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

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 ([1]), in particolare l'articolo 92, paragrafo 2, terzo comma,

considerando quanto segue:

(1) È necessario stabilire requisiti applicabili ai dispositivi, alle procedure e ai sistemi di cui chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività deve disporre per segnalare ordini, operazioni e altri aspetti del funzionamento della tecnologia a registro distribuito (DLT), compreso il meccanismo di consenso, laddove vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso. Tali requisiti sono essenziali e dovrebbero aiutare a prevenire e individuare gli abusi di mercato. Dovrebbero inoltre contribuire a far sì che le segnalazioni di ragionevoli sospetti su ordini, operazioni e altri aspetti del funzionamento della tecnologia a registro distribuito (STOR) trasmesse alle autorità competenti siano significative, complete e utili.

(2) Per garantire che la prevenzione e l'individuazione degli abusi di mercato siano efficaci, si dovrebbero approntare sistemi adeguati per monitorare gli ordini, le operazioni e altri aspetti del funzionamento della DLT, in base alla scala, alle dimensioni e alla natura dell'attività professionale della persona che predispone o esegue a titolo professionale operazioni. Tali sistemi dovrebbero prevedere un'analisi umana effettuata da personale formato adeguatamente sulla base di informazioni oggettive a disposizione del soggetto segnalante. Il soggetto segnalante dovrebbe raccogliere dati personali supplementari solo per garantire un'adeguata analisi umana. Per consentire un'analisi più approfondita dei potenziali casi di abuso di informazioni privilegiate, manipolazione di mercato ovvero tentato abuso di informazioni privilegiate o tentata manipolazione di mercato, i sistemi di monitoraggio degli abusi di mercato dovrebbero essere in grado di produrre un allarme in funzione di parametri predefiniti. L'accesso a tali allarmi dovrebbe essere registrato per assicurare che essi siano utilizzati esclusivamente per individuare abusi di mercato. È probabile che il processo nel suo insieme richieda un certo livello di automazione.

(3) Allo scopo di analizzare l'adeguatezza dei dispositivi, dei sistemi e delle procedure per prevenire e individuare gli abusi di mercato, è necessario valutare l'impatto che la persona che predispone o esegue a titolo professionale le operazioni può esercitare sul mercato. Nell'ambito di questa valutazione tali persone dovrebbero valutare se detengono una posizione significativa o dominante in qualsiasi segmento di attività del mercato delle cripto-attività; in tal caso dispositivi, sistemi e procedure dovrebbero essere proporzionati alla loro posizione.

(4) La prevenzione e l'individuazione degli abusi di mercato richiedono un monitoraggio continuo di tutti gli ordini e le operazioni predisposti o eseguiti da chiunque predisponga o esegua a titolo professionale operazioni, indipendentemente dal fatto che tali ordini e operazioni siano eseguiti nel registro distribuito («on-chain») o al di fuori del registro distribuito («off-chain»), compresi i trasferimenti di cripto-attività da o verso conti di clienti dello stesso prestatore di servizi per le cripto-attività.

([1]) GU L 150 del 9.6.2023, pag. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

(5) Per favorire e promuovere in tutta l'Unione la coerenza dell'impostazione e delle pratiche in materia di prevenzione, individuazione e sanzione degli abusi di mercato, è necessario prevedere modalità che armonizzino il contenuto, il modello e i tempi delle segnalazioni di sospetti su ordini, operazioni e altri aspetti del funzionamento della DLT.

(6) Per condividere risorse, sviluppare e mantenere sistemi di monitoraggio a livello centrale e creare competenze di monitoraggio degli ordini e delle operazioni sospetti, chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività dovrebbe poter delegare all'interno di un gruppo la prevenzione e l'individuazione di tali ordini, operazioni e altri aspetti del funzionamento della DLT sospetti, o delegare l'analisi dei dati e la generazione degli allarmi, a condizioni adeguate. La delega non dovrebbe impedire alle autorità competenti di valutare in qualsiasi momento se i dispositivi, sistemi e procedure del delegato siano effettivamente in linea con l'obbligo di prevenire e individuare gli abusi di mercato. L'obbligo di segnalazione e la responsabilità di conformarsi al presente regolamento e all'articolo 92 del regolamento (UE) 2023/1114 dovrebbero rimanere in capo al delegante.

(7) I prestatori di servizi per le cripto-attività che gestiscono una piattaforma di negoziazione dovrebbero disporre di regole di negoziazione adeguate che contribuiscano a prevenire gli abusi di mercato. Tali soggetti dovrebbero inoltre dotarsi di sistemi che permettano di ripercorrere il portafoglio ordini al fine di analizzare l'attività di negoziazione.

Un modello unico e armonizzato per la trasmissione elettronica delle segnalazioni di ordini e operazioni sospetti («STOR») dovrebbe favorire, nelle indagini transfrontaliere, un efficiente scambio di informazioni tra le autorità competenti sugli ordini e le operazioni sospetti.

(8) Se compilati all'insegna della chiarezza, completezza, oggettività e accuratezza, i campi informativi di questo modello STOR dovrebbero aiutare le autorità competenti a valutare prontamente tali ordini e operazioni sospetti e ad adottare gli interventi necessari. Il modello STOR dovrebbe pertanto consentire alla persona che trasmette la STOR di inserire le informazioni che le autorità competenti ritengono pertinenti circa i sospetti sugli ordini, le operazioni o altri aspetti del funzionamento della tecnologia a registro distribuito segnalati, esponendo i motivi che la inducono a sospettare. Il modello STOR dovrebbe inoltre consentire alla persona che trasmette la STOR l'inserimento di dati personali che permettano di identificare le persone implicate nell'attività sospetta e di aiutare le autorità competenti nelle loro indagini. Tali dati dovrebbero essere disponibili fin dall'inizio per non compromettere l'integrità dell'indagine obbligando potenzialmente l'autorità competente a rivolgersi, a indagine avviata, alla persona che ha trasmesso la STOR. Ai sensi del presente regolamento i dati personali dovrebbero essere trattati conformemente al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il principio della minimizzazione dei dati dovrebbe essere rispettato in particolare quando i dati personali sono raccolti per garantire il rispetto del presente regolamento.

(9) Per facilitare la STOR, il modello dovrebbe offrire la possibilità di accludere i documenti e il materiale di supporto della notifica necessari, anche sotto forma di allegato in cui sono elencati gli ordini o le operazioni sospetti, con indicazione dei relativi prezzi e volumi. Il modello STOR dovrebbe inoltre consentire la segnalazione di comportamenti sospetti connessi al funzionamento della DLT.

(10) Le persone che predispongono o eseguono a titolo professionale operazioni in cripto-attività non dovrebbero notificare tutti gli ordini ricevuti e le operazioni effettuate che hanno determinato un allarme interno. Siffatto obbligo sarebbe in contrasto con l'obbligo di valutare caso per caso se sussistano motivi ragionevoli per sospettare.

(11) L'analisi degli ordini, delle operazioni o di altri aspetti del funzionamento della DLT dovrebbe tenere conto non solo delle informazioni interne della persona che predispone o esegue a titolo professionale operazioni in cripto-attività, ma di tutte le informazioni pubblicamente disponibili, comprese le informazioni sulle operazioni incorporate in un sistema di registro pubblico.

([2]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Le STOR dovrebbero essere trasmesse all'autorità competente immediatamente all'emergere di un ragionevole sospetto circa l'esistenza di abusi di mercato. L'analisi volta a stabilire se l'ordine o l'operazione vadano considerati sospetti dovrebbe basarsi sui fatti e non su ipotesi o congetture e dovrebbe essere effettuata in tempi il più possibile brevi. Ritardare la trasmissione di una segnalazione al fine di integrarvi ulteriori sospetti su ordini, operazioni o altri aspetti del funzionamento della DLT, oppure accumulare varie STOR, sarebbe inconciliabile con l'obbligo di agire senza indugio laddove sia già emerso un ragionevole sospetto. In ogni caso chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività dovrebbe valutare caso per caso se sia possibile segnalare in un'unica STOR vari ordini, operazioni o altri aspetti del funzionamento della DLT.

(13) Può verificarsi che il ragionevole sospetto di abusi di mercato emerga a distanza di tempo dal compimento dell'attività sospetta grazie a eventi verificatisi o informazioni resesi disponibili successivamente. Questo non dovrebbe costituire un motivo per non segnalare l'attività sospetta all'autorità competente. In tale specifica situazione la persona che trasmette la STOR dovrebbe essere in grado di dimostrare di aver rispettato gli obblighi di segnalazione giustificando lo sfasamento temporale tra il compimento dell'attività sospetta e l'emergere del ragionevole sospetto che sia stato commesso, sia in atto o possa essere commesso un abuso di mercato.

(14) Per formarsi un'opinione nei successivi casi di ordini o operazioni sospetti, chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività dovrebbe poter recuperare ed esaminare le analisi sia delle STOR effettivamente trasmesse, sia degli ordini, delle operazioni e dei comportamenti connessi al funzionamento della DLT sospetti che sono stati analizzati, ma per i quali le autorità competenti interessate hanno poi concluso la non ragionevolezza dei motivi di sospetto.

(15) Per prevenire il più possibile gli abusi di mercato, chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività dovrebbe essere in grado di perfezionare i sistemi di sorveglianza e individuare modelli reiterati di comportamento la cui somma, considerata nell'insieme, potrebbe determinare un ragionevole sospetto di abusi di mercato. Tali persone dovrebbero pertanto essere tenute ad analizzare ordini, operazioni, comportamenti e altri aspetti sospetti connessi al funzionamento della tecnologia a registro distribuito da cui non è scaturita una STOR e a registrare tali analisi. Tali registrazioni dovrebbero inoltre aiutare queste persone a dimostrare la conformità all'articolo 92 del regolamento (UE) 2023/1114 e dovrebbero agevolare le autorità competenti nell'esercizio delle loro funzioni di vigilanza, di indagine e di contrasto a norma dell'articolo 92 del regolamento (UE) 2023/1114.

(16) Considerando che i mercati delle cripto-attività sono intrinsecamente transfrontalieri, è necessario specificare le procedure di coordinamento tra le autorità competenti per individuare e sanzionare i casi di abusi di mercato transfrontalieri. Tali procedure di coordinamento dovrebbero scongiurare la possibilità di indagini o attività di contrasto confliggenti. In tale contesto tra gli abusi di mercato transfrontalieri dovrebbero rientrare i casi in cui in uno Stato membro si effettuano operazioni sospette riguardanti una cripto-attività ammessa alla negoziazione in un altro Stato membro, nonché i casi in cui il prestatore di servizi per le cripto-attività interessato opera in più di uno Stato membro.

(17) È necessario stabilire disposizioni per la trasmissione delle STOR tra le autorità competenti. In assenza di un regime di segnalazione delle operazioni, tali requisiti sono fondamentali per garantire l'efficienza della vigilanza e delle attività di contrasto, evitando nel contempo la trasmissione di un flusso massiccio di informazioni che non sarebbero utili per l'autorità ricevente.

(18) Il presente regolamento si basa sui progetti di norme tecniche di regolamentazione che l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) ha presentato alla Commissione.

(19) L'ESMA ha svolto consultazioni pubbliche sui progetti di norme tecniche di regolamentazione su cui si basa il presente regolamento, ne ha analizzato i potenziali costi e benefici e ha richiesto la consulenza del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati, istituito dall'articolo 37 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([3]).

([3]) Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 ([4]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 22 gennaio 2025,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «segnalazione di ordini e operazioni sospetti» (STOR): segnalazione degli ordini o delle operazioni sospetti - compresa qualsiasi cancellazione o modifica degli stessi - e di altri aspetti del funzionamento della DLT sospetti qualora vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso;

2) «mezzo elettronico»: attrezzatura elettronica per il trattamento (compresa la compressione digitale), lo stoccaggio e la trasmissione di dati tramite cavo, onde radio, tecnologie ottiche o qualsiasi altro mezzo elettromagnetico;

3) «gruppo»: gruppo ai sensi dell'articolo 2, punto 11), della direttiva 2013/34/UE del Parlamento europeo e del Consiglio ([5]);

4) «ordine»: ogni singolo ordine, compresa ogni singola quotazione, sia esso volto alla prima presentazione, alla modifica, all'aggiornamento o alla cancellazione di un ordine e quale ne sia la tipologia.

Articolo 2

Obblighi generali

1. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività istituisce e mantiene dispositivi, sistemi e procedure per:

a) monitorare efficacemente e su base continuativa tutti gli ordini ricevuti e trasmessi e tutte le operazioni in cripto-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 STOR alle autorità competenti in adempimento degli obblighi imposti dal presente regolamento, utilizzando il modello riportato nell'allegato.

([4]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE del Consiglio (GU L 182 del 29.6.2013, pag. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

2. Gli obblighi di cui al paragrafo 1 si applicano agli ordini, alle operazioni e ad altri aspetti del funzionamento della DLT che potrebbero costituire abuso di mercato e si applicano a prescindere dai seguenti elementi:

a) la veste in cui l'ordine è inoltrato o l'operazione è eseguita;

b) la tipologia di clienti interessata;

c) il luogo in cui l'ordine è inoltrato o l'operazione è eseguita, sia esso su una piattaforma di negoziazione o al di fuori di essa.

3. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività provvede affinché i dispositivi, sistemi e procedure di cui al paragrafo 1 siano:

a) adeguati e proporzionati alla scala, alle dimensioni e alla natura delle loro attività professionale;

b) valutati periodicamente, almeno mediante verifica interna annuale, e aggiornati quando necessario;

c) documentati chiaramente per iscritto, con eventuali modifiche o aggiornamenti, ai fini della conformità al presente regolamento, e la documentazione informativa sia conservata per un periodo di cinque anni.

4. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività comunica, su richiesta, all'autorità competente le informazioni sulla valutazione di cui al paragrafo 3, comprese le informazioni sul livello di automazione messo in atto.

Articolo 3

Prevenzione, monitoraggio e rilevamento

1. I dispositivi, sistemi e procedure di cui all'articolo 92, paragrafo 1, del regolamento (UE) 2023/1114:

a) coprono l'intera gamma delle attività di negoziazione intraprese dalle persone che predispongono o eseguono a titolo professionale operazioni in cripto-attività;

b) generano allarmi per indicare le attività per le quali è necessario approfondire l'analisi al fine di individuare potenziali abusi di mercato;

c) consentono ai prestatori di servizi per le cripto-attività che gestiscono una piattaforma di negoziazione di:

   i) effettuare l'analisi individuale e comparativa di ogni singola operazione eseguita e di ogni singolo ordine inoltrato, modificato, cancellato o rifiutato nei sistemi della piattaforma di negoziazione;

   ii) impedire il reiterarsi di comportamenti osservati sulla stessa piattaforma di negoziazione;

d) permettere a chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività di effettuare l'analisi individuale e comparativa di ogni singola operazione eseguita e di ogni singolo ordine inoltrato, modificato, cancellato o rifiutato all'interno e al di fuori di una piattaforma di negoziazione, a prescindere dal fatto che gli ordini e le operazioni siano inoltrati ed eseguiti tramite il registro distribuito, nonché degli aspetti del funzionamento della DLT che potrebbero costituire abuso di mercato.

2. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività istituisce e mantiene dispositivi e procedure che assicurano un livello adeguato di analisi umana per la prevenzione, il monitoraggio, il rilevamento e l'individuazione delle operazioni, degli ordini e degli aspetti del funzionamento della tecnologia a registro distribuito che indicano la probabilità o l'esistenza di comportamenti di abuso di mercato. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività raccoglie dati personali supplementari al solo scopo di assicurare un livello adeguato di analisi umana.

3. Ai fini dell'articolo 92, paragrafo 1, del regolamento (UE) 2023/1114**,** chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività utilizza sistemi TIC in misura adeguata e proporzionata alla scala, alle dimensioni e alla natura della propria attività professionale.

Tra i sistemi TIC di cui al primo comma figurano sistemi TIC che permettono la lettura automatizzata differita e la possibilità di ripercorrere e analizzare i dati del portafoglio ordini. Tali sistemi hanno capacità sufficiente per operare in ambiente di negoziazione algoritmica.

Ai fini del secondo comma, per negoziazione algoritmica si intende la negoziazione di cripto-attività in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, tra cui se avviare l'ordine, i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presentazione, con intervento umano minimo o nullo e non comprende i sistemi utilizzati unicamente per trasmettere ordini a una o più piattaforme di negoziazione, per trattare ordini che non comportano la determinazione di parametri di trading, per confermare ordini o per eseguire il trattamento post-negoziazione delle operazioni eseguite.

4. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività può, con accordo scritto, esternalizzare a terzi o delegare a una persona giuridica facente parte dello stesso gruppo, quale definito all'articolo 2, punto 11), della direttiva 2013/34/UE del Parlamento europeo e del Consiglio ([6]), («prestatori del servizio»), le funzioni relative a prevenzione, monitoraggio, rilevamento e individuazione di ordini, operazioni o altri aspetti del funzionamento della DLT che potrebbero costituire abuso di mercato, tra cui l'analisi dei dati, compresi i dati sugli ordini e sulle operazioni, e la generazione degli allarmi. Chiunque deleghi o esternalizzi tali funzioni rimane pienamente responsabile del rispetto di tutti gli obblighi che gli incombono a norma del presente regolamento e dell'articolo 92 del regolamento (UE) 2023/1114. Qualora tali funzioni siano esternalizzate a terzi, le persone che esternalizzano tali funzioni rispettano in ogni momento i seguenti requisiti:

a) mantengono le competenze e le risorse necessarie per:

   i) valutare la qualità dei servizi prestati e l'adeguatezza organizzativa dei prestatori dei servizi;

   ii) vigilare sui servizi esternalizzati;

   iii) gestire i rischi associati all'esternalizzazione di tali funzioni su base continuativa;

b) hanno accesso diretto a tutte le pertinenti informazioni relative all'analisi dei dati e alla generazione degli allarmi.

L'accordo scritto di cui al primo comma illustra i diritti e gli obblighi della persona che delega o esternalizza le funzioni e quelli del prestatore del servizio. Stabilisce i motivi in base ai quali la persona che delega o esternalizza le funzioni può cessare l'accordo.

5. Nell'ambito dei dispositivi, dei sistemi e delle procedure di cui al primo e al secondo comma, chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività conserva per un periodo di 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. Tali informazioni comprendono l'analisi effettuata e i motivi che hanno indotto a trasmettere la STOR o viceversa a non trasmetterla. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività comunica tali informazioni all'autorità competente su richiesta di quest'ultima.

([6]) Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE del Consiglio (GU L 182 del 29.6.2013, pag. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

Articolo 4

Formazione

Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività organizza e impartisce una formazione efficace e completa al personale incaricato di prevenire, monitorare, rilevare e individuare gli ordini, le operazioni e gli altri aspetti del funzionamento della DLT che potrebbero indicare l'esistenza di abusi di mercato, compreso il personale incaricato dell'elaborazione degli ordini e delle operazioni o del funzionamento della DLT. La formazione è offerta periodicamente ed è adeguata e proporzionata alla scala, alle dimensioni e alla natura dell'attività professionale svolta.

Articolo 5

Segnalazione di ordini o operazioni sospetti

1. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività istituisce e mantiene dispositivi, sistemi e procedure efficaci per poter valutare, ai fini della trasmissione della STOR, se in merito a un ordine, un'operazione o altri aspetti della DLT vi possano essere circostanze che indichino che un abuso di mercato sia stato commesso, sia in atto o possa essere commesso. Tali dispositivi, sistemi e procedure comprendono un livello adeguato di analisi umana.

2. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività trasmette la STOR:

a) utilizzando il modello STOR di cui all'allegato e 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;

b) tramite il mezzo elettronico indicato dall'autorità stessa.

Ai fini del primo comma, lettera b), l'autorità competente indica sul proprio sito Internet il mezzo elettronico da utilizzare e assicura che quest'ultimo lasci impregiudicate la completezza, l'integrità e la riservatezza delle informazioni durante la trasmissione.

La STOR di cui al primo comma si basa su fatti e analisi, tenendo conto di tutte le informazioni di cui dispongono le persone che predispongono o eseguono a titolo professionale operazioni in cripto-attività.

3. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività garantisce e preserva la riservatezza delle informazioni contenute nella segnalazione di ordini o operazioni sospetti; garantisce inoltre che né al soggetto nei cui confronti la STOR è creata, né a chiunque altro non sia tenuto a esserne a conoscenza per la funzione svolta o la posizione occupata presso il segnalante, giungano informazioni relative:

a) alla generazione degli allarmi di cui all'articolo 3, paragrafo 1, lettera b);

b) alla valutazione che può condurre alla trasmissione di una STOR;

c) al fatto che il segnalante completerà la STOR senza inviare richieste di informazioni alla persona nei cui confronti la STOR può essere creata per completare determinati campi;

d) alla trasmissione di una STOR all'autorità competente o all'intenzione di trasmetterla.

Articolo 6

Tempi della STOR

1. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività assicura di disporre di dispositivi, sistemi e procedure efficaci per trasmettere una STOR immediatamente all'emergere di un ragionevole sospetto di abuso di mercato.

2. I dispositivi, sistemi e procedure di cui al paragrafo 1 contemplano la possibilità di trasmettere STOR relative a operazioni, ordini o altri aspetti del funzionamento della DLT passati se il sospetto emerge grazie a eventi verificatisi o informazioni resesi disponibili successivamente. In siffatti casi chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività spiega nella STOR i motivi dello sfasamento temporale tra la presunta violazione e la trasmissione della STOR, illustrando le circostanze specifiche del caso.

3. Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività comunica all'autorità competente tutte le informazioni supplementari di cui sia venuto a conoscenza dopo la trasmissione della STOR e fornisce qualsiasi informazione o documento richiesti dall'autorità competente.

Articolo 7

Scambio di segnalazioni tra autorità competenti

1. Le autorità competenti trasmettono le STOR utilizzando il formulario per la trasmissione spontanea di informazioni di cui all'allegato IV del regolamento di esecuzione (UE) 2024/2545 della Commissione ([7]).

2. L'autorità competente mittente allega la STOR al formulario di cui al paragrafo 1, ma non è tenuta a tradurla nella lingua dell'autorità competente ricevente. L'autorità competente mittente include eventuali documenti supplementari forniti nella STOR che specificano la base giuridica per la comunicazione delle informazioni.

Articolo 8

Procedure di coordinamento per individuare e sanzionare gli abusi di mercato transfrontalieri

1. L'autorità competente che sospetta si sia verificato, possa essersi verificato o si stia verificando un abuso di mercato transfrontaliero comunica senza indebito ritardo lo status della propria valutazione preliminare alle altre autorità competenti interessate, comprese se del caso le autorità competenti delle piattaforme di negoziazione in cui la cripto-attività è ammessa alla negoziazione.

Una volta informate in merito ad abusi di mercato transfrontalieri, le autorità competenti riceventi condividono, senza indebito ritardo, informazioni sulla pianificazione o sull'esistenza di qualsiasi attività o misura di vigilanza o, se del caso e se tali informazioni sono a disposizione dell'autorità competente ricevente, in merito a un'indagine penale esistente sullo stesso caso.

2. Le autorità competenti interessate:

a) si aggiornano periodicamente a vicenda in merito agli abusi di mercato transfrontalieri;

b) si informano a vicenda in merito a importanti sviluppi sopraggiunti nell'intervallo relativi ad abusi di mercato transfrontalieri;

c) coordinano le azioni di vigilanza e di contrasto.

([7]) Regolamento di esecuzione (UE) 2024/2545 della Commissione, del 24 settembre 2024, che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio per quanto riguarda formati, modelli e procedure standard per la cooperazione e lo scambio di informazioni tra le autorità competenti (GU L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

3. L'autorità competente che ha formalmente avviato un'indagine o un'attività di contrasto o, se del caso, che è a conoscenza di un'indagine penale ne informa le altre autorità competenti interessate, comprese, se del caso, le autorità competenti delle piattaforme di negoziazione in cui la cripto-attività è ammessa alla negoziazione. L'autorità competente segnalante può informare l'ESMA.

4. Le autorità competenti che hanno avviato un'indagine o un'attività di contrasto in un contesto transfrontaliero, o vi hanno partecipato, possono chiedere il coordinamento dell'ESMA.

5. Ai fini del presente articolo, per «abusi di mercato transfrontalieri» si intende una delle situazioni seguenti:

a) una situazione in cui più di un'autorità competente è competente a individuare, indagare o sanzionare un potenziale caso di abuso di mercato;

b) una situazione in cui è necessaria la cooperazione tra due o più autorità competenti per individuare, indagare o sanzionare un potenziale caso di abuso di mercato.

Articolo 9

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 29 aprile 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Modello per la segnalazione di ordine o operazione sospetti (STOR)

Si noti che **tutti** *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

Chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività — Specificare per ogni caso

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 cripto-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 cripto-attività	Descrivere la cripto-attività o le cripto-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 cripto-attività, le attività, gli ordini e le operazioni effettuati) o la descrizione della cripto-attività in assenza del DTI. Se il comportamento sospetto riguarda una coppia di negoziazione, elencare entrambe le cripto-attività della coppia; — il tipo di cripto-attività (token collegato ad attività, token di moneta elettronica, altra cripto-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 cripto-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]
Identificativo del cliente	[Se il sospettato è cliente del soggetto segnalante]
Relazione con l'emittente della cripto-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:
  — l'eventualità che l'operazione sia passata attraverso una coda (criptata) di operazioni pubblica o privata (un mempool) prima della sua convalida sulla DLT;
  — l'eventualità che la DLT sia pubblica (priva di autorizzazioni) o privata (con autorizzazioni);
  — 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:
  — abitudini di negoziazione del sospettato;
  — comparabilità dell'entità dell'ordine/operazione segnalato con l'entità media degli ordini presentati/delle operazioni effettuate dal sospettato negli ultimi 12 mesi;
  — 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:
  — nomi;
— 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.]

([1]) Regolamento delegato (UE) 2025/1140 della Commissione, del 27 febbraio 2025, che integra il regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano le registrazioni da conservare relative a tutti i servizi per le cripto-attività, le attività, gli ordini e le operazioni effettuati (GU L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).