al pubblico di informazioni privilegiate purché siano soddisfatte tutte le condizioni seguenti:

- la divulgazione immediata potrebbe pregiudicare i legittimi interessi degli emittenti, degli offerenti o delle persone che chiedono l'ammissione alla negoziazione;
- è improbabile che il ritardo nella divulgazione abbia l'effetto di fuorviare il pubblico;
- gli emittenti, gli offerenti o le persone che chiedono l'ammissione alla negoziazione sono in grado di garantire la riservatezza di tali informazioni.

Per ritardare la divulgazione al pubblico di informazioni privilegiate a norma dell'articolo 88, MiCAR, la Società usa strumenti tecnici⁶ che assicurano l'accessibilità, la leggibilità e la conservazione su supporto durevole⁷ di tutte le informazioni seguenti:

- a) data e ora: i) della prima esistenza delle informazioni privilegiate; ii) dell'assunzione della decisione di ritardare la divulgazione delle informazioni privilegiate; iii) della data di probabile divulgazione delle informazioni privilegiate da parte di Conio;
- b) posizioni/funzioni delle persone che, presso la Società, sono responsabili: i) dell'assunzione della decisione di ritardare la divulgazione delle informazioni privilegiate e della decisione che stabilisce l'inizio del periodo di ritardo e la sua probabile fine; ii) del monitoraggio continuo delle condizioni che consentono di ritardare la divulgazione delle informazioni privilegiate; iii) dell'assunzione della decisione di divulgare le informazioni privilegiate; iv) della comunicazione all'autorità competente delle informazioni sul ritardo e della spiegazione scritta; c) prova del soddisfacimento iniziale delle condizioni di cui all'articolo 88, paragrafo 2, MiCAR⁸ e di qualsiasi modifica al riguardo sopravvenuta

⁶ Il mezzo elettronico assicura che la notifica del ritardo nella divulgazione delle informazioni privilegiate comprenda le informazioni seguenti: a) l'identità dell'emittente, dell'offerente o della persona che chiede l'ammissione alla negoziazione, compresa la denominazione legale completa, se del caso; b) l'identità del notificante, compresi nome, cognome e posizione di tale persona presso l'emittente, l'offerente o la persona che chiede l'ammissione alla negoziazione; c) il punto di contatto per quanto riguarda la notifica, compresi indirizzo di posta elettronica e numero di telefono professionali; d) l'identificazione delle informazioni privilegiate la cui divulgazione al pubblico è stata effettuata in ritardo, ossia il titolo della dichiarazione relativa alla divulgazione, il numero di riferimento, se assegnato dal sistema di diffusione utilizzato, nonché la data e l'ora della divulgazione al pubblico delle informazioni privilegiate; e) la data e l'ora della decisione di ritardare la divulgazione delle informazioni privilegiate; f) le funzioni dei responsabili della decisione di ritardare la divulgazione al pubblico delle informazioni privilegiate.

⁷ Per «supporto durevole» si intende qualsiasi strumento che consente di memorizzare le informazioni in modo che siano accessibili per la futura consultazione durante un periodo di tempo adeguato ai fini cui esse sono destinate e che permette la riproduzione inalterata delle informazioni memorizzate.

⁸ Conio può ritardare la divulgazione al pubblico di informazioni privilegiate purché siano soddisfatte tutte le condizioni seguenti: a) la divulgazione immediata potrebbe pregiudicare i legittimi interessi degli emittenti, degli offerenti o delle persone che chiedono l'ammissione alla negoziazione; b) è improbabile che il ritardo nella divulgazione abbia l'effetto di fuorviare il pubblico; c) gli emittenti, gli offerenti o le persone che chiedono l'ammissione alla negoziazione sono in grado di garantire la riservatezza di tali informazioni.

durante il periodo di ritardo, tra cui: i) barriere protettive delle informazioni erette sia all'interno sia verso l'esterno per impedire l'accesso alle informazioni privilegiate da parte di altre persone oltre quelle che, presso l'emittente, l'offerente o la persona che chiede l'ammissione alla negoziazione, devono accedervi nell'ambito del normale esercizio della propria attività lavorativa, professione o funzione; ii) le disposizioni adottate qualora la riservatezza delle informazioni privilegiate non sia più garantita.

Conio notifica per iscritto alla CONSOB il ritardo nella divulgazione delle informazioni privilegiate e ne fornisce una spiegazione per iscritto, per il tramite di un apposito punto di contatto istituito presso di essa o da essa designato e usando i mezzi elettronici indicati dall'Autorità. Tale notifica include anche l'identità e i recapiti della persona responsabile della divulgazione su precisata.

6. VIOLAZIONE DELLE NORME IN MATERIA DI ABUSI DI MERCATO

Conio informa tutti i destinatari della Policy che la violazione delle norme in materia di abusi mercato può comportare la comminazione delle seguenti sanzioni:

- a) una dichiarazione pubblica indicante la persona fisica o giuridica responsabile e la natura della violazione;
- b) un'ingiunzione diretta alla persona fisica o giuridica responsabile di porre termine al comportamento che costituisce la violazione e di astenersi dal ripeterlo;
- c) la restituzione dei profitti realizzati o delle perdite evitate grazie alla violazione, nella misura in cui possono essere determinati;

- d) la revoca o la sospensione dell'autorizzazione di un prestatore di servizi per le cripto-attività;
- e) in caso di ripetute violazioni dell'articolo 89, 90, 91 o 92 MiCAR, l'interdizione per almeno 10 anni di qualsiasi membro dell'organo di amministrazione del prestatore di servizi per le cripto-attività o di qualsiasi altra persona fisica ritenuta responsabile della violazione dall'esercizio di funzioni di gestione in un prestatore di servizi per le cripto-attività;
- f) in caso di violazioni delle disposizioni di cui all'articolo 88 del regolamento (UE) 2023/1114, o dei relativi atti delegati e norme tecniche di regolamentazione e attuazione:
 - i. nei confronti delle persone giuridiche, la sanzione amministrativa pecuniaria da euro 30.000 fino a euro 2,5 milioni ovvero, se superiore, fino al 2 per cento del fatturato totale annuo;
 - ii. nei confronti dei soggetti che svolgono funzioni di amministrazione, direzione o controllo e del personale delle Società e al ricorrere delle condizioni ivi stabilite nell'art. 36 D. Lgs. 5 settembre 2024, n. 129, la sanzione amministrativa pecuniaria da euro 5.000 fino a euro 1 milione;
- g) in caso di violazioni delle disposizioni di cui all'articolo 92 del regolamento (UE) 2023/1114, o dei relativi atti delegati e norme tecniche di regolamentazione e attuazione, si applica:
 - i. nei confronti delle persone giuridiche, la sanzione amministrativa pecuniaria da euro 30.000 fino a euro 15 milioni ovvero, se superiore, fino al 15 per cento del fatturato totale annuo;
 - ii. nei confronti dei soggetti che svolgono funzioni di amministrazione, direzione o controllo e del personale delle Società e al ricorrere delle condizioni ivi stabilite

nell'art. 36 D. Lgs. 5 settembre 2024, n. 129, la sanzione amministrativa pecuniaria da euro 5.000 fino a euro 5 milioni;

- h) con la sanzione amministrativa pecuniaria da euro 5.000 fino a euro 5 milioni chiunque viola il divieto di abuso di informazioni privilegiate di cui all'articolo 89 del regolamento (UE) 2023/1114, di comunicazione illecita di informazioni privilegiate di cui all'articolo 90 o di manipolazione del mercato di cui all'articolo 91 del citato regolamento; Non può essere assoggettato a sanzione amministrativa per violazione dell'articolo 91 del regolamento (UE) 2023/1114 chi dimostri di avere agito per motivi legittimi;
- i) nei casi di cui alle precedenti lett. f), g) e h), se il vantaggio ottenuto dall'autore della violazione come conseguenza della violazione stessa è superiore ai limiti massimi indicati nel presente articolo, la sanzione amministrativa pecuniaria è elevata fino al triplo dell'ammontare del vantaggio ottenuto, purché tale ammontare sia determinabile

ALLEGATO 2 – Modello STOR

Segnalazione di ordine o operazione sospetti (STOR)

Indicazioni per la compilazione: i campi delle sezioni da 1 a 4 sono obbligatori. Qualora non sia possibile fornire informazioni per un campo specifico, si prega di indicare «NA» e di spiegarne brevemente i motivi.

SEZIONE 1 — IDENTITÀ DEL SOGGETTO/DELLA PERSONA CHE TRASMETTE LA STOR

Nome della persona fisica

[Nome e cognome della persona fisica incaricata della trasmissione della STOR presso il soggetto trasmittente]

Posizione presso il soggetto segnalante	[Posizione occupata dalla persona fisica incaricata di trasmettere la STOR presso il soggetto trasmittente]
Nome del soggetto segnalante	[Nome completo del soggetto segnalante; per le persone giuridiche anche: - se applicabile, forma giuridica specificata nel registro del paese a norma della cui legge la persona giuridica è costituita; - identificativo della persona giuridica (codice LEI) secondo la norma ISO 17442]
Indirizzo del soggetto segnalante	[Indirizzo completo (ad esempio via, numero civico, codice postale, località, regione/provincia) e Stato]
Veste del soggetto relativamente agli ordini, operazioni o comportamenti connessi al funzionamento della DLT che potrebbero costituire abuso di mercato	[Descrizione della veste in cui il soggetto segnalante ha agito relativamente agli ordini, operazioni o comportamenti connessi al funzionamento della tecnologia a registro distribuito che potrebbero indicare l'esistenza di abusi di mercato, ad esempio esecuzione di ordini per conto dei clienti, gestione di una piattaforma di negoziazione...]
Tipo di attività di negoziazione (market making, arbitraggio ecc.) e tipo di crypto-attività negoziata dal soggetto segnalante	[Descrizione degli eventuali accordi o circostanze o relazioni di natura societaria, contrattuale o organizzativa]

Referente per la richiesta di ulteriori informazioni	[Persona di contatto presso il soggetto segnalante per la richiesta di ulteriori informazioni relative alla segnalazione (ad esempio responsabile della conformità) e relativi estremi di contatto, qualora non si tratti della stessa persona incaricata di trasmettere la STOR: - nome e cognome; - posizione del referente presso il soggetto segnalante; - indirizzo e-mail professionale; - numero di telefono professionale]
I fatti sono già stati segnalati alle autorità pubbliche?	[Indicare se i fatti sono già stati segnalati all'autorità pubblica (e in tal caso indicare il nome dell'autorità)]
SEZIONE 2 — OPERAZIONE/ORDINE/COMPORTAMENTO E ALTRI ASPETTI CONNESSI AL FUNZIONAMENTO DELLA TECNOLOGIA A REGISTRO DISTRIBUITO	

Descrizione della crypto-attività	[Descrivere la crypto-attività o le crypto-attività oggetto della STOR, indicandone: - il nome completo (compresi l'identificativo del token digitale (DTI) conformemente alla norma ISO 24165-2 o un identificativo univoco equivalente di cui all'articolo 15 del regolamento delegato (UE) 2025/1140 della Commissione (1) che specifica le registrazioni da conservare relative a tutti i servizi per le crypto-attività, le attività, gli ordini e le operazioni effettuati) o la descrizione della crypto-attività in assenza del DTI. Se il comportamento sospetto riguarda una coppia di negoziazione, elencare entrambe le crypto-attività della coppia; - il tipo di crypto-attività (token collegato ad attività, token di moneta elettronica, altra crypto-attività) e, per i token collegati ad attività e i token di moneta elettronica, il valore, il diritto o la valuta ufficiale (o una loro combinazione) cui la crypto-attività fa riferimento al fine di mantenere un valore stabile]
Nome del registro distribuito o dei registri distribuiti	[Indicare il nome completo del registro distribuito o dei registri distribuiti in cui è stato osservato il comportamento sospetto.]
La piattaforma di negoziazione in cui è stato inoltrato l'ordine o è stata eseguita l'operazione	[Specificare il nome e il codice identificativo del mercato (MIC) conformemente alla norma ISO 10383 per identificare la piattaforma di negoziazione in cui è stato inoltrato l'ordine o è stata eseguita l'operazione. Se l'ordine o l'operazione non sono stati identificati in una piattaforma di negoziazione, indicare «al di fuori di una piattaforma di negoziazione» e l'identificativo della persona

	giuridica (codice LEI) del prestatore di servizi per le cripto-attività che ha eseguito l'operazione, se del caso.]
Luogo (Stato)	[Nome completo dello Stato e codice paese a due caratteri secondo la norma ISO 3166-1] [Specificare il luogo in cui: - l'ordine è stato emesso; - l'operazione è stata eseguita; - il comportamento connesso al funzionamento della tecnologia a registro distribuito ha luogo.]

Descrizione dell'ordine, operazione o comportamento sospetto connesso al funzionamento della DLT	[Descrivere almeno le seguenti caratteristiche degli ordini, delle operazioni o dei comportamenti segnalati: - data e ora degli ordini, delle operazioni o dei comportamenti (la data e l'ora devono essere indicate nel formato UTC secondo ISO 8601); - numero di riferimento dell'ordine o dell'operazione oppure hash dell'operazione; - data e ora di regolamento; - prezzo di acquisto/vendita; - volume/quantità di cripto-attività; - soltanto per gli ordini, il tipo di ordine (ad esempio «comprare fino a x EUR»); [In presenza di vari ordini o operazioni che potrebbero costituire abuso di mercato, è possibile trasmettere all'autorità competente i dati sui relativi prezzi e volumi in un allegato della STOR.] [Informazioni sulla cancellazione o modifica dell'ordine tra cui: - natura della modifica (ad esempio modifica del prezzo o della quantità) e entità della modifica In presenza di vari ordini o operazioni che potrebbero costituire abuso di informazioni privilegiate, manipolazione di mercato ovvero tentato abuso di informazioni privilegiate o tentata manipolazione di mercato, è possibile trasmettere all'autorità competente i dati sui relativi prezzi e volumi in un allegato della STOR. - mezzo usato per modificare l'ordine (ad esempio, posta elettronica, telefono ecc.)
--	---

	In caso di segnalazione di un comportamento sospetto connesso al funzionamento del registro distribuito, fornire il maggior numero di dati possibile, compreso l'impatto sulla convalida delle operazioni e il metodo utilizzato per modificare il funzionamento della DLT.]
--	--

SEZIONE 3 — DESCRIZIONE DELLA NATURA DEL SOSPETTO

Natura del sospetto	[Specificare il tipo di violazione in base al quale gli ordini, operazioni e comportamenti connessi al funzionamento della DLT oggetto di segnalazione potrebbero costituire un abuso di mercato.]
Motivi del sospetto	[Descrizione dell'attività (operazioni e ordini, modalità di inoltro degli ordini o di esecuzione delle operazioni e caratteristiche degli ordini e operazioni che li rendono sospetti, comportamenti connessi al funzionamento della DLT) e del modo in cui la questione ha richiamato l'attenzione del segnalante e precisazione dei motivi per sospettare. Per le cripto-attività ammesse alla negoziazione o negoziate in una piattaforma di negoziazione, descrizione della natura dell'interazione con il portafoglio ordini/delle operazioni sul portafoglio ordini che potrebbero costituire abuso di mercato.]

SEZIONE 4 — IDENTIFICAZIONE DELLA PERSONA O DELLE PERSONE RESPONSABILI DEGLI ORDINI, OPERAZIONI O COMPORTAMENTI CONNESSI AL FUNZIONAMENTO DELLA TECNOLOGIA A REGISTRO DISTRIBUITO CHE POTREBBERO COSTITUIRE ABUSO DI MERCATO («I SOSPETTATI»)

Nome	[Per le persone fisiche: nome e cognome] [Per le persone giuridiche: nome completo compresa, se applicabile, la forma giuridica specificata nel registro del paese a norma della cui legge la persona giuridica è costituita; identificativo della persona giuridica (codice LEI) secondo la norma ISO 17442]
-------------	---

Numero di identificazione nazionale	[Numero e/o testo] [Se il numero di identificazione nazionale non è applicabile o noto, indicare la data di nascita (solo per le persone fisiche) nel formato ISO 8601.]
Indirizzo	[Indirizzo completo (ad esempio via, numero civico, codice postale, località, regione/provincia) e Stato]
Informazioni sull'attività professionale Luogo — Posizione	[Informazioni sull'attività professionale del sospettato tratte dalle fonti di cui il soggetto segnalante dispone al suo interno (ad esempio, documentazione del conto per i clienti, dati sul personale per i dipendenti del soggetto segnalante)]
Numero o numeri di conto e indirizzo o indirizzi del portafoglio	[Numero del o dei conti in contante, conti congiunti o deleghe su conti detenuti dal sospettato; indirizzo o indirizzi del portafoglio coinvolti nell'operazione o nel comportamento sospetto]
Identificato del cliente	[Se il sospettato è cliente del soggetto segnalante]
Relazione con l'emittente della crypto-attività in questione	[Descrizione degli eventuali accordi o circostanze o relazioni di natura societaria, contrattuale o organizzativa]
SEZIONE 5 — INFORMAZIONI SUPPLEMENTARI Altre informazioni pertinenti per la segnalazione, a seconda dell'attività	

L'elenco seguente è indicativo e non esaustivo. È possibile fornire altre informazioni ritenute utili dal segnalante, se pertinenti per la STOR.]

- Posizione del sospettato (ad esempio, cliente al dettaglio, ente);
- natura dell'intervento del sospettato (per proprio conto, per conto di un cliente, quale validatore di operazioni in un sistema a registro distribuito, altro);
- se il comportamento sospetto avviene su una DLT, altre informazioni pertinenti possono comprendere:
 - o l'eventualità che l'operazione sia passata attraverso una coda (criptata) di operazioni pubblica o privata (un mempool) prima della sua convalida sulla DLT;
 - o l'eventualità che la DLT sia pubblica (priva di autorizzazioni) o privata (con autorizzazioni);
 - o potenziali interazioni con i contratti intelligenti, compresa l'indicazione dell'indirizzo del contratto e della funzione chiamata;
- entità del portafoglio del sospettato;
- se il sospettato è cliente del soggetto segnalante, data di inizio della relazione professionale;
- tipo di attività dell'unità di negoziazione del sospettato, se disponibile;
- modelli di negoziazione del sospettato; indicativamente possono risultare utili le informazioni seguenti:
 - o abitudini di negoziazione del sospettato;
 - o comparabilità dell'entità dell'ordine/operazione segnalato con l'entità media degli ordini presentati/delle operazioni effettuate dal sospettato negli ultimi 12 mesi;
 - o abitudini del sospettato in termini di cripto-attività negoziate negli ultimi 12 mesi, in particolare indicando se l'ordine/operazione segnalato

riguarda una cripto-attività che il sospettato ha negoziato nell'ultimo anno;

- altri soggetti/persone notoriamente implicati negli ordini o operazioni che potrebbero costituire abuso di mercato;
- attività (ad esempio esecuzione di ordini per conto di clienti, negoziazione per proprio conto, gestione di una piattaforma di negoziazione, convalida delle operazioni).

SEZIONE 6 — DOCUMENTAZIONE ALLEGATA

[Elencare i documenti e il materiale giustificativi allegati alla STOR.]

Esempi di documentazione: messaggi di posta elettronica, registrazioni di conversazioni, registrazioni di ordini o operazioni, registrazioni della tecnologia a registro distribuito, conferme, rapporti dei broker, documenti di delega e commenti dei media se pertinenti.

[Se le informazioni particolareggiate sugli ordini, operazioni e comportamenti connessi al funzionamento della tecnologia a registro distribuito previste alla sezione 2 sono comunicate in un allegato distinto, indicare il titolo di tale allegato.]