REGOLAMENTO DELEGATO (UE) 2025/303 DELLA COMMISSIONE

del 31 ottobre 2024

che integra il regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano le informazioni che devono essere incluse da talune entità finanziarie nella notifica dell'intenzione di prestare servizi per le cripto-attività

(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 60, paragrafo 13, terzo comma,

considerando quanto segue:

(1) Per consentire alle autorità competenti di valutare se talune entità finanziarie che intendono prestare servizi per le cripto-attività soddisfano i requisiti applicabili di cui al titolo V e, se del caso, al titolo VI del regolamento (UE) 2023/1114, le informazioni che devono essere comunicate da tali entità in merito alla loro intenzione di prestare servizi per le cripto-attività dovrebbero essere sufficientemente dettagliate e complete senza comportare oneri indebiti.

(2) Conformemente all'articolo 60, paragrafo 7, lettera a), del regolamento (UE) 2023/1114, una notifica dell'intenzione di prestare servizi per le cripto-attività deve contenere un programma operativo. Al fine di fornire un quadro completo delle operazioni che l'ente notificante intende effettuare, il programma operativo dovrebbe comprendere una descrizione della struttura organizzativa dell'ente notificante, della sua strategia di prestazione di servizi per le cripto-attività ai clienti destinatari e della sua capacità operativa per i tre anni successivi alla data della notifica. Per quanto riguarda la strategia utilizzata per rivolgersi ai clienti, l'ente notificante dovrebbe descrivere i mezzi di marketing che intende utilizzare, compresi siti web, applicazioni di telefonia mobile, riunioni in presenza, comunicati stampa o qualsiasi forma di mezzo fisico o elettronico, tra cui strumenti per campagne sui social media, annunci pubblicitari o banner su Internet, reindirizzamento della pubblicità, accordi con influencer, accordi di sponsorizzazione, chiamate, webinar, inviti a eventi, campagne di affiliazione, tecniche di ludicizzazione, inviti a compilare un modulo di risposta o a seguire un corso di formazione, account dimostrativi o materiale didattico.

(3) Per consentire alle autorità competenti di valutare la resilienza dell'ente notificante in termini di resistenza agli shock finanziari esterni, compresi quelli riguardanti il valore delle cripto-attività, l'ente notificante dovrebbe includere nella notifica scenari di stress che simulino eventi gravi ma plausibili nel piano contabile previsionale.

(4) Per evitare interruzioni delle attività che potrebbero avere gravi conseguenze sul piano finanziario, regolamentare e reputazionale per l'ente notificante e più in generale per i mercati delle cripto-attività, è fondamentale mantenere le attività o almeno le funzioni essenziali dei prestatori di servizi per le cripto-attività e ridurre al minimo i tempi di inattività dovuti a perturbazioni impreviste, compresi gli attacchi informatici e le calamità naturali. Una notifica dovrebbe pertanto contenere informazioni dettagliate sui dispositivi dell'ente notificante per garantire la continuità e la regolarità della prestazione di servizi per le cripto-attività, compresa una descrizione dettagliata dei rischi e dei piani di continuità operativa.

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

(5) Sono necessari meccanismi, sistemi e procedure efficaci conformi alla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio ([2]) per garantire che gli enti notificanti affrontino adeguatamente i rischi e le pratiche di riciclaggio di denaro e finanziamento del terrorismo nella prestazione di servizi per le cripto-attività. Gli enti notificanti dovrebbero pertanto fornire nella notifica informazioni dettagliate sui meccanismi, i sistemi e le procedure messi in atto per prevenire i rischi associati alle loro attività commerciali in relazione, tra l'altro, alla lotta al riciclaggio di denaro e al finanziamento del terrorismo.

(6) Data la natura decentrata e digitale delle cripto-attività, i rischi di cibersicurezza per i prestatori di servizi per le cripto-attività sono significativi e assumono molteplici forme. Per garantire che l'ente notificante sia in grado di prevenire violazioni dei dati e perdite finanziarie che potrebbero essere causate da attacchi informatici, le informazioni sui sistemi TIC utilizzati dall'ente notificante e sui relativi dispositivi di sicurezza di cui all'articolo 60, paragrafo 7, lettera c), del regolamento (UE) 2023/1114, quali l'identità e l'ubicazione geografica dei prestatori, la descrizione delle attività o dei servizi TIC esternalizzati con le loro caratteristiche principali, la copia degli accordi contrattuali, dovrebbero includere le risorse umane destinate ad affrontare i rischi di cibersicurezza.

(7) La separazione delle cripto-attività e dei fondi dei clienti protegge questi ultimi dalle perdite del prestatore di servizi per le cripto-attività e dall'uso improprio delle loro cripto-attività e dei loro fondi. L'articolo 70 del regolamento (UE) 2023/1114 impone pertanto ai prestatori di servizi per le cripto-attività di adottare disposizioni adeguate per tutelare i diritti di titolarità dei clienti. Tale obbligo si applica anche ai prestatori di servizi per le cripto-attività che non prestano servizi di custodia e amministrazione.

(8) Per consentire alle autorità competenti di valutare l'adeguatezza delle norme operative dell'ente notificante per le proprie piattaforme di negoziazione di cripto-attività, l'ente notificante dovrebbe specificare determinati elementi nella descrizione di tali norme. In particolare dovrebbe approfondire gli aspetti delle norme operative che riguardano l'ammissione alla negoziazione, la negoziazione e il regolamento delle cripto-attività. Per quanto riguarda l'ammissione alla negoziazione di cripto-attività, gli enti notificanti dovrebbero fornire informazioni dettagliate sul modo in cui le cripto-attività ammesse rispettano le norme dell'ente notificante, sui tipi di cripto-attività che l'ente notificante non ammetterà alla negoziazione sulla sua piattaforma di negoziazione e sui motivi di tali esclusioni, nonché sulle commissioni per l'ammissione alla negoziazione. Per quanto riguarda la negoziazione di cripto-attività, l'ente notificante dovrebbe specificare gli elementi delle norme operative che disciplinano l'esecuzione e la cancellazione degli ordini, la negoziazione ordinata, la trasparenza e la tenuta delle registrazioni. Infine l'ente notificante dovrebbe includere nella descrizione delle norme operative gli elementi che disciplinano il regolamento delle operazioni in cripto-attività sulla piattaforma di negoziazione, indicando se il regolamento è avviato utilizzando la tecnologia a registro distribuito (DLT), i tempi di avvio dell'esecuzione, la definizione del momento in cui il regolamento è definitivo, tutte le verifiche necessarie per garantire l'efficace regolamento dell'operazione e qualsiasi misura volta a limitare i mancati regolamenti.

(9) Per consentire alle autorità competenti di valutare l'adeguatezza dell'ente notificante a prestare determinati servizi per le cripto-attività quali lo scambio di cripto-attività con fondi o altre cripto-attività, l'esecuzione, la prestazione di consulenza sulle cripto-attività o di servizi di gestione di portafogli di cripto-attività e servizi di trasferimento, l'ente notificante dovrebbe specificare i dettagli delle modalità di prestazione di tali servizi per le cripto-attività nonché le disposizioni messe in atto per garantire che l'ente notificante rispetti le pertinenti disposizioni del regolamento (UE) 2023/1114 per quanto riguarda la prestazione di tali servizi per le cripto-attività.

(10) Qualsiasi trattamento dei dati personali nel quadro del presente regolamento è conforme alle prescrizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]).

([2]) Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (GU L 141 del 5.6.2015, pag. 73, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

([3]) 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).

(11) 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 ed elaborato in stretta cooperazione con l'Autorità bancaria europea.

(12) L'ESMA ha condotto consultazioni pubbliche sui progetti di norme tecniche di regolamentazione sui quali si basa il presente regolamento, ha analizzato i potenziali costi e benefici collegati e ha chiesto 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 ([4]).

(13) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([5]), il Garante europeo della protezione dei dati è stato consultato e ha formulato osservazioni formali il 21 giugno 2024,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Programma operativo

1. Ai fini dell'articolo 60, paragrafo 7, lettera a), del regolamento (UE) 2023/1114, l'ente notificante fornisce all'autorità competente il programma operativo per i tre anni successivi alla data della notifica, comprese le informazioni seguenti:

a) se l'ente notificante appartiene a un gruppo quale definito all'articolo 2, punto 11), della direttiva 2013/34/UE del Parlamento europeo e del Consiglio ([6]), una spiegazione del modo in cui le attività dell'ente notificante si inseriscono nella strategia di tale gruppo e interagiscono con le attività degli altri soggetti di tale gruppo, compresa una panoramica dell'organizzazione e della struttura attuali e previste di tale gruppo;

b) una spiegazione del modo in cui si prevede che le attività dei soggetti affiliati all'ente notificante, anche nel caso in cui vi siano soggetti regolamentati all'interno del gruppo, incideranno sulle attività dell'ente notificante, compresi un elenco dei soggetti affiliati all'ente notificante e informazioni su di essi e, nel caso in cui vi siano soggetti regolamentati, i servizi prestati da tali soggetti e i nomi di dominio di ciascun sito web gestito da tali soggetti;

c) un elenco dei servizi per le cripto-attività che l'ente notificante intende prestare e i tipi di cripto-attività cui i servizi per le cripto-attività si riferiranno;

d) altre attività pianificate, regolamentate conformemente al diritto dell'Unione o nazionale o non regolamentate, compresi i servizi diversi dai servizi per le cripto-attività, che l'ente notificante intende prestare;

e) se l'ente notificante intende offrire cripto-attività al pubblico o chiede l'ammissione alla negoziazione di cripto-attività e, in tal caso, quale tipo di cripto-attività;

f) un elenco delle giurisdizioni, sia nell'Unione che nei paesi terzi, in cui l'ente notificante prevede di prestare servizi per le cripto-attività, comprese informazioni sul numero previsto di clienti per area geografica;

g) i tipi di potenziali clienti cui si rivolgono i servizi per le cripto-attività dell'ente notificante;

([4]) 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).

([5]) 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).

([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).

h) una descrizione dei mezzi di accesso dei clienti ai servizi per le cripto-attività dell'ente notificante, compresi tutti gli elementi seguenti:

   i) i nomi di dominio per ciascun sito web o altra applicazione basata sulle TIC attraverso cui l'ente notificante presterà i servizi per le cripto-attività e le informazioni sulle lingue in cui il sito web o altra applicazione basata sulle TIC sarà disponibile, i tipi di servizi per le cripto-attività cui si potrà accedere tramite tale sito web o altra applicazione basata sulle TIC e, se del caso, da quali Stati membri il sito web o altra applicazione basata sulle TIC sarà accessibile;

   ii) il nome di qualsiasi applicazione basata sulle TIC a disposizione dei clienti per accedere ai servizi per le cripto-attività, le lingue in cui tale applicazione basata sulle TIC è disponibile e i servizi per le cripto-attività cui è possibile accedere mediante tale applicazione basata sulle TIC;

i) le attività e le modalità promozionali e di marketing previste per i servizi per le cripto-attività, compreso quanto segue:

   i) tutti i mezzi di marketing da utilizzare per ciascuno dei servizi;

   ii) i mezzi di identificazione previsti dell'ente notificante;

   iii) informazioni sulla categoria pertinente di clienti destinatari;

   iv) i tipi di cripto-attività;

   v) le lingue che saranno utilizzate per le attività promozionali e di marketing;

j) una descrizione dettagliata delle risorse umane, finanziarie e TIC assegnate ai servizi per le cripto-attività previsti e la loro ubicazione geografica;

k) la politica di esternalizzazione dell'ente notificante e il modo in cui è stata adattata ai servizi per le cripto-attività, nonché una descrizione dettagliata degli accordi di esternalizzazione previsti dell'ente notificante, compresi gli accordi infragruppo, e il modo in cui l'ente notificante si conformerà all'articolo 73 del regolamento (UE) 2023/1114, compresi informazioni sulla funzione o sulla persona responsabile dell'esternalizzazione, sulle risorse umane e TIC destinate al controllo delle funzioni, dei servizi o delle attività esternalizzati dei relativi accordi e sulla valutazione del rischio connessa all'esternalizzazione;

l) l'elenco dei soggetti che presteranno i servizi esternalizzati per la prestazione di servizi per le cripto-attività, la loro ubicazione geografica e i servizi esternalizzati pertinenti;

m) un piano contabile previsionale comprendente scenari di stress a livello individuale e, se del caso, a livello consolidato di gruppo e subconsolidato conformemente alla direttiva 2013/34/UE, tenendo conto di eventuali prestiti infragruppo che l'ente notificante ha concesso o concederà o che ad esso sono stati o saranno concessi;

n) qualsiasi scambio di cripto-attività con fondi e altre cripto-attività che l'ente notificante intende effettuare, anche attraverso eventuali applicazioni di finanza decentrata con le quali l'ente notificante intende interagire per proprio conto.

2. L'ente notificante, qualora intenda prestare il servizio di ricezione e trasmissione di ordini di cripto-attività per conto di clienti, fornisce all'autorità competente una copia delle procedure e una descrizione dei dispositivi che garantiscono la conformità all'articolo 80 del regolamento (UE) 2023/1114.

3. L'ente notificante, qualora intenda prestare il servizio di collocamento di cripto-attività, fornisce all'autorità competente una copia delle procedure per individuare, prevenire, gestire e segnalare i conflitti di interesse e una descrizione dei dispositivi attuati per conformarsi all'articolo 79 del regolamento (UE) 2023/1114 e al regolamento delegato (UE) della Commissione che stabilisce norme tecniche adottate a norma dell'articolo 72, paragrafo 5, del regolamento (UE) 2023/1114.

Articolo 2

Piano di continuità operativa

1. Ai fini dell'articolo 60, paragrafo 7, lettera b), punto iii), del regolamento (UE) 2023/1114, l'ente notificante presenta all'autorità competente una descrizione dettagliata del piano di continuità operativa, comprese le misure da adottare per garantire la continuità e la regolarità della prestazione dei suoi servizi per le cripto-attività.

2. La descrizione di cui al paragrafo 1 include gli elementi seguenti:

a) informazioni dettagliate che dimostrino che il piano di continuità operativa istituito è adeguato e che sono stati predisposti dispositivi per mantenere e testare periodicamente tale piano;

b) per quanto riguarda le funzioni essenziali o importanti supportate da prestatori di servizi terzi, informazioni dettagliate sul modo in cui è garantita la continuità operativa nel caso in cui la qualità della prestazione di tali funzioni peggiori a un livello inaccettabile o venga meno;

c) informazioni sul modo in cui è garantita la continuità operativa in caso di decesso di una persona chiave e, se del caso, sui rischi politici nella giurisdizione del prestatore di servizi.

Articolo 3

Individuazione e prevenzione del riciclaggio di denaro e del finanziamento del terrorismo

Ai fini dell'articolo 60, paragrafo 7, lettera b), punti i) e ii), del regolamento (UE) 2023/1114, l'ente notificante fornisce all'autorità competente informazioni sui suoi meccanismi di controllo interno, politiche e procedure volti ad assicurare il rispetto delle disposizioni della legislazione nazionale di recepimento della direttiva (UE) 2015/849 e sul quadro di valutazione del rischio per la gestione dei rischi connessi al riciclaggio di denaro e al finanziamento del terrorismo, compresi gli elementi seguenti:

a) la valutazione, da parte dell'ente notificante, dei rischi intrinseci e residui di riciclaggio di denaro e finanziamento del terrorismo associati alla sua prestazione di servizi per le cripto-attività, compresi i rischi relativi a quanto segue:

   i) la clientela dell'ente notificante;

   ii) i servizi prestati;

   iii) i canali di distribuzione utilizzati;

   iv) le aree geografiche di attività;

b) le misure che l'ente notificante ha adottato o adotterà per prevenire i rischi individuati e rispettare gli obblighi applicabili in materia di lotta al riciclaggio e al finanziamento del terrorismo, compresi il processo di valutazione del rischio dell'ente notificante, le politiche e procedure per conformarsi agli obblighi di adeguata verifica della clientela e le politiche e procedure per individuare e segnalare operazioni o attività sospette;

c) informazioni dettagliate sulla misura in cui i meccanismi di controllo interno, le politiche e le procedure sono adeguati e proporzionati alla portata, alla natura e al rischio intrinseco di riciclaggio di denaro e finanziamento del terrorismo, compresi la gamma di servizi per le cripto-attività prestati, la complessità del modello aziendale e il modo in cui l'ente notificante garantisce la propria conformità alla direttiva (UE) 2015/849 e al regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio ([7]);

d) l'identità della persona incaricata di garantire il rispetto, da parte dell'ente notificante, degli obblighi in materia di lotta al riciclaggio e al finanziamento del terrorismo, compresa la prova delle sue competenze ed esperienza;

e) le disposizioni e le risorse umane e finanziarie destinate a garantire, sulla base di indicazioni annuali, che il personale dell'ente notificante sia adeguatamente formato in materia di lotta al riciclaggio e al finanziamento del terrorismo e su specifici rischi connessi alle cripto-attività;

([7]) Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio, del 31 maggio 2023, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849 (GU L 150 del 9.6.2023, pag. 1, ELI: http://data.europa.eu/eli/reg/2023/1113/oj).

f) una copia delle politiche, delle procedure e dei sistemi dell'ente notificante per la lotta al riciclaggio e al finanziamento del terrorismo;

g) un documento di sintesi che illustri le modifiche apportate per effetto dei servizi per le cripto-attività previsti alle procedure e ai sistemi dell'ente notificante per la lotta al riciclaggio e al finanziamento del terrorismo;

h) la frequenza della valutazione dell'adeguatezza e dell'efficacia dei meccanismi di controllo interno, dei sistemi e delle procedure, compresa l'identità della persona o della funzione responsabile di tale valutazione.

Articolo 4

Sistemi TIC e relativi dispositivi di sicurezza

Ai fini dell'articolo 60, paragrafo 7, lettera c), del regolamento (UE) 2023/1114, l'ente notificante fornisce all'autorità competente le informazioni seguenti:

a) la documentazione tecnica dei sistemi TIC, dell'infrastruttura DLT utilizzata, se del caso, e dei dispositivi di sicurezza, compresa una descrizione dei dispositivi e delle risorse umane e TIC impiegate, elaborata per conformarsi al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([8]), compreso quanto segue:

   i) una descrizione del modo in cui l'ente notificante garantisce un quadro solido, completo e ben documentato per la gestione dei rischi relativi alle TIC nell'ambito del suo sistema generale di gestione del rischio, compresa una descrizione dettagliata dei sistemi, dei protocolli e degli strumenti TIC e del modo in cui le procedure, le politiche e i sistemi dell'ente notificante tuteleranno la sicurezza, l'integrità, la disponibilità, l'autenticità e la riservatezza dei dati conformemente ai regolamenti (UE) 2022/2554 e (UE) 2016/679;

   ii) l'identificazione dei servizi TIC a supporto di funzioni essenziali o importanti, sviluppati o mantenuti dall'ente notificante, nonché di quelli prestati da prestatori di servizi terzi, e una descrizione di tali accordi contrattuali e del modo in cui detti accordi sono conformi all'articolo 73 del regolamento (UE) 2023/1114 e al capo V del regolamento (UE) 2022/2554;

   iii) una descrizione delle procedure, delle politiche, dei dispositivi e dei sistemi dell'ente notificante per la gestione della sicurezza e degli incidenti;

b) se disponibile, la descrizione di un audit sulla cibersicurezza condotto da un revisore della cibersicurezza terzo con sufficiente esperienza conformemente al regolamento delegato (UE) della Commissione che stabilisce norme tecniche a norma dell'articolo 26, paragrafo 11, quarto comma, del regolamento (UE) 2022/2554, che comprenda idealmente gli audit o i test seguenti condotti da parti esterne indipendenti:

   i) dispositivi lungo tutto il ciclo di vita relativi alla cibersicurezza organizzativa, alla sicurezza fisica e allo sviluppo sicuro del software;

   ii) valutazioni delle vulnerabilità e valutazioni della sicurezza della rete;

   iii) revisioni della configurazione delle risorse TIC a supporto di funzioni essenziali e importanti quali definite all'articolo 3, punto 22), del regolamento (UE) 2022/2554;

   iv) test di penetrazione sulle risorse TIC a supporto di funzioni essenziali e importanti quali definiti all'articolo 3, punto 17), del regolamento (UE) 2022/2554, conformemente a tutti i metodi di prova di audit elencati di seguito:

      1) scatola nera: il revisore non dispone di altre informazioni oltre agli indirizzi IP e agli URL associati al bersaglio sottoposto ad audit. Questa fase è generalmente preceduta dalla scoperta di informazioni e dall'identificazione del bersaglio mediante l'interrogazione dei servizi del sistema dei nomi di dominio (DNS), la scansione delle porte aperte, la scoperta della presenza di apparecchiature di filtraggio;

([8]) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

2) scatola grigia: i revisori dispongono delle conoscenze di un utente standard del sistema informatico (autenticazione legittima, postazione di lavoro «standard»). Gli identificatori possono appartenere a profili utente diversi per testare livelli di privilegio diversi;

3) scatola bianca: i revisori dispongono di quante più informazioni tecniche possibile (architettura, codice sorgente, contatti telefonici, identificatori ecc.) prima di avviare l'analisi, nonché dell'accesso ai contatti tecnici relativi al bersaglio;

v) se l'ente notificante utilizza e/o sviluppa contratti intelligenti, un riesame dei relativi codici sorgente per la cibersicurezza;

c) una descrizione degli audit effettuati sui sistemi TIC, se del caso, compresi l'infrastruttura DLT e i dispositivi di sicurezza utilizzati;

d) una descrizione delle informazioni pertinenti di cui alle lettere a) e b) in linguaggio non tecnico.

Articolo 5

Separazione e custodia delle cripto-attività e dei fondi dei clienti

1. Ai fini dell'articolo 60, paragrafo 7, lettera d), del regolamento (UE) 2023/1114, l'ente notificante che intende detenere cripto-attività appartenenti a clienti o i mezzi di accesso a tali cripto-attività ovvero fondi dei clienti diversi dai token di moneta elettronica fornisce all'autorità competente una descrizione dettagliata delle proprie procedure per la separazione delle cripto-attività e dei fondi dei clienti, compresi gli elementi seguenti:

a) in che modo l'ente notificante garantisce che:

i) i fondi dei clienti non siano utilizzati per conto proprio;

ii) le cripto-attività appartenenti ai clienti non siano utilizzate per conto proprio;

iii) i portafogli che detengono cripto-attività dei clienti siano diversi dai portafogli propri dell'ente notificante;

b) una descrizione dettagliata del sistema di approvazione delle chiavi crittografiche e della custodia delle chiavi crittografiche, compresi i portafogli a firma multipla;

c) il modo in cui l'ente notificante separa le cripto-attività dei clienti, anche dalle cripto-attività di altri clienti, laddove i portafogli contenenti cripto-attività di più di un cliente siano tenuti in conti omnibus;

d) una descrizione della procedura atta a garantire che i fondi dei clienti diversi dai token di moneta elettronica siano depositati presso una banca centrale o un ente creditizio entro la fine del giorno lavorativo successivo al giorno in cui tali fondi sono stati ricevuti e siano detenuti in un conto distinto da quelli utilizzati per detenere fondi appartenenti all'ente notificante;

e) qualora non intenda depositare fondi presso la banca centrale pertinente, quali fattori l'ente notificante prende in considerazione per selezionare gli enti creditizi presso i quali depositare i fondi dei clienti, comprese la politica di diversificazione dell'ente notificante, se disponibile, e la frequenza di riesame della selezione degli enti creditizi presso i quali depositare i fondi dei clienti;

f) in che modo l'ente notificante garantisce che i clienti siano informati in un linguaggio chiaro, conciso e non tecnico in merito agli aspetti fondamentali dei sistemi, delle politiche e delle procedure dell'ente notificante per conformarsi all'articolo 70, paragrafi 1, 2 e 3, del regolamento (UE) 2023/1114.

2. Conformemente all'articolo 70, paragrafo 5, del regolamento (UE) 2023/1114, i prestatori di servizi per le cripto-attività che sono istituti di moneta elettronica o enti creditizi forniscono solo le informazioni di cui al paragrafo 1 del presente articolo.

Articolo 6

Politica di custodia e amministrazione

Ai fini dell'articolo 60, paragrafo 7, lettera e), del regolamento (UE) 2023/1114, l'ente notificante fornisce all'autorità competente le informazioni seguenti:

a) una descrizione degli accordi legati al tipo di custodia offerto ai clienti, una copia dell'accordo standard dell'ente notificante per la custodia e l'amministrazione di cripto-attività per conto dei clienti a norma dell'articolo 75, paragrafo 1, del regolamento (UE) 2023/1114 e una copia della sintesi della politica di custodia messa a disposizione dei clienti conformemente all'articolo 75, paragrafo 3, del medesimo regolamento;

b) la politica di custodia e amministrazione dell'ente notificante, compresa una descrizione delle fonti individuate di rischi operativi e relativi alle TIC per la custodia e il controllo delle cripto-attività o dei mezzi di accesso alle cripto-attività dei clienti, unitamente a quanto segue:

   i) le politiche e procedure e una descrizione dei dispositivi per conformarsi all'articolo 75, paragrafo 8, del regolamento (UE) 2023/1114;

   ii) le politiche e procedure e una descrizione dei sistemi e dei controlli per la gestione dei rischi operativi e relativi alle TIC, anche nel caso in cui la custodia e l'amministrazione di cripto-attività per conto dei clienti siano esternalizzate a terzi;

   iii) le politiche e procedure relative ai sistemi per garantire l'esercizio dei diritti connessi alle cripto-attività da parte dei clienti, e una descrizione di tali sistemi;

   iv) le politiche e procedure relative ai sistemi che garantiscono la restituzione ai clienti delle cripto-attività o dei mezzi di accesso, e una descrizione di tali sistemi;

c) informazioni sulle modalità di identificazione delle cripto-attività e dei mezzi di accesso alle cripto-attività dei clienti;

d) informazioni sui dispositivi per ridurre al minimo il rischio di perdita di cripto-attività o di mezzi di accesso alle cripto-attività;

e) se il prestatore di servizi per le cripto-attività ha delegato a terzi la prestazione di servizi di custodia e amministrazione di cripto-attività per conto di clienti:

   i) informazioni sull'identità dei terzi che prestano il servizio di custodia e amministrazione di cripto-attività e sul loro status conformemente all'articolo 59 o all'articolo 60 del regolamento (UE) 2023/1114;

   ii) una descrizione di eventuali funzioni relative alla custodia e all'amministrazione delle cripto-attività delegate dal prestatore di servizi per le cripto-attività, l'elenco degli eventuali delegati e sottodelegati, a seconda dei casi, e gli eventuali conflitti di interesse che potrebbero derivare da tale delega;

   iii) una descrizione del modo in cui l'ente notificante intende vigilare sulle deleghe o sottodeleghe.

Articolo 7

Norme operative della piattaforma di negoziazione e individuazione degli abusi di mercato

1. Ai fini dell'articolo 60, paragrafo 7, lettera f), del regolamento (UE) 2023/1114, l'ente notificante che intende gestire una piattaforma di negoziazione di cripto-attività fornisce all'autorità competente le informazioni seguenti:

a) le regole relative all'ammissione delle cripto-attività alla negoziazione;

b) la procedura di approvazione per l'ammissione delle cripto-attività alla negoziazione, compresa l'adeguata verifica della clientela effettuata conformemente alla direttiva (UE) 2015/849;

c) l'elenco delle categorie di cripto-attività che non saranno ammesse alla negoziazione e i motivi di tale esclusione;

d) le politiche, le procedure e le commissioni per l'ammissione alla negoziazione, unitamente a una descrizione, se del caso, dell'adesione, degli sconti e delle relative condizioni;

e) le norme che disciplinano l'esecuzione degli ordini, comprese eventuali procedure di cancellazione degli ordini eseguiti e per la comunicazione di tali informazioni ai partecipanti al mercato;

f) i metodi messi in atto per valutare l'adeguatezza delle cripto-attività conformemente all'articolo 76, paragrafo 2, del regolamento (UE) 2023/1114;

g) i sistemi, le procedure e i dispositivi attuati per conformarsi all'articolo 76, paragrafo 7, del regolamento (UE) 2023/1114;

h) le modalità con cui rendere pubblici tutti i prezzi di domanda e offerta, lo spessore degli interessi di negoziazione ai prezzi pubblicizzati per le cripto-attività attraverso le sue piattaforme di negoziazione e il prezzo, il volume e l'ora delle operazioni eseguite in relazione alle cripto-attività negoziate sulla sua piattaforma di negoziazione, conformemente all'articolo 76, paragrafi 9 e 10, del regolamento (UE) 2023/1114;

i) le strutture tariffarie e una giustificazione del modo in cui tali strutture sono conformi all'articolo 76, paragrafo 13, del regolamento (UE) 2023/1114;

j) i sistemi, le procedure e i dispositivi attuati per tenere a disposizione dell'autorità competente i dati relativi a tutti gli ordini o il meccanismo per garantire che l'autorità competente abbia accesso al book di negoziazione e a qualsiasi altro sistema di negoziazione;

k) per quanto riguarda il regolamento delle operazioni:

   i) se il regolamento definitivo delle operazioni è avviato nel registro distribuito o al di fuori di esso;

   ii) l'intervallo di tempo durante il quale è avviato il regolamento definitivo delle operazioni in cripto-attività;

   iii) il modo per verificare la disponibilità di fondi e cripto-attività;

   iv) il modo per confermare i dettagli pertinenti delle operazioni;

   v) le misure previste per limitare i mancati regolamenti;

   vi) il momento in cui il regolamento è definitivo e il momento di avvio del regolamento definitivo dopo l'esecuzione dell'operazione;

l) le procedure e i sistemi messi in atto per individuare e prevenire gli abusi di mercato, comprese le informazioni sulle comunicazioni all'autorità competente di eventuali casi di abuso di mercato.

2. Gli enti notificanti che intendono gestire una piattaforma di negoziazione di cripto-attività forniscono all'autorità competente una copia delle norme operative della piattaforma di negoziazione ed eventuali procedure per individuare e prevenire gli abusi di mercato.

Articolo 8

Scambio di cripto-attività con fondi o scambio di cripto-attività con altre cripto-attività

Ai fini dell'articolo 60, paragrafo 7, lettera g), del regolamento (UE) 2023/1114, l'ente notificante che intende scambiare cripto-attività con fondi o altre cripto-attività fornisce all'autorità competente le informazioni seguenti:

a) una descrizione della politica commerciale stabilita conformemente all'articolo 77, paragrafo 1, del regolamento (UE) 2023/1114;

b) il metodo per determinare il prezzo delle cripto-attività che l'ente notificante propone di scambiare con fondi o altre cripto-attività conformemente all'articolo 77, paragrafo 2, del regolamento (UE) 2023/1114, compreso il modo in cui il volume e la volatilità di mercato delle cripto-attività incidono sul meccanismo di determinazione del prezzo.

Articolo 9

Politica di esecuzione

Ai fini dell'articolo 60, paragrafo 7, lettera h), del regolamento (UE) 2023/1114, l'ente notificante che intende eseguire ordini di cripto-attività per conto di clienti fornisce all'autorità competente la sua politica di esecuzione, comprese le informazioni seguenti:

a) i dispositivi che garantiscono che il cliente abbia dato il proprio consenso alla politica di esecuzione prima dell'esecuzione dell'ordine;

b) un elenco delle piattaforme di negoziazione di cripto-attività che l'ente notificante utilizzerà per l'esecuzione degli ordini e i criteri per la valutazione delle sedi di esecuzione incluse nella politica di esecuzione conformemente all'articolo 78, paragrafo 6, del regolamento (UE) 2023/1114;

c) quali piattaforme di negoziazione l'ente notificante intende utilizzare per ciascun tipo di cripto-attività e la conferma che l'ente notificante non riceverà alcuna forma di remunerazione, sconto o beneficio non monetario per il fatto di canalizzare gli ordini ricevuti verso una particolare piattaforma di negoziazione di cripto-attività;

d) il modo in cui l'esecuzione tiene conto del prezzo, dei costi, della velocità, della probabilità di esecuzione e regolamento, delle dimensioni, della natura, delle condizioni di custodia delle cripto-attività o di qualsiasi altro fattore pertinente considerato parte di tutte le misure necessarie per ottenere il miglior risultato possibile per il cliente;

e) se del caso, le modalità per informare i clienti che l'ente notificante eseguirà ordini al di fuori di una piattaforma di negoziazione e il modo in cui l'ente notificante otterrà il consenso esplicito preventivo dei suoi clienti prima di eseguire tali ordini;

f) il modo in cui il cliente è avvertito che eventuali istruzioni specifiche di un cliente possono impedire all'ente notificante di adottare le misure necessarie, in linea con le modalità stabilite e attuate da quest'ultimo nella sua politica di esecuzione, per ottenere il miglior risultato possibile per l'esecuzione di tali ordini in relazione agli elementi contemplati da tali istruzioni;

g) il processo di selezione delle sedi di negoziazione, le strategie di esecuzione impiegate, le modalità adottate per analizzare la qualità dell'esecuzione ottenuta e il modo in cui l'ente notificante monitora e verifica che siano stati ottenuti i migliori risultati possibili per i clienti;

h) i dispositivi volti a prevenire l'uso improprio di qualsiasi informazione relativa agli ordini dei clienti da parte dei dipendenti dell'ente notificante;

i) i dispositivi e le procedure relativi alle modalità con cui l'ente notificante comunicherà ai clienti informazioni sulla sua strategia di esecuzione degli ordini e notificherà loro eventuali modifiche sostanziali di tale strategia;

j) le modalità per dimostrare all'autorità competente, su richiesta di quest'ultima, la conformità all'articolo 78 del regolamento (UE) 2023/1114.

Articolo 10

Prestazione di consulenza sulle cripto-attività o di servizi di gestione del portafoglio di cripto-attività

Ai fini dell'articolo 60, paragrafo 7, lettera i), del regolamento (UE) 2023/1114, l'ente notificante che intende prestare consulenza sulle cripto-attività o servizi di gestione del portafoglio di cripto-attività fornisce all'autorità competente le informazioni seguenti:

a) una descrizione dettagliata delle modalità messe in atto dall'ente notificante per conformarsi all'articolo 81, paragrafo 7, del regolamento (UE) 2023/1114, compreso quanto segue:

   i) i meccanismi per controllare, valutare e mantenere efficacemente le conoscenze e le competenze delle persone fisiche che prestano consulenza sulle cripto-attività o gestiscono portafogli di cripto-attività;

   ii) le disposizioni volte a garantire che le persone fisiche coinvolte nella prestazione di consulenza o nella gestione del portafoglio conoscano, comprendano e applichino le politiche e procedure interne dell'ente notificante stabilite per conformarsi al regolamento (UE) 2023/1114, in particolare all'articolo 81, paragrafo 1, di tale regolamento, e alla direttiva (UE) 2015/849;

iii) l'entità delle risorse umane e finanziarie che l'ente notificante intende destinare annualmente allo sviluppo professionale e alla formazione del personale che presta consulenza sulle cripto-attività o gestisce portafogli di cripto-attività;

b) i meccanismi per controllare, valutare e mantenere le conoscenze e le competenze delle persone fisiche che prestano consulenza per conto dell'ente notificante, necessarie, secondo i criteri di tale valutazione utilizzati nella legislazione nazionale, per valutare l'adeguatezza di cui all'articolo 81, paragrafo 1, del regolamento (UE) 2023/1114.

Articolo 11

Servizi di trasferimento

Ai fini dell'articolo 60, paragrafo 7, lettera k), del regolamento (UE) 2023/1114, l'ente notificante che intende prestare servizi di trasferimento di cripto-attività per conto di clienti fornisce all'autorità competente le informazioni seguenti:

a) informazioni dettagliate sui tipi di cripto-attività per i quali l'ente notificante intende prestare servizi di trasferimento;

b) una descrizione dettagliata delle modalità messe in atto dall'ente notificante per conformarsi all'articolo 82 del regolamento (UE) 2023/1114, comprese informazioni dettagliate sui dispositivi dell'ente notificante e sulle risorse umane e TIC impiegate per affrontare i rischi in modo tempestivo, efficiente e completo durante la prestazione di servizi di trasferimento di cripto-attività per conto di clienti, tenendo conto delle potenziali carenze operative e dei rischi di cibersicurezza;

c) se disponibile, una descrizione della polizza assicurativa dell'ente notificante, compresa la copertura assicurativa del pregiudizio alle cripto-attività del cliente che può derivare dai rischi di cibersicurezza;

d) disposizioni volte a garantire che i clienti siano adeguatamente informati in merito alle modalità di cui alla lettera b).

Articolo 12

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 31 ottobre 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN