Amtsblatt
der Europäischen Union

DE
Reihe L

2025/885

20.8.2025

DELEGIERTE VERORDNUNG (EU) 2025/885 DER KOMMISSION

vom 29. April 2025

zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Vorkehrungen, Systeme und Verfahren zur Vorbeugung, Aufdeckung und Meldung von Marktmissbrauch, der für die Meldung eines vermuteten Marktmissbrauchs zu verwendenden Muster und der Verfahren für die Abstimmung zwischen den jeweils zuständigen Behörden bei der Aufdeckung von grenzüberschreitendem Marktmissbrauch und dessen Belegung mit Sanktionen

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 ([1]), insbesondere auf Artikel 92 Absatz 2 Unterabsatz 3,

in Erwägung nachstehender Gründe:

(1) Für die Vorkehrungen, Verfahren und Systeme, über die Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, für die Meldung von Aufträgen, Geschäften und anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie (DLT), einschließlich des Konsensmechanismus, verfügen müssen, wenn Umstände vorliegen könnten, die darauf hindeuten, dass Marktmissbrauch begangen wurde, begangen wird oder wahrscheinlich begangen wird, sollten Anforderungen festgelegt werden. Diese Anforderungen sind von entscheidender Bedeutung und sollten zur Vorbeugung und Aufdeckung von Marktmissbrauch beitragen. Diese Anforderungen sollten sicherzustellen helfen, dass die Meldungen über begründete Verdachtsmomente in Bezug auf Aufträge, Geschäfte und andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie an die zuständigen Behörden aussagekräftig, umfassend und zweckdienlich sind.

(2) Um bei der Vorbeugung und Aufdeckung von Marktmissbrauch wirksam vorgehen zu können, bedarf es geeigneter Systeme zur Überwachung von Aufträgen, Geschäften und anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie entsprechend dem Umfang, der Größe und der Art der Geschäftstätigkeit der Person, die beruflich Geschäfte vermittelt oder ausführt. Diese Systeme sollten von Menschen durchgeführte Untersuchungen vorsehen, die sich auf objektive, dem meldenden Unternehmen vorliegende Informationen stützen und von hinreichend geschulten Personen vorgenommen werden. Das Unternehmen sollte zusätzliche personenbezogene Daten nur erheben, um angemessene, von Menschen durchgeführte Untersuchungen zu gewährleisten. Damit weitere Untersuchungen zu möglichen Insidergeschäften, Marktmanipulation oder dem Versuch hierzu vorgenommen werden können, sollten die Systeme für die Überwachung von Marktmissbrauch vorgegebenen Parametern entsprechend Warnmeldungen ausgeben können. Der Zugang zu solchen Warnmeldungen sollte aufgezeichnet werden, um sicherzustellen, dass sie nur zur Aufdeckung von Marktmissbrauch verwendet werden. Der gesamte Prozess dürfte einen gewissen Grad an Automatisierung erfordern.

(3) Für die Untersuchung, ob die Vorkehrungen, Systeme und Verfahren für die Vorbeugung und Aufdeckung von Marktmissbrauch angemessen sind, müssen die Auswirkungen bewertet werden, die die Person, die beruflich Geschäfte vermittelt oder ausführt, auf den Markt haben kann. Im Rahmen dieser Bewertung sollten diese Personen prüfen, ob sie in einem Segment des Markts für Kryptowerte eine erhebliche oder beherrschende Stellung innehaben; in diesem Fall sollten die Vorkehrungen, Systeme und Verfahren in einem angemessenen Verhältnis zu ihrer Stellung stehen.

(4) Die Vorbeugung und Aufdeckung von Marktmissbrauch bedarf einer fortlaufenden Überwachung aller Aufträge und Geschäfte, die von Personen, die beruflich Geschäfte vermitteln oder ausführen, vermittelt oder ausgeführt werden, unabhängig davon, ob diese Aufträge und Geschäfte über das Distributed Ledger („on-chain“) oder außerhalb des Distributed Ledger („off-chain“) ausgeführt werden, einschließlich Transfers von Kryptowerten auf oder von Konten von Kunden desselben Anbieters von Kryptowerte-Dienstleistungen.

([1]) ABl. L 150 vom 9.6.2023, S. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

(5) Um bei der Vorbeugung und Aufdeckung von Marktmissbrauch sowie dessen Belegung mit Sanktionen unionsweit eine einheitliche Methodik und Vorgehensweise zu fördern, ist es notwendig, den Inhalt des Musters für die Meldung verdächtiger Aufträge und Geschäfte wie auch den Meldezeitpunkt und andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie durch detaillierte Regelungen zu harmonisieren.

(6) Um Ressourcen gemeinsam zu nutzen, Überwachungssysteme zentral zu entwickeln und aufrechtzuerhalten und im Rahmen der Überwachung von Aufträgen und Geschäften neue Kompetenzen zu entwickeln, sollten Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, die Möglichkeit haben, die Vorbeugung und Aufdeckung solcher Aufträge, Geschäfte und anderer Aspekte der Funktionsweise der Distributed-Ledger-Technologie innerhalb einer Gruppe zu übertragen oder aber die Datenanalyse und die Erstellung von Warnmeldungen zu übertragen, sofern geeignete Voraussetzungen gegeben sind. Eine derartige Übertragung sollte die zuständigen Behörden nicht daran hindern, jederzeit zu beurteilen, ob die Vorkehrungen, Systeme und Verfahren der Person, der die Aufgaben übertragen werden, geeignet sind, der Verpflichtung zur Vorbeugung und Aufdeckung von Marktmissbrauch nachzukommen. Die Meldepflicht und die Pflicht zur Einhaltung dieser Verordnung und des Artikels 92 der Verordnung (EU) 2023/1114 sollten bei der übertragenden Person verbleiben.

(7) Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform betreiben, sollten über angemessene Handelsregeln verfügen, die zur Verhinderung von Marktmissbrauch beitragen. Außerdem sollten Möglichkeiten zum Wiederabruf des Orderbuchs vorhanden sein, um die Handelstätigkeiten analysieren zu können.

Ein einheitliches und harmonisiertes Muster für die elektronische Meldung verdächtiger Geschäfte und Aufträge (im Folgenden „Verdachtsmeldung“) sollte bei grenzüberschreitenden Untersuchungen einen effizienten Informationsaustausch zu verdächtigen Aufträgen und Geschäften zwischen zuständigen Behörden erleichtern.

(8) Werden die Informationsfelder des Musters für Verdachtsmeldungen eindeutig, vollständig, objektiv und genau ausgefüllt, sollten die zuständigen Behörden in der Lage sein, auf der Grundlage dieser Angaben die verdächtigen Aufträge und Geschäfte umgehend zu beurteilen und die erforderlichen Maßnahmen zu ergreifen. Ein solches Muster sollte es daher den meldenden Personen ermöglichen, die zu den verdächtigen Aufträgen, Geschäften und anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie von den zuständigen Behörden als relevant angesehenen Informationen bereitzustellen und die Gründe für ihren Verdacht zu erläutern. Mit dem Muster für Verdachtsmeldungen sollte den Personen, die eine Verdachtsmeldung übermitteln, außerdem die Übermittlung personenbezogener Daten möglich sein, anhand derer die Identifizierung der an den verdächtigen Aktivitäten beteiligten Personen vorgenommen werden kann und die die zuständigen Behörden bei ihren Untersuchungen nutzen können. Solche Informationen sollten zudem gleich zu Beginn bereitgestellt werden, sodass die Integrität der Untersuchung nicht dadurch gefährdet wird, dass sich die zuständige Behörde während der Untersuchung möglicherweise mit weiteren Auskunftsersuchen an die Person wenden muss, von der die Verdachtsmeldung übermittelt wurde. Jede Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung sollte gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erfolgen. Um die Einhaltung dieser Verordnung zu gewährleisten. sollte insbesondere der Grundsatz der Datenminimierung eingehalten werden, wenn personenbezogene Daten erhoben werden.

(9) Um die Übermittlung einer Verdachtsmeldung zu erleichtern, sollten dem Muster die zur Untermauerung der Meldung notwendigen Unterlagen und Materialien beigefügt werden können, unter anderem in Form eines Anhangs, in dem die verdächtigen Aufträge oder Geschäfte aufgelistet und ihre Preise und Volumina detailliert angegeben werden. Darüber hinaus sollte das Muster die Meldung verdächtiger Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie ermöglichen.

(10) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, sollten nicht alle eingegangenen Aufträge oder ausgeführten Geschäfte melden, die einen internen Alarm ausgelöst haben. Eine solche Forderung stünde nicht im Einklang mit der Forderung nach Beurteilung auf Einzelfallbasis, ob hinreichende Verdachtsgründe vorliegen.

(11) Bei der Analyse von Aufträgen, Geschäften oder anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie sollten nicht nur die internen Informationen der Person, die beruflich Geschäfte mit Kryptowerten vermittelt oder ausführt, berücksichtigt werden, sondern auch alle öffentlich zugänglichen Informationen, einschließlich Informationen über Geschäfte, die in ein Public-Ledger-System eingebettet sind.

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Die Verdachtsmeldungen sollten der zuständigen Behörde unverzüglich übermittelt werden, sobald ein begründeter Verdacht auf das Vorliegen eines Marktmissbrauchs besteht. Bei der Untersuchung dazu, ob ein Auftrag oder ein Geschäft als verdächtig anzusehen ist, sollte nicht von Spekulationen oder Annahmen, sondern von Tatsachen ausgegangen werden, und sie ist so rasch wie möglich durchzuführen. Eine verzögerte Übermittlung einer Meldung zwecks Einbeziehung weiterer verdächtiger Aufträge, Geschäfte oder anderer Aspekte der Funktionsweise der Distributed-Ledger-Technologie oder das Sammeln mehrerer Verdachtsmeldungen wäre unvereinbar mit der Pflicht zum unverzüglichen Handeln, sobald ein begründeter Verdacht vorliegt. In jedem Fall sollten Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, auf Einzelfallbasis prüfen, ob mehrere Aufträge, Geschäfte oder andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie in einer Meldung zusammengefasst werden könnten.

(13) Folgeereignisse oder die Verfügbarkeit der Informationen können unter Umständen dazu führen, dass ein begründeter Verdacht auf Marktmissbrauch erst geraume Zeit nach der verdächtigen Tätigkeit auftritt. Das sollte kein Grund sein, die verdächtige Tätigkeit der zuständigen Behörde nicht zu melden. Zum Zweck der Einhaltung der Berichterstattungspflichten unter diesen besonderen Umständen sollte die Person, die die Verdachtsmeldung übermittelt, in der Lage sein, den zeitlichen Abstand zwischen der verdächtigen Tätigkeit und dem Auftreten des begründeten Verdachts auf Marktmissbrauch, der begangen wurde, begangen wird oder wahrscheinlich begangen wird, entsprechend zu rechtfertigen.

(14) Für Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, wäre es bei der Beurteilung späterer verdächtiger Aufträge oder Geschäfte hilfreich, wenn sie die im Zusammenhang mit übermittelten Verdachtsmeldungen durchgeführten Analysen ebenso abrufen und prüfen könnten wie die verdächtigen Aufträge, Geschäfte und Verhaltensweisen in Verbindung mit der Funktionsweise der Distributed-Ledger-Technologie, zu denen es zwar eine Untersuchung gab, die Verdachtsgründe von der betreffenden zuständigen Behörde aber für nicht hinreichend befunden wurden.

(15) Um Marktmissbrauch so weit wie möglich zu verhindern, sollten Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, in der Lage sein, ihre Aufsichtssysteme weiterzuentwickeln und wiederholt auftretende Verhaltensweisen, die — in ihrer Gesamtheit betrachtet — zu einem begründeten Verdacht auf Marktmissbrauch führen könnten, zu ermitteln. Diese Personen sollten daher verpflichtet werden, verdächtige Aufträge, Geschäfte, Verhaltensweisen und andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie, die nicht zu einer Verdachtsmeldung geführt haben, zu analysieren und solche Analysen aufzuzeichnen. Solche Aufzeichnungen sollten diesen Personen auch zum Nachweis der Erfüllung der Anforderungen des Artikels 92 der Verordnung (EU) 2023/1114 dienen und den zuständigen Behörden die Wahrnehmung ihrer Überwachungs-, Ermittlungs- und Durchsetzungsaufgaben gemäß Artikel 92 der Verordnung (EU) 2023/1114 erleichtern.

(16) Da Märkte für Kryptowerte naturgemäß grenzüberschreitend sind, müssen Verfahren für die Abstimmung zwischen den jeweils zuständigen Behörden bei der Aufdeckung von Marktmissbrauch und dessen Belegung mit Sanktionen festgelegt werden. Solche Abstimmungsverfahren sollten sicherstellen, dass keine gegensätzlichen Untersuchungen oder Durchsetzungsmaßnahmen durchgeführt werden. In diesem Zusammenhang sollten Fälle von grenzüberschreitendem Marktmissbrauch auch Fälle umfassen, in denen in einem Mitgliedstaat verdächtige Geschäfte mit einem Kryptowert durchgeführt werden, der in einem anderen Mitgliedstaat zum Handel zugelassen ist, sowie Fälle, in denen der betreffende Anbieter von Kryptowerte-Dienstleistungen in mehr als einem Mitgliedstaat tätig ist.

(17) Für die Übermittlung von Verdachtsmeldungen zwischen den zuständigen Behörden sind Vorschriften erforderlich. Diese Vorschriften sind in Ermangelung eines Systems zur Meldung von Geschäften von entscheidender Bedeutung, um eine effiziente Marktaufsicht und Rechtsdurchsetzung zu gewährleisten und gleichzeitig die Übermittlung eines massiven Informationsflusses zu verhindern, der für die empfangende Behörde nicht von Nutzen wäre.

(18) Diese Verordnung basiert auf dem Entwurf technischer Regulierungsstandards, der der Kommission von der Europäischen Wertpapier- und Marktaufsichtsbehörde (im Folgenden „ESMA“) vorgelegt wurde.

(19) Die ESMA hat zu diesem Entwurf öffentliche Konsultationen durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([3]) eingesetzten Interessengruppe Wertpapiere und Wertpapiermärkte eingeholt.

([3]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 ([4]) konsultiert und hat am 22. Januar 2025 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Meldung verdächtiger Geschäfte und Aufträge“ (Verdachtsmeldung) die Meldung verdächtiger Aufträge oder Geschäfte, einschließlich deren Stornierung oder Änderung, und anderer Aspekte der Funktionsweise der Distributed-Ledger-Technologie, wenn Umstände vorliegen könnten, die darauf hindeuten, dass Marktmissbrauch begangen wurde, begangen wird oder wahrscheinlich begangen wird;

2. „elektronische Hilfsmittel“ elektronische Geräte für die Verarbeitung (einschließlich der digitalen Komprimierung), Speicherung und Übertragung von Daten über Kabel, Funk, optische Technologien oder andere elektromagnetische Verfahren;

3. „Gruppe“ eine Gruppe im Sinne von Artikel 2 Nummer 11 der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates ([5]);

4. „Auftrag“ jeden Auftrag, einschließlich aller Quotes, unabhängig davon, ob ihr Zweck in der Ersterteilung, Änderung, Aktualisierung oder Stornierung eines Auftrags besteht sowie unabhängig von dessen Art.

Artikel 2

Allgemeine Anforderungen

(1) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, schaffen und unterhalten Vorkehrungen, Systeme und Verfahren zur Sicherung

a) der wirksamen und fortlaufenden Überwachung aller eingegangenen und übermittelten Aufträge und aller ausgeführten Geschäfte mit Kryptowerten für die Zwecke der Vorbeugung, Aufdeckung und Identifizierung von Aufträgen und Geschäften, wenn Umstände vorliegen könnten, die darauf hindeuten, dass Marktmissbrauch begangen wurde, begangen wird oder wahrscheinlich begangen wird;

b) der wirksamen und fortlaufenden Überwachung von Aspekten der Funktionsweise der Distributed-Ledger-Technologie für die Zwecke der Aufdeckung und Identifizierung anderer Aspekte der Funktionsweise der Distributed-Ledger-Technologie, einschließlich des Konsensmechanismus, wenn Umstände vorliegen könnten, die darauf hindeuten, dass Marktmissbrauch begangen wurde, begangen wird oder wahrscheinlich begangen wird;

c) der Übermittlung von Verdachtsmeldungen an zuständige Behörden entsprechend den Anforderungen dieser Verordnung und unter Verwendung des im Anhang enthaltenen Musters.

([4]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

(2) Die in Absatz 1 genannten Verpflichtungen gelten für Aufträge, Geschäfte und andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie, die Marktmissbrauch darstellen könnten, und gelten unabhängig

a) von der Eigenschaft, in der jemand den Auftrag erteilt oder das Geschäft ausgeführt hat,

b) von den Arten der Kunden, die betroffen sind,

c) davon, ob die Erteilung der Aufträge oder die Ausführung der Geschäfte auf oder außerhalb einer Handelsplattform erfolgt ist.

(3) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, stellen sicher, dass die in Absatz 1 genannten Vorkehrungen, Systeme und Verfahren

a) geeignet sind und in einem angemessenen Verhältnis zu Umfang, Größe und Art ihrer Geschäftstätigkeit stehen,

b) regelmäßig bewertet werden, zumindest durch jährliche Audits und interne Überprüfungen, und dass gegebenenfalls eine Aktualisierung erfolgt,

c) zwecks Einhaltung dieser Verordnung unmissverständlich schriftlich dokumentiert sind, einschließlich Änderungen und Aktualisierungen, und dass die dokumentierten Informationen für einen Zeitraum von fünf Jahren aufbewahrt werden.

(4) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, stellen der zuständigen Behörde auf Anfrage Informationen über die Bewertung gemäß Absatz 3, einschließlich Informationen zum Grad der Automatisierung, zur Verfügung.

Artikel 3

Vorbeugung, Überwachung und Aufdeckung

(1) Die Vorkehrungen, Systeme und Verfahren nach Artikel 92 Absatz 1 der Verordnung (EU) 2023/1114

a) decken das gesamte Spektrum der Handelstätigkeiten der Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, ab,

b) produzieren Warnmeldungen, mit denen Tätigkeiten angezeigt werden, die weitere Untersuchungen für die Zwecke der Aufdeckung von Marktmissbrauch erforderlich machen,

c) ermöglichen Anbietern von Kryptowerte-Dienstleistungen, die eine Handelsplattform betreiben,

   i) einzelne und vergleichende Untersuchungen zu allen innerhalb der Systeme der Handelsplattform ausgeführten Geschäfte und erteilten, geänderten, stornierten oder abgelehnten Aufträgen,

   ii) die Verhinderung des wiederholten Auftretens von beobachteten Verhaltensweisen auf derselben Handelsplattform,

d) ermöglichen Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, einzelne und vergleichende Untersuchungen zu allen innerhalb und außerhalb einer Handelsplattform ausgeführten Geschäften und erteilten, geänderten, stornierten oder abgelehnten Aufträgen, unabhängig davon, ob die Aufträge und Geschäfte mittels Distributed Ledger erteilt und ausgeführt werden, sowie von Aspekten der Funktionsweise der Distributed-Ledger-Technologie, die Marktmissbrauch darstellen könnten.

(2) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, schaffen und unterhalten Vorkehrungen und Verfahren, die gewährleisten, dass bei der Vorbeugung, Überwachung, Aufdeckung und Identifizierung von Geschäften, Aufträgen und Aspekten der Funktionsweise der Distributed-Ledger-Technologie, die auf die Wahrscheinlichkeit oder das Vorliegen von Marktmissbrauch hindeuten, in angemessenem Umfang von Menschen durchgeführte Untersuchungen vorgenommen werden. Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, erheben zusätzliche personenbezogene Daten nur, um in angemessenem Umfang von Menschen durchgeführte Untersuchungen zu gewährleisten.

(3) Für die Zwecke des Artikels 92 Absatz 1 der Verordnung (EU) 2023/1114 setzen Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, IKT-Systeme in einem Umfang ein, der geeignet ist und in einem angemessenen Verhältnis zu Umfang, Größe und Art ihrer Geschäftstätigkeit steht.

Die in Unterabsatz 1 genannten IKT-Systeme umfassen IKT-Systeme zum verzögerten automatischen Lesen, Wiederabrufen und Analysieren von Orderbuchdaten. Diese Systeme verfügen über ausreichende Kapazität für den Einsatz im algorithmischen Handel.

Für die Zwecke des Unterabsatzes 2 bezeichnet „algorithmischer Handel" den Handel mit Kryptowerten, bei denen ein Computeralgorithmus die einzelnen Auftragsparameter automatisch bestimmt, z. B. ob der Auftrag eingeleitet werden soll, Zeitpunkt, Preis bzw. Quantität des Auftrags oder wie der Auftrag nach seiner Einreichung mit eingeschränkter oder gar keiner menschlichen Beteiligung bearbeitet werden soll, unter Ausschluss von Systemen, die nur zur Weiterleitung von Aufträgen zu einem oder mehreren Handelsplattformen, zur Bearbeitung von Aufträgen ohne Bestimmung von Auftragsparametern, zur Bestätigung von Aufträgen oder zur Nachhandelsbearbeitung ausgeführter Aufträge verwendet werden.

(4) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, können im Wege einer schriftlichen Vereinbarung die Wahrnehmung der Aufgaben im Zusammenhang mit der Vorbeugung, Überwachung, Aufdeckung und Identifizierung von Aufträgen, Geschäften oder anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie, die Marktmissbrauch darstellen könnten, an Dritte auslagern oder auf eine juristische Person, die derselben Gruppe angehört, im Sinne des Artikels 2 Nummer 11 der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates [6] (im Folgenden „Anbieter") übertragen, unter anderem die Analyse von Daten, einschließlich Order- und Geschäftsdaten, und der Erstellung von Warnmeldungen. Personen, die diese Aufgaben übertragen oder auslagern, bleiben in vollem Umfang für die Erfüllung aller ihnen aus dieser Verordnung und Artikel 92 der Verordnung (EU) 2023/1114 erwachsenden Pflichten verantwortlich. Werden diese Aufgaben an einen Dritten ausgelagert, erfüllen Personen, die diese Aufgaben auslagern, jederzeit die folgenden Anforderungen:

a) Sie sorgen für die Erhaltung der Fachkenntnisse und der Ressourcen, die erforderlich sind, um

   i) die Qualität der erbrachten Dienstleistungen sowie die Angemessenheit der Organisationsstruktur der Anbieter zu bewerten,

   ii) die Aufsicht über ausgelagerte Dienste auszuüben,

   iii) die mit der Auslagerung dieser Aufgaben verbundenen Risiken kontinuierlich zu steuern.

b) Sie haben unmittelbaren Zugang zu allen relevanten Informationen über die Datenanalyse und die Erstellung von Warnmeldungen.

Die in Unterabsatz 1 genannte schriftliche Vereinbarung enthält die Beschreibung der Rechte und Pflichten der Person, die eine Übertragung oder Auslagerung der Aufgaben vornimmt, sowie der Rechte und Pflichten des Anbieters. Außerdem ist anzugeben, bei Vorliegen welcher Gründe die Person, die die Aufgaben überträgt oder auslagert, die Vereinbarung kündigen kann.

(5) Im Rahmen der Vorkehrungen, Systeme und Verfahren nach den Unterabsätzen 1 und 2 tragen Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, dafür Sorge, dass die Informationen, die die in Bezug auf Aufträge, Geschäfte und Aspekte der Funktionsweise der Distributed-Ledger-Technologie, die Marktmissbrauch darstellen könnten, durchgeführten Untersuchungen belegen, für einen Zeitraum von fünf Jahren auf. Diese Informationen umfassen die durchgeführten Untersuchungen und die Gründe für die Übermittlung oder Nichtübermittlung einer Verdachtsmeldung. Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, legen der zuständigen Behörde diese Informationen auf Anfrage vor.

[6] Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

Artikel 4

Schulung

Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, organisieren und veranstalten effiziente und umfassende Schulungsmaßnahmen für das Personal, das an der Vorbeugung, Überwachung, Aufdeckung und Identifizierung von Aufträgen, Geschäften und anderen Aspekten der Funktionsweise der Distributed-Ledger-Technologie beteiligt ist, die auf Marktmissbrauch hindeuten könnten, wobei auch das mit der Bearbeitung von Aufträgen und Geschäften oder mit der Funktionsweise der Distributed-Ledger-Technologie befasste Personal mit einbezogen wird. Die Schulungsmaßnahmen finden regelmäßig statt, sind für diese Zwecke geeignet und stehen in einem angemessenen Verhältnis zu Umfang, Größe und Art der Geschäftstätigkeit.

Artikel 5

Meldung verdächtiger Aufträge oder Geschäfte

(1) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, schaffen und unterhalten wirksame Vorkehrungen, Systeme und Verfahren, mit deren Hilfe sie zwecks Übermittlung einer Verdachtsmeldung beurteilen können, ob bei einem Auftrag, einem Geschäft oder anderen Aspekten der Distributed-Ledger-Technologie Umstände vorliegen könnten, die darauf hindeuten, dass Marktmissbrauch begangen wurde, begangen wird oder wahrscheinlich begangen wird. Diese Vorkehrungen, Systeme und Verfahren gewährleisten, dass in angemessenem Umfang von Menschen durchgeführte Untersuchungen vorgenommen werden.

(2) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, übermitteln eine Verdachtsmeldung,

a) indem sie das Muster im Anhang verwenden und die für die gemeldeten Aufträge, Geschäfte oder sonstigen Aspekte der Funktionsweise der Distributed-Ledger-Technologie relevanten Informationsfelder eindeutig und detailliert ausfüllen, einschließlich aller Belege oder Anhänge,

b) und die von der zuständigen Behörde angegebenen elektronischen Mittel verwenden.

Für die Zwecke von Unterabsatz 1 Buchstabe b gibt die zuständige Behörde auf ihrer Website an, welche elektronischen Mittel zu verwenden sind, und stellt sicher, dass diese elektronischen Mittel die Wahrung der Vollständigkeit, Integrität und Vertraulichkeit der Informationen während der Übermittlung gewährleisten.

Die in Unterabsatz 1 genannte Verdachtsmeldung basiert auf Fakten und Untersuchungen, wobei alle Informationen berücksichtigt werden, die den Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, zur Verfügung stehen.

(3) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, stellen sicher, dass die Vertraulichkeit der in der Meldung verdächtiger Aufträge oder Geschäfte enthaltenen Informationen gewahrt bleibt und dass die Person, zu der die Verdachtsmeldung übermittelt wurde, und andere Personen, die nicht aufgrund ihrer Funktion oder Position innerhalb der meldenden Person von der Übermittlung der Verdachtsmeldung Kenntnis haben müssen, nicht unterrichtet werden über

a) die Erstellung der Warnmeldungen gemäß Artikel 3 Absatz 1 Buchstabe b,

b) die Bewertung, die zur Übermittlung einer Verdachtsmeldung führen kann,

c) die Tatsache, dass die meldende Person die Verdachtsmeldung ausfüllt, ohne dass zum Zweck des Ausfüllens bestimmter Felder ein Auskunftsersuchen an die Person übermittelt wird, auf die sich die Verdachtsmeldung bezieht,

d) die Übermittlung oder die beabsichtigte Übermittlung einer Verdachtsmeldung an die zuständige Behörde.

Artikel 6

Zeitpunkt der Verdachtsmeldungen

(1) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, stellen sicher, dass sie über wirksame Vorkehrungen, Systeme und Verfahren verfügen, mit deren Hilfe sie bei Aufkommen eines begründeten Verdachts auf Marktmissbrauch unverzüglich eine Verdachtsmeldung übermitteln können.

(2) Hat sich der Verdacht aufgrund von Folgeereignissen oder späteren Informationen ergeben, beinhalten die in Absatz 1 genannten Vorkehrungen, Systeme und Verfahren die Möglichkeit der Übermittlung von Verdachtsmeldungen in Bezug auf Geschäfte, Aufträge oder andere Aspekte der Funktionsweise der Distributed-Ledger-Technologie aus der Vergangenheit. In solchen Fällen erläutern die Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, in der Verdachtsmeldung die zeitliche Verzögerung zwischen dem mutmaßlichen Verstoß und der Übermittlung der Verdachtsmeldung unter Bezugnahme auf die spezifischen Umstände des Falls.

(3) Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen, übermitteln der zuständigen Behörde alle zusätzlichen sachdienlichen Informationen, von denen sie nach der Übermittlung der Verdachtsmeldung Kenntnis erhalten, und stellen alle von der zuständigen Behörde angeforderten Informationen und Unterlagen bereit.

Artikel 7

Austausch von Meldungen zwischen den zuständigen Behörden

(1) Die zuständigen Behörden übermitteln Verdachtsmeldungen unter Verwendung des in Anhang IV der Durchführungsverordnung (EU) 2024/2545 der Kommission ([7]) enthaltenen Formulars für die unaufgeforderte Bereitstellung von Informationen.

(2) Die übermittelnde zuständige Behörde fügt die Verdachtsmeldung dem in Absatz 1 genannten Formular bei, ohne dass es in die Sprache der empfangenden zuständigen Behörde übersetzt werden muss. Die übermittelnde zuständige Behörde fügt der Verdachtsmeldung alle zusätzlichen Unterlagen bei, aus denen die Rechtsgrundlage für die Bereitstellung der Informationen hervorgeht.

Artikel 8

Koordinierungsverfahren für die Aufdeckung von grenzüberschreitendem Marktmissbrauch und dessen Belegung mit Sanktionen

(1) Eine zuständige Behörde, die den Verdacht hat, dass ein grenzüberschreitender Marktmissbrauch stattgefunden hat, möglicherweise stattgefunden hat oder stattfinden könnte, meldet den anderen betroffenen zuständigen Behörden, gegebenenfalls auch den zuständigen Behörden der Handelsplattformen, auf denen der Kryptowert zum Handel zugelassen ist, unverzüglich den Stand ihrer vorläufigen Bewertung.

Werden die empfangenden zuständigen Behörden über grenzüberschreitenden Marktmissbrauch unterrichtet, tauschen sie unverzüglich Informationen über geplante oder laufende Aufsichtstätigkeiten oder -maßnahmen oder gegebenenfalls über laufende strafrechtliche Ermittlungen in dem betreffenden Fall, sofern diese Informationen der empfangenden zuständigen Behörde zur Verfügung stehen, aus.

(2) Die betroffenen zuständigen Behörden

a) halten sich gegenseitig regelmäßig über Fälle von grenzüberschreitendem Marktmissbrauch auf dem Laufenden,

b) unterrichten einander über wesentliche zwischenzeitlich eingetretene Entwicklungen im Zusammenhang mit Fällen von grenzüberschreitendem Marktmissbrauch,

c) koordinieren ihre Aufsichts- und Durchsetzungsmaßnahmen.

([7]) Durchführungsverordnung (EU) 2024/2545 der Kommission vom 24. September 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Muster und Verfahren für die Zusammenarbeit und den Informationsaustausch zwischen zuständigen Behörden (ABl. L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

(3) Eine zuständige Behörde, die förmlich eine Untersuchung oder Durchsetzungsmaßnahme eingeleitet hat oder der gegebenenfalls eine strafrechtliche Ermittlung bekannt ist, unterrichtet die anderen betroffenen zuständigen Behörden, gegebenenfalls auch die zuständigen Behörden der Handelsplattformen, auf denen der Kryptowert zum Handel zugelassen ist. Die meldende zuständige Behörde kann die ESMA unterrichten.

(4) Zuständige Behörden, die eine Untersuchung oder Durchsetzungsmaßnahme im Zusammenhang mit grenzüberschreitenden Fällen eingeleitet haben oder daran beteiligt sind, können die ESMA um Koordinierung ersuchen.

(5) Für die Zwecke dieses Artikels bezeichnet der Ausdruck „Fälle von grenzüberschreitendem Marktmissbrauch" folgende Fälle:

a) Fälle, in denen mehr als eine zuständige Behörde für die Aufdeckung oder Untersuchung eines potenziellen Marktmissbrauchs oder dessen Belegung mit Sanktionen zuständig ist,

b) Fälle, in denen eine Zusammenarbeit zwischen zwei oder mehr zuständigen Behörden erforderlich ist, um einen potenziellen Marktmissbrauchsfall aufzudecken, zu untersuchen oder mit Sanktionen zu belegen.

Artikel 9

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 29. April 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Muster für Verdachtsmeldungen

*Bitte beachten Sie, dass **alle** Felder in den Abschnitten 1 bis 4 Pflichtfelder sind. Können für ein bestimmtes Feld keine Angaben gemacht werden, tragen Sie bitte „N/A“ ein und erläutern Sie kurz die Gründe dafür.*

ABSCHNITT 1 — IDENTITÄT DES UNTERNEHMENS/DER PERSON, DAS/DIE DIE VERDACHTSMELDUNG ÜBERMITTELT

Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen — In jedem Fall genau anzugeben:

Name der natürlichen Person	[Vorname(n) und Nachname(n) der natürlichen Person, die beim meldenden Unternehmen für Verdachtsmeldungen zuständig ist]
Position innerhalb des meldenden Unternehmens	[Position der natürlichen Person, die beim meldenden Unternehmen für Verdachtsmeldungen zuständig ist]
Name des meldenden Unternehmens	[Vollständiger Name des meldenden Unternehmens, einschließlich für juristische Personen: — Rechtsform entsprechend der Eintragung im Register des Landes, nach dessen Recht es gegründet wurde, falls zutreffend, und — Rechtsträger-Kennung (Legal Entity Identifier, LEI) entsprechend LEI-Code nach ISO 17442]
Anschrift des meldenden Unternehmens	[Vollständige Anschrift (z. B. Straße, Hausnummer, Postleitzahl, Stadt, Bundesland/Provinz) und Land]
Eigenschaft, in der das Unternehmen in Bezug auf die Aufträge, Geschäfte oder Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie gehandelt hat, die Marktmissbrauch darstellen könnten	[Beschreibung der Eigenschaft, in der das meldende Unternehmen in Bezug auf den Auftrag/die Aufträge, das Geschäft/die Geschäfte oder die Verhaltensweise/die Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie gehandelt hat, die auf Marktmissbrauch hindeuten könnten, z. B. Auftragsausführung für Kunden, Betrieb einer Handelsplattform...]
Art der Handelstätigkeit des meldenden Unternehmens (Marktpflege, Arbitrage usw.) und Art des von ihm gehandelten Kryptowerts	[Beschreibung aller unternehmensbezogenen, vertraglichen oder organisatorischen Regelungen oder Umstände oder Beziehungen]
Ansprechpartner für weitere Auskunftsersuchen	[Ansprechpartner innerhalb des meldenden Unternehmens für weitere Auskunftsersuchen in Bezug auf diese Meldung (z. B. Compliance-Beauftragter) und entsprechende Kontaktangaben, falls nicht identisch mit der für die Übermittlung der Verdachtsmeldung zuständigen Person: — Vorname(n) und Nachname(n), — Position des Ansprechpartners innerhalb des meldenden Unternehmens, — dienstliche E-Mail-Adresse, — dienstliche Telefonnummer.]
Wurde der Sachverhalt bereits den Behörden gemeldet?	Bitte geben Sie an, ob der Sachverhalt bereits einer Behörde gemeldet wurde (in diesem Fall den Namen der Behörde angeben).

ABSCHNITT 2 — GESCHÄFT/AUFTRAG/VERHALTENSWEISE UND ANDERE ASPEKTE IM ZUSAMMENHANG MIT DER FUNKTIONSWEISE DER DISTRIBUTED-LEDGER-TECHNOLOGIE

Beschreibung des Kryptowerts:	Beschreibung des Kryptowerts/der Kryptowerte, der/die Gegenstand der Verdachtsmeldung ist/sind, mit folgenden genauen Angaben: — vollständige Bezeichnung (einschließlich des Digital Token Identifier (DTI) gemäß ISO 24165-2 oder einer gleichwertigen eindeutigen Kennung gemäß Artikel 15 der Delegierten Verordnung (EU) 2025/1140 der Kommission [1] zur Festlegung der über sämtliche Kryptowerte-Dienstleistungen, Tätigkeiten, Aufträge und Geschäfte zu führenden Aufzeichnungen) oder Beschreibung des Kryptowerts, falls kein DTI vorliegt. Wenn die verdächtige Verhaltensweise ein Handelspaar betrifft, bitte beide Kryptowerte des Handelspaars aufführen, — Art des Kryptowerts (vermögenswertereferenzierter Token (ART), E-Geld-Token (EMT), anderer Kryptowert) und bei ART und EMT Wert, Recht oder amtliche Währung (oder eine Kombination daraus), auf die sich der Kryptowert bezieht, um Wertstabilität zu wahren.
Name(n) des/der Distributed Ledger(s):	[Vollständige(r) Name(n) des/der Distributed Ledger(s), bei dem/denen die verdächtige Verhaltensweise beobachtet wurde]
Handelsplattform, auf der der Auftrag erteilt oder das Geschäft ausgeführt wurde	[Bezeichnung und Market Identifier Code (MIC) gemäß ISO 10383 der Handelsplattform, auf der der Auftrag erteilt oder das Geschäft ausgeführt wurde. Wurde der Auftrag/das Geschäft nicht auf einer Handelsplattform erteilt/ausgeführt, bitte Angabe „außerhalb einer Handelsplattform“ und gegebenenfalls des LEI-Codes des Kryptowerte-Dienstleisters, der das Geschäft ausgeführt hat.]
Ort (Land)	[Vollständiger Name des Landes und ISO-3166-1-Ländercode aus zwei Buchstaben] [Angabe des Orts: — der Auftragserteilung — der Geschäftsausführung — an dem die Verhaltensweise im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie stattfindet]
Beschreibung des Auftrags, des Geschäfts oder des verdächtigen Verhaltens im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie	[Beschreibung zumindest der folgenden Merkmale des Auftrags/der Aufträge, des Geschäfts/der Geschäfte oder der Verhaltensweise/der Verhaltensweisen, zu dem/der/denen die Meldung übermittelt wurde: — Datum und Uhrzeit des Auftrags/der Aufträge, des Geschäfts/der Geschäfte oder der Verhaltensweise/der Verhaltensweisen (Datum und Uhrzeit sind in UTC gemäß dem ISO-8601-Format anzugeben) — Referenznummer des Geschäfts oder des Auftrags oder Transaktionshash — Datum und Zeitpunkt der Abrechnung — Ankaufspreis/Verkaufspreis — Volumen/Menge der Kryptowerte — Art des Auftrags (z. B. „Kauf mit Obergrenze x EUR“) (nur bei Aufträgen)] [Gibt es mehrere Aufträge oder Geschäfte, die Marktmissbrauch darstellen könnten, können genaue Angaben zu deren Preisen und Volumen der zuständigen Behörde in einem Anhang zur Verdachtsmeldung übermittelt werden.]

	— Information zur Auftragsstornierung oder -änderung, einschließlich: — Art der Änderung (z. B. Änderung des Preises oder der Menge) und Umfang der Änderung [Gibt es mehrere Aufträge oder Geschäfte, die Insidergeschäfte, Marktmanipulation oder versuchte Insidergeschäfte oder versuchte Marktmanipulation darstellen könnten, können genaue Angaben zu deren Preisen und Volumen der zuständigen Behörde in einem Anhang zur Verdachtsmeldung übermittelt werden.] — Art und Weise der Auftragsänderung (z. B per E-Mail, Telefon usw.) Falls eine verdächtige Verhaltensweise im Zusammenhang mit der Funktionsweise des Distributed Ledger gemeldet wird, geben Sie bitte so viele Einzelheiten wie möglich an, einschließlich der Auswirkungen auf die Validierung von Geschäften und der Methode, die zur Änderung der Funktionsweise der Distributed-Ledger-Technologie verwendet wurde.
ABSCHNITT 3 — BESCHREIBUNG DER ART DES VERDACHTS	
Art des Verdachts	[Genaue Angabe der Art des Verstoßes, der bei dem gemeldeten Auftrag/den gemeldeten Aufträgen, des gemeldeten Geschäfts/den gemeldeten Geschäften oder der gemeldeten Verhaltensweise/den gemeldeten Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie Marktmissbrauch darstellen könnte]
Gründe für den Verdacht	[Beschreibung der Tätigkeit (Geschäfte und Aufträge, Art und Weise der Auftragserteilung oder der Ausführung der Geschäfte und Merkmale der Aufträge und Geschäfte, die sie verdächtig machen, Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie) und der Umstände, unter denen die meldende Person auf die Angelegenheit aufmerksam wurde, sowie genaue Darlegung der Gründe für den Verdacht. Bei Kryptowerten, die zum Handel auf einer Handelsplattform zugelassen/auf einer Handelsplattform gehandelt werden, eine Beschreibung der Orderbuch-Interaktion/-Geschäfte, die Marktmissbrauch darstellen könnten]
ABSCHNITT 4 — IDENTITÄT DER PERSON(EN), DIE FÜR AUFTRÄGE, GESCHÄFTE ODER VERHALTENSWEISEN IM ZUSAMMENHANG MIT DER FUNKTIONSWEISE DER DISTRIBUTED-LEDGER-TECHNOLOGIE, DIE EINEN MARKTMISSBRAUCH DARSTELLEN KÖNNTEN, VERANTWORTLICH IST/SIND (IM FOLGENDEN „VERDÄCHTIGE PERSON“)	
Name	[Bei natürlichen Personen: Vorname(n) und Nachname(n)] [Bei juristischen Personen: vollständiger Name, einschließlich Rechtsform entsprechend der Eintragung im Register des Landes, nach dessen Recht es gegründet wurde, falls zutreffend, und Rechtsträger-Kennung (Legal Entity Identifier, LEI) entsprechend LEI-Code nach ISO 17442]
Nationale Identifikationsnummer	[Nummer und/oder Text] [Wenn die nationale Identifikationsnummer nicht anwendbar oder bekannt ist, bitte das Geburtsdatum (nur bei natürlichen Personen) im ISO-8601-Format angeben]
Anschrift	[Vollständige Anschrift (z. B. Straße, Hausnummer, Postleitzahl, Stadt, Bundesland/Provinz) und Land]
Angaben zur Beschäftigung: — Ort — Position	[Angaben zur Beschäftigung der verdächtigen Person aus internen Informationsquellen des meldenden Unternehmens (z. B. Kontodokumentation im Fall von Kunden, Mitarbeiterinformationssystem im Fall von Beschäftigten des meldenden Unternehmens)]
Kontonummer(n) und Adresse(n) der elektronischen Geldbörse	[Nummern des Geldkontos/der Geldkonten, alle gemeinsamen Konten oder alle Vollmachten für das Konto des verdächtigen Unternehmens/der verdächtigen Person] Adresse(n) der elektronischen Geldbörse, die an dem Geschäft oder dem verdächtigen Verhalten beteiligt ist/sind]
Kundenkennzeichen	[Falls die verdächtige Person Kunde des meldenden Unternehmens ist]
Verhältnis zum Emittenten des betreffenden Kryptowerts	[Beschreibung aller unternehmensbezogenen, vertraglichen oder organisatorischen Regelungen oder Umstände oder Beziehungen]

ELI: http://data.europa.eu/eli/reg_del/2025/885/oj

ABSCHNITT 5 — ZUSÄTZLICHE INFORMATIONEN

Sonstige Informationen, die je nach Aktivität für die Meldung von Belang sind

[Die nachstehende Liste ist nicht erschöpfend. Geben Sie sonstige Informationen an, die nach Ansicht der meldenden Person für die Meldung zweckdienlich sein können.]

— die Position der verdächtigen Person (z. B. Kleinanleger, Institutionen)

— die Art der Intervention des verdächtigen Unternehmens/der verdächtigen Person (für eigene Rechnung, im Auftrag eines Kunden, eines Validierers von Geschäften in einem Distributed-Ledger-System, Sonstiges)

— Findet die verdächtige Verhaltensweise über eine Distributed-Ledger-Technologie statt, kann es sich bei den sonstigen relevanten Informationen um Folgende handeln:

  — ob das Geschäft vor seiner Validierung über die Distributed-Ledger-Technologie eine öffentliche oder private (verschlüsselte) Transaktionswarteschlange (d. h. Mempool) durchlaufen hat

  — ob die Distributed-Ledger-Technologie öffentlich (zulassungsfrei) oder privat (zulassungsbeschränkt) ist

  — mögliche Interaktionen mit Smart Contracts, z. B. Angabe der Adresse des Vertrags und der Bezeichnung des Funktionsaufrufs

— die Größe des Portfolios des verdächtigen Unternehmens/der verdächtigen Person

— das Datum der Aufnahme der Geschäftsbeziehung mit dem Kunden, sofern das verdächtige Unternehmen/die verdächtige Person Kunde der meldenden Person/des meldenden Unternehmens ist

— die Art der Tätigkeit des Trading Desk, sofern vorhanden, des verdächtigen Unternehmens

— Muster der Handelstätigkeit des verdächtigen Unternehmens/der verdächtigen Person. Als Orientierung nachfolgend einige Beispiele für Informationen, die zweckdienlich sein könnten:

  — Handelsgewohnheiten des verdächtigen Unternehmens/der verdächtigen Person

  — Vergleichbarkeit des Umfangs des gemeldeten Auftrags/Geschäfts mit dem durchschnittlichen Umfang der von dem verdächtigen Unternehmen/der verdächtigen Person in den vergangenen 12 Monaten erteilten Aufträge/ausgeführten Geschäfte

  — Gewohnheiten des verdächtigen Unternehmens/der verdächtigen Person bezüglich der Kryptowerte, die es/sie in den vergangenen 12 Monaten gehandelt hat, speziell der Aspekt, ob sich der gemeldete Auftrag/das gemeldete Geschäft auf einen Kryptowert bezieht, der/die im vorangegangenen Jahr von dem verdächtigen Unternehmen/der verdächtigen Person gehandelt wurde.

— Andere Unternehmen/Personen, die bekanntermaßen in die Aufträge oder Geschäfte einbezogen sind, die Marktmissbrauch darstellen könnten:

  — Namen,

— Tätigkeit (z. B. Auftragsausführung für Kunden, Eigenhandel, Betrieb einer Handelsplattform, Validierung von Geschäften)

ABSCHNITT 6 — BEIGEFÜGTE UNTERLAGEN

[Auflistung der zusammen mit dieser Verdachtsmeldung übermittelten Belege und Materialien]

[Zu diesen Unterlagen gehören beispielsweise E-Mails, Gesprächsaufzeichnungen, Auftrags-/Geschäftsunterlagen, Aufzeichnungen zur Distributed-Ledger-Technologie, Bestätigungen, Brokerberichte, Vollmachten und Medienkommentare, sofern zutreffend.

Werden die in Abschnitt 2 genannten detaillierten Informationen zu den Aufträgen/Geschäften/Verhaltensweisen im Zusammenhang mit der Funktionsweise der Distributed-Ledger-Technologie in einem separaten Anhang bereitgestellt, ist der Titel dieses Anhangs anzugeben.]

([1]) Delegierte Verordnung (EU) 2025/1140 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der über sämtliche Kryptowerte-Dienstleistungen, Tätigkeiten, Aufträge und Geschäfte zu führenden Aufzeichnungen (ABl. L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).