

Orientamenti

sulle prassi di vigilanza delle autorità competenti ai fini della prevenzione e dell'individuazione degli abusi di mercato ai sensi del regolamento relativo ai mercati delle cripto-attività (MiCA)

Indice

1	Ambito di applicazione	2
2	Riferimenti normativi, abbreviazioni e definizioni	3
2.1	Riferimenti normativi	3
2.2	Abbreviazioni	3
2.3	Definizioni	3
3	Finalità.....	5
Conformità e obblighi di notifica		6
3.1	Status degli orientamenti	6
3.2	Obblighi di notifica.....	6
4	Orientamenti sulle prassi di vigilanza per le autorità competenti ai fini della prevenzione e dell'individuazione degli abusi di mercato.....	7
4.1	Proporzionalità nell'applicazione degli orientamenti (orientamento 1).....	7
4.2	Approccio generale alla prevenzione e all'individuazione di abusi di mercato ai sensi del MiCA (orientamento 2)	7
4.3	Integrazione delle prassi di vigilanza esistenti (orientamento 3).....	8
4.4	Cultura comune della vigilanza per garantire l'integrità del mercato ai sensi del MiCA (orientamento 4).....	9
4.5	Adeguatezza delle risorse (orientamento 5)	9
4.6	Dialogo aperto con le parti interessate in merito ai rischi per l'integrità del mercato (orientamento 6)	10
4.7	Iniziative volte a promuovere l'integrità del mercato tra i partecipanti al mercato (orientamento 7)	10
4.8	Monitoraggio e sorveglianza da parte delle autorità nazionali competenti (orientamento 8)	11
4.9	Vigilanza sui dispositivi, sui sistemi e sulle procedure delle PPAET per la prevenzione e l'individuazione degli abusi di mercato (orientamento 9)	12
4.10	Reazione a una segnalazione di ordini o operazioni sospetti (orientamento 10). 12	
4.11	Coordinamento dell'ESMA (orientamento 11)	13
4.12	Ostacoli dei paesi terzi all'esercizio efficace delle funzioni di vigilanza delle ANC per l'individuazione degli abusi di mercato transfrontalieri (orientamento 12)	13

1 Ambito di applicazione

1 Destinatari

I presenti orientamenti si applicano alle autorità competenti di cui all'articolo 3, paragrafo 1, punto 35), del MiCA.

2 Oggetto

I presenti orientamenti si applicano in relazione all'articolo 92, paragrafo 3, del MiCA.

3 Tempistica

I presenti orientamenti si applicano a partire da tre mesi dopo la data della loro pubblicazione sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE.

2 Riferimenti normativi, abbreviazioni e definizioni

2.1 Riferimenti normativi

MiCA	Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle crypto-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⁾
Norme tecniche di regolamentazione in materia di segnalazioni di ordini o operazioni sospetti	Regolamento delegato (UE) xxxx/xxx della Commissione, del [data], che specifica taluni requisiti in relazione all'individuazione e alla prevenzione degli abusi di mercato ai sensi del regolamento relativo ai mercati delle crypto-attività (MiCA)
Regolamento ESMA	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 ⁽²⁾

2.2 Abbreviazioni

CASP	Prestatore di servizi per le crypto-attività
CE	Commissione europea
ESMA	Autorità europea degli strumenti finanziari e dei mercati
MEV	Valore massimo estraibile
PPAET	Persone che predispongono o eseguono operazioni a titolo professionale
UE	Unione europea

2.3 Definizioni

Piattaforme basate sul web	Piattaforme online che raccolgono e diffondono dati e informazioni relativi alle crypto-attività, accessibili a titolo gratuito e su base non discriminatoria, per promuovere decisioni di investimento informate, secondo la definizione di cui all'articolo 1 del regolamento di esecuzione (UE) 2024/2861 della Commissione ⁽³⁾
----------------------------	---

⁽¹⁾ GU L 150 del 9.6.2023, pag. 40.

⁽²⁾ GU L 331 del 15.12.2010, pag. 84.

⁽³⁾ Regolamento di esecuzione (UE) 2024/2861 della Commissione, del 12 novembre 2024, che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio per quanto riguarda gli strumenti tecnici per l'adeguata comunicazione al pubblico delle informazioni privilegiate e la comunicazione al pubblico tardiva di tali informazioni (GU L 2024/2861 del 13.11.2024).

Social media

Servizio di social network online, secondo la definizione di cui all'articolo 2, punto 7), del regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio ⁽⁴⁾

⁽⁴⁾ Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) (GU L 265 del 12.10.2022, pag. 1).

3 Finalità

I presenti orientamenti si basano sull'articolo 92, paragrafo 3, del MiCA e sull'articolo 16 del regolamento ESMA. Hanno l'obiettivo di assicurare la coerenza tra le prassi di vigilanza delle autorità competenti ai fini della prevenzione e dell'individuazione degli abusi di mercato riguardanti crypto-attività.

Più specificamente, mirano a stabilire prassi di vigilanza uniformi, efficienti ed efficaci tra le autorità competenti ai fini della prevenzione e dell'individuazione dell'abuso di informazioni privilegiate, della divulgazione illecita di informazioni privilegiate e della manipolazione del mercato, nonché a garantire l'applicazione uniforme e coerente del titolo VI del MiCA (articoli da 86 a 92).

Conformità e obblighi di notifica

3.1 Status degli orientamenti

Ai sensi dell'articolo 16, paragrafo 3, del regolamento ESMA, le autorità competenti devono compiere ogni sforzo per conformarsi ai presenti orientamenti.

Le autorità competenti alle quali si applicano i presenti orientamenti dovrebbero conformarvisi integrandoli nei propri quadri giuridici e/o di vigilanza nazionali, secondo il caso.

3.2 Obblighi di notifica

Entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE, le autorità competenti alle quali si applicano i presenti orientamenti devono notificare all'ESMA se i) sono conformi, ii) non sono conformi, ma intendono conformarsi o iii) non sono conformi e non intendono conformarsi agli orientamenti.

In caso di non conformità, le autorità competenti devono inoltre notificare all'ESMA, entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE, i motivi per cui non si conformano a tali orientamenti.

Un modello di notifica è disponibile sul sito web dell'ESMA. Una volta compilato, il modello va trasmesso all'ESMA.

4 Orientamenti sulle prassi di vigilanza per le autorità competenti ai fini della prevenzione e dell'individuazione degli abusi di mercato

4.1 Proporzionalità nell'applicazione degli orientamenti (orientamento 1)

1. Le autorità competenti dovrebbero applicare i presenti orientamenti in modo proporzionato alla rilevanza delle attività e dei servizi svolti dalle persone soggette a vigilanza nel mercato delle cripto-attività e al rischio che tali attività e servizi comportano per l'integrità del mercato. Le autorità competenti sono pertanto incoraggiate a sviluppare e mantenere una comprensione adeguata dei rischi posti dai CASP e dagli emittenti soggetti a vigilanza diretta, nonché dei rischi posti da altre persone (operatori, miner, validatori o soggetti pertinenti attivi sui social media), le cui azioni possono costituire abusi di mercato [ad esempio manipolazione del book di negoziazione, strategie MEV (5) o diffusione di informazioni false o fuorvianti].
2. Considerando la rapida evoluzione dei mercati delle cripto-attività, le autorità competenti dovrebbero essere particolarmente attente e vigili rispetto a eventuali nuove forme di comportamenti di abuso di mercato, adottando un approccio basato sul rischio per quanto riguarda le attività indicate nei presenti orientamenti.
3. Nell'applicare i presenti orientamenti, le autorità competenti dovrebbero inoltre adeguare il loro approccio alla vigilanza del mercato tenendo conto dei progressi compiuti in relazione, ad esempio, alla disponibilità di dati e allo sviluppo di nuovi strumenti di vigilanza del mercato.

4.2 Approccio generale alla prevenzione e all'individuazione di abusi di mercato ai sensi del MiCA (orientamento 2)

4. L'approccio delle autorità competenti alla vigilanza in relazione agli abusi di mercato nel settore delle cripto-attività dovrebbe essere basato sul rischio. Ciò significa che le autorità competenti dovrebbero dare priorità alle loro risorse e utilizzarle in modo efficiente e proporzionato rispetto al livello di rischio individuato.
5. Nel considerare i rischi, le autorità competenti dovrebbero essere lungimiranti, tenendo conto per quanto possibile dei rischi potenziali ed emergenti di abusi di mercato.
6. Le autorità competenti sono incoraggiate a monitorare il mercato delle cripto-attività in modo da poter rispondere ai rischi individuati per l'integrità del mercato senza indebito ritardo. In particolare, le autorità competenti, quando rilevano una minaccia per

⁽⁵⁾ Valore massimo che un miner o un validatore di una blockchain può ottenere modificando l'ordine delle operazioni durante la creazione di un blocco.

l'integrità del mercato, dovrebbero darvi seguito in tempi ragionevoli. I problemi individuati non dovrebbero rimanere privi di una conclusione o un piano d'azione adeguati.

7. Laddove siano rilevati nuovi rischi per l'integrità del mercato nel settore delle cripto-attività, le autorità competenti dovrebbero integrare, cercare di ampliare o adeguare la loro strategia di vigilanza per le cripto-attività e agire come appropriato.
8. Le autorità competenti sono incoraggiate a integrare nella loro strategia di vigilanza gli obiettivi e le priorità relativi alla prevenzione e all'individuazione degli abusi di mercato ai sensi del MiCA.

4.3 Integrazione delle prassi di vigilanza esistenti (orientamento 3)

9. Le autorità competenti sono incoraggiate a integrare nelle loro prassi di vigilanza esistenti misure specifiche per la prevenzione e l'individuazione degli abusi di mercato nei mercati delle cripto-attività. Prima di integrare nuove misure, le autorità competenti sono incoraggiate a valutare in che misura le prassi già in atto per l'individuazione e la prevenzione degli abusi di mercato relativi agli strumenti finanziari possano coprire le forme specifiche di abusi di mercato relative alle cripto-attività e ad adattarle o estenderle, come appropriato.
10. Ad esempio, le autorità competenti potrebbero includere nella loro attività di monitoraggio le prassi manipolative che possono derivare dalla tecnologia specifica alla base delle cripto-attività (ad esempio strategie MEV abusive) o dal modo in cui queste sono offerte o valutate (ad esempio la manipolazione dell'offerta di token o, per le stablecoin, la valutazione delle attività di copertura).
11. Inoltre, le autorità competenti dovrebbero prendere in considerazione la possibilità di monitorare i social media, con la massima diligenza possibile, per quanto riguarda le informazioni pubblicate sulle cripto-attività, dato il rischio più elevato di diffusione di informazioni false o fuorvianti che tali mezzi di comunicazione possono presentare nel contesto delle cripto-attività rispetto ai mercati finanziari tradizionali.
12. Analogamente, per quanto concerne l'abuso di informazioni privilegiate, le autorità competenti dovrebbero prendere in considerazione, oltre al possesso di informazioni privilegiate da parte di una persona che ha accesso a tali informazioni nell'esercizio di un'attività lavorativa, di una professione o di una funzione (ad esempio un dipendente di un CASP a conoscenza della decisione di inserire un nuovo token in una piattaforma di negoziazione), il possesso di informazioni privilegiate da parte di una persona in relazione al suo ruolo nella tecnologia a registro distribuito o in una tecnologia analoga (ad esempio miner o validatori che ricorrono alla pratica del front running o influenzano il flusso delle operazioni convalidate).

4.4 Cultura comune della vigilanza per garantire l'integrità del mercato ai sensi del MiCA (orientamento 4)

13. Le autorità competenti dovrebbero svolgere un ruolo attivo nella creazione di una cultura comune della vigilanza nell'UE e di prassi di vigilanza uniformi ai sensi del MiCA.
14. Per conseguire tale obiettivo, le autorità competenti dovrebbero condividere tra loro informazioni per facilitare una comprensione comune dei rischi per l'integrità del mercato posti dalle crypto-attività, dagli emittenti, dai CASP e da qualsiasi altro partecipante al mercato.
15. Le autorità competenti dovrebbero informarsi reciprocamente in merito alle misure adottate per la prevenzione e l'individuazione degli abusi di mercato ai sensi dei presenti orientamenti e confrontarsi sulle migliori prassi individuate per assicurare l'integrità del mercato.
16. Inoltre, le autorità competenti sono incoraggiate a condividere le loro esperienze dirette di vigilanza nell'ambito degli abusi di mercato relativi alle crypto-attività e a evidenziare le difficoltà incontrate, presentando e discutendo casi di vigilanza nei gruppi pertinenti dell'ESMA.
17. A seguito di tali scambi, le autorità competenti possono anche proporre all'ESMA di adottare specifici strumenti di convergenza in materia di vigilanza al fine di promuovere la convergenza della vigilanza in tutta l'UE.
18. Per avere una visione più completa dei partecipanti e dei prodotti dei mercati delle crypto-attività, nel rispetto delle norme sul segreto professionale, le autorità competenti possono, su base volontaria, prendere in considerazione la possibilità di avviare dialoghi e scambi di esperienze con altre autorità (ad esempio le autorità responsabili della protezione dei consumatori o della prevenzione e le autorità antiriciclaggio), qualora la loro attività di vigilanza appaia collegata ai mercati delle crypto-attività.

4.5 Adeguatezza delle risorse (orientamento 5)

19. Al fine di assicurare la disponibilità di risorse sufficienti per conseguire i loro obiettivi di vigilanza, le autorità competenti sono incoraggiate a disporre di personale specificamente preposto allo svolgimento delle loro funzioni e dei loro compiti in materia di sorveglianza dei mercati delle crypto-attività.
20. Per individuare le risorse e il personale necessari per l'individuazione e la prevenzione degli abusi di mercato nei mercati delle crypto-attività, le autorità competenti sono incoraggiate a considerare i seguenti elementi:
 - a) le conoscenze e le competenze del loro personale per quanto riguarda il funzionamento delle crypto-attività e le pertinenti tecnologie utilizzate (ad esempio, i meccanismi di consenso), nonché i ruoli dei partecipanti alle operazioni on-chain;

b) la necessità di strumenti adeguati specifici per la sorveglianza dei mercati delle cripto-attività;

c) la necessità di effettuare una sorveglianza del mercato basata sui dati, oltre a quella basata sugli eventi.

21. Le autorità competenti sono incoraggiate a partecipare a iniziative per la formazione continua del personale pertinente.

4.6 Dialogo aperto con le parti interessate in merito ai rischi per l'integrità del mercato (orientamento 6)

22. Per comprendere meglio gli sviluppi tecnologici e i potenziali rischi emergenti per l'integrità del mercato per quanto riguarda le cripto-attività, le autorità competenti dovrebbero dialogare in modo proattivo con le parti interessate connesse o associate ai mercati delle cripto-attività, nonché con esperti, accademici, gruppi pubblici di sensibilizzazione pertinenti, imprese informatiche e fornitori di servizi di dati nonché persone alle quali le PPAET hanno esternalizzato l'esecuzione di compiti relativi alla prevenzione, al monitoraggio e all'individuazione di potenziali abusi di mercato.

23. Le autorità competenti dovrebbero prendere in considerazione i risultati di tali scambi nell'individuazione dei rischi emergenti e delle nuove strategie di abuso di mercato nonché nell'elaborazione di possibili soluzioni, compresi nuovi strumenti volti ad attenuare i rischi per l'integrità del mercato con riferimento alle cripto-attività.

4.7 Iniziative volte a promuovere l'integrità del mercato tra i partecipanti al mercato (orientamento 7)

24. Per promuovere l'integrità del mercato, le autorità competenti dovrebbero prendere in considerazione l'adozione di iniziative di formazione che sensibilizzino i partecipanti al mercato in merito ai comportamenti che possono costituire abusi di mercato e alle relative sanzioni. Nel fornire le informazioni pertinenti, le autorità competenti dovrebbero utilizzare un linguaggio adeguato alla natura delle persone cui sono rivolte le iniziative.

25. Tali iniziative potrebbero ad esempio prevedere:

a) l'utilizzo del sito web delle autorità competenti e di altri canali di comunicazione (ad esempio social media, blog, newsletter e podcast, ove disponibili) per spiegare quali comportamenti possono costituire abusi di mercato e per fornire esempi pertinenti relativi alle cripto-attività;

b) formazione periodica per i partecipanti al mercato in materia di conformità e prevenzione degli abusi di mercato ai sensi del MiCA;

c) sessioni di domande e risposte a scopo informativo, relative alla prevenzione e all'individuazione degli abusi di mercato.

26. Le autorità competenti possono elaborare le iniziative di formazione descritte nel presente orientamento autonomamente o in collaborazione con altre autorità competenti e con l'ESMA, come appropriato.
27. Per promuovere ulteriormente la prevenzione degli abusi di mercato, le autorità competenti dovrebbero anche considerare l'opportunità di:
- a) incoraggiare gli emittenti, le PPAET e i CASP che non rientrano nella categoria delle PPAET ad adottare migliori prassi che vadano oltre i requisiti di legge. Ad esempio, le autorità competenti potrebbero suggerire agli emittenti di informare i dipendenti che hanno accesso a informazioni privilegiate in merito alle azioni che possono costituire abuso di informazioni privilegiate o divulgazione illecita di informazioni privilegiate e alle relative conseguenze o suggerire ai gestori di piattaforme di negoziazione di informare i loro utenti riguardo ai comportamenti che possono costituire abuso di mercato e alle relative sanzioni;
 - b) informare gli operatori delle piattaforme di negoziazione per le cripto-attività della necessità di potenziare e aggiornare la loro infrastruttura di sorveglianza per far fronte ai rischi di manipolazione del mercato recentemente individuati o emergenti; e
 - c) fornire indicazioni e riscontri mirati sulle misure di conformità che devono essere attuate dalle PPAET.
28. Le informazioni fornite nel contesto di iniziative di formazione o di altro tipo da parte delle autorità competenti ai sensi del presente orientamento non dovrebbero essere qualificate come consulenza legale né ridurre la responsabilità dei partecipanti al mercato per quanto riguarda i loro obblighi ai sensi del MiCA o di altre leggi o normative applicabili.

4.8 Monitoraggio e sorveglianza da parte delle autorità nazionali competenti (orientamento 8)

29. Per proteggere l'integrità dei mercati delle cripto-attività, le autorità nazionali competenti dovrebbero condurre attività di monitoraggio e sorveglianza del mercato basate sui dati, in collaborazione con altre autorità competenti o, sotto la loro responsabilità, mediante delega ad altre autorità o fornitori di servizi, come appropriato.
30. Le attività di monitoraggio e sorveglianza del mercato delle autorità competenti dovrebbero includere dati pubblicamente disponibili, dati normativi sugli ordini e sulle operazioni ottenuti dai CASP e, nella misura possibile, la riconciliazione di dati on-chain, off-chain e trasversali del mercato.
31. Le autorità competenti dovrebbero inoltre considerare di includere, nella loro attività di monitoraggio e sorveglianza del mercato, qualsiasi comunicazione relativa alle cripto-attività, comprese le comunicazioni su piattaforme web, social media e blog, newsletter e podcast, se utilizzate per diffondere informazioni sulle cripto-attività, adottando un

approccio basato sul rischio (tenendo conto, ad esempio, dei soggetti, del numero di utenti e dell'accessibilità).

32. Nello svolgimento della vigilanza costante sui mezzi di comunicazione, le autorità competenti possono adottare un monitoraggio automatizzato in grado di individuare schemi, parole chiave e tendenze, che dovrà essere integrato da un'analisi umana.

4.9 Vigilanza sui dispositivi, sui sistemi e sulle procedure delle PPAET per la prevenzione e l'individuazione degli abusi di mercato (orientamento 9)

33. Le autorità competenti dovrebbero assicurare che i dispositivi, i sistemi e le procedure delle PPAET per la prevenzione e l'individuazione degli abusi di mercato a norma dell'articolo 92, paragrafo 1, del MiCA e delle norme tecniche di regolamentazione in materia di segnalazioni di ordini o operazioni sospetti rimangano adeguati su base continuativa.
34. Nel quadro di un approccio alla vigilanza basato sul rischio, la frequenza e la pertinenza delle azioni di vigilanza delle autorità competenti dovrebbero essere proporzionate e adeguate alla scala, alle dimensioni e alla natura dell'attività svolta dalla PPAET, ad esempio operando una distinzione tra CASP che gestiscono una piattaforma di negoziazione e CASP che si limitano a ricevere, trasmettere o eseguire ordini per conto dei clienti.

4.10 Reazione a una segnalazione di ordini o operazioni sospetti (orientamento 10)

35. Le autorità competenti dovrebbero adottare procedure adeguate e proporzionate per analizzare le segnalazioni di ordini o operazioni sospetti ricevute dalle PPAET, al fine di assicurare un'analisi efficace e un'azione di vigilanza appropriata. Dette procedure dovrebbero:
- a) individuare chiaramente tutte le fasi che le autorità competenti dovrebbero seguire quando ricevono una segnalazione di ordini o operazioni sospetti;
 - b) per ogni fase, indicare l'unità/la funzione responsabile all'interno delle autorità competenti; e
 - c) fornire i criteri per classificare il comportamento indicato mediante le segnalazioni di ordini o operazioni sospetti in base a parametri quali la gravità e la ricorrenza.
36. Le misure adottate dalle autorità competenti ai sensi della suddetta procedura dovrebbero essere proporzionate alla minaccia individuata.

4.11 Coordinamento dell'ESMA (orientamento 11)

37. Le autorità competenti dovrebbero prendere in considerazione la possibilità di richiedere all'ESMA di coordinare le ispezioni o le indagini, conformemente all'articolo 95, paragrafo 5, del MiCA, ogniqualvolta, in un caso transfrontaliero:
- a) vi siano prove o sospetti che più di due autorità competenti siano competenti per un caso;
 - b) un'azione non coordinata possa compromettere l'esito finale di un'indagine; o
 - c) un'azione non coordinata possa comportare un onere aggiuntivo per i partecipanti al mercato.

4.12 Ostacoli dei paesi terzi all'esercizio efficace delle funzioni di vigilanza delle ANC per l'individuazione degli abusi di mercato transfrontalieri (orientamento 12)

38. Un'autorità competente dovrebbe informare le altre autorità competenti pertinenti e l'ESMA qualora, nel corso delle sue attività di vigilanza, individui:
- a) CASP il cui modello di business potrebbe ostacolare l'esercizio efficace delle funzioni di vigilanza delle autorità competenti in materia di abusi di mercato. Un esempio potrebbe essere quello di un CASP autorizzato a eseguire ordini per conto dei clienti che invia un numero significativo di operazioni a piattaforme di negoziazione al di fuori dell'UE, poiché ciò potrebbe impedire l'utilizzo delle segnalazioni di ordini o operazioni sospetti come strumento per la lotta agli abusi di mercato. Qualora tali CASP siano individuati, le autorità competenti dovrebbero adoperarsi per concordare un approccio comune alla vigilanza in questi casi;
 - b) eventuali ostacoli nelle sue interazioni con le autorità competenti di paesi terzi che potrebbero contrastare l'esercizio efficace delle loro funzioni di vigilanza in relazione agli abusi di mercato.
39. Nel valutare se vi siano potenziali ostacoli a una vigilanza efficace, le autorità competenti dovrebbero prendere in considerazione tutte le informazioni pertinenti, tra cui:
- a) le disposizioni legislative, regolamentari o amministrative pertinenti di un paese terzo;
 - b) eventuali difficoltà dovute all'applicazione di tali disposizioni legislative, regolamentari o amministrative;
 - c) la possibilità di scambiare informazioni con le autorità competenti del paese terzo ed eventuali difficoltà nell'ottenere informazioni da queste;

- d) la complessità e la trasparenza della struttura del gruppo a cui appartiene un'entità sottoposta a vigilanza ai sensi del MiCA e delle persone che hanno stretti legami con un'entità sottoposta a vigilanza ai sensi del MiCA;
- e) l'ubicazione o le attività svolte dalle entità che fanno parte del gruppo cui appartiene un'entità sottoposta a vigilanza ai sensi del MiCA o delle persone che hanno stretti legami con un'entità sottoposta a vigilanza ai sensi del MiCA.