REGULAMENTO DELEGADO (UE) 2025/885 DA COMISSÃO

de 29 de abril de 2025

que complementa o Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os mecanismos, sistemas e procedimentos para prevenir, detetar e comunicar o abuso de mercado, os modelos a utilizar para a comunicação das suspeitas de abuso de mercado e os procedimentos de coordenação entre as autoridades competentes para detetar e sancionar o abuso de mercado em situações transfronteiriças dessa natureza

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo aos mercados de criptoativos e que altera os Regulamento (UE) n.º 1093/2010 e (UE) n.º 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937 ([1]), nomeadamente o artigo 92.º, n.º 2, terceiro parágrafo,

Considerando o seguinte:

(1) As pessoas que, a título profissional, organizem ou executem transações de criptoativos devem estabelecer requisitos quanto aos mecanismos, procedimentos e sistemas de que deverão dispor para a comunicação de ordens, transações e outros aspetos do funcionamento da tecnologia de registo distribuído (DLT), incluindo mecanismos de consenso, quando existam circunstâncias que indiciem que foi, está a ser ou poderá ser praticado algum abuso de mercado. Esses requisitos são fundamentais e devem contribuir para a prevenção e deteção do abuso de mercado. Devem contribuir também para assegurar que as comunicações de suspeitas razoáveis sobre ordens, transações e outros aspetos do funcionamento da tecnologia de registo distribuído (STOR) apresentadas às autoridades competentes sejam significativas, abrangentes e úteis.

(2) A fim de assegurar a eficácia da prevenção e deteção do abuso de mercado, devem existir sistemas adequados de controlo das ordens, das transações e de outros aspetos do funcionamento da DLT, de acordo com a escala, a dimensão e a natureza da atividade económica da pessoa que, a título profissional, organiza ou executa transações. Esses sistemas devem prever uma análise humana realizada por pessoal devidamente qualificado, com base em informações objetivas à disposição da entidade responsável pela comunicação. A entidade deve recolher dados pessoais adicionais, apenas para assegurar uma análise humana adequada. A fim de permitir uma análise mais aprofundada do potencial abuso de informação privilegiada, manipulação de mercado ou tentativa de abuso de informação privilegiada ou de manipulação de mercado, os sistemas de controlo do abuso de mercado devem ser capazes de produzir alertas em conformidade com parâmetros especificados. O acesso a estes alertas deve ficar registado, a fim de garantir que só são utilizados para detetar abusos de mercado. É provável que todo este processo exija um certo nível de automatização.

(3) A fim de analisar se os mecanismos, sistemas e procedimentos para prevenir e detetar abusos de mercado são adequados, é necessário avaliar o impacto que a pessoa que, a título profissional, organiza ou executa transações pode ter no mercado. No âmbito dessa avaliação, a pessoa deverá avaliar se detém uma posição significativa ou dominante em qualquer segmento de ativos do mercado de criptoativos, devendo nesse caso os mecanismos, sistemas e procedimentos ser proporcionados à sua posição.

(4) A prevenção e deteção de abusos de mercado exige um acompanhamento contínuo de todas as ordens e transações organizadas ou executadas por pessoas que, a título profissional, organizem ou executem transações, independentemente de serem executadas no registo distribuído («em cadeia») ou fora dele («fora da cadeia»), incluindo as transferências de criptoativos para ou a partir de contas de clientes do mesmo prestador de serviços de criptoativos.

([1]) JO L 150 de 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

(5) A fim de facilitar e promover uma abordagem e práticas coerentes em toda a União no que se refere a prevenir, detetar e sancionar o abuso de mercado, é necessário estabelecer disposições pormenorizadas que harmonizem o conteúdo, o modelo e o calendário para a comunicação de ordens e transações suspeitas e outros aspetos do funcionamento da DLT.

(6) A fim de partilhar recursos, elaborar e manter sistemas de controlo a nível centralizado e desenvolver experiência no contexto do controlo das ordens e transações suspeitas, as pessoas que, a título profissional, organizam ou executam transações de criptoativos devem poder delegar as tarefas de prevenção e deteção de tais ordens, transações e outros aspetos do funcionamento da DLT no âmbito de um grupo, ou delegar a análise de dados e o lançamento de alertas, sob reserva das condições adequadas. Essa delegação não deverá impedir as autoridades competentes de avaliar, em qualquer momento, se os mecanismos, sistemas e procedimentos da pessoa em quem as funções são delegadas estão efetivamente em conformidade com a obrigação de prevenir e detetar os abusos de mercado. A obrigação de comunicação e a responsabilidade pelo cumprimento do presente regulamento e do artigo 92.º do Regulamento (UE) 2023/1114 incumbirão à pessoa que delega.

(7) Os prestadores de serviços de criptoativos que operam plataformas de negociação devem dispor de regras de negociação adequadas que contribuam para a prevenção do abuso de mercado. Essas entidades devem dispor, além disso, de mecanismos que permitam reproduzir o livro de ordens a fim de analisar a atividade de negociação.

Um modelo único e harmonizado para a apresentação, por via eletrónica, de uma comunicação de transações ou ordens suspeitas («STOR») deverá facilitar a partilha eficiente de informações sobre essas mesmas ordens e transações suspeitas entre as autoridades competentes em investigações transfronteiriças.

(8) Os campos de informação desse modelo STOR, se preenchidos de forma clara, abrangente, objetiva e precisa, devem ajudar as autoridades competentes a avaliar de imediato essas ordens e transações suspeitas e a tomar as medidas necessárias. Esse modelo STOR deve, por conseguinte, permitir que as pessoas que apresentam a STOR forneçam as informações que as autoridades competentes considerem pertinentes sobre suspeitas quanto a ordens, transações ou outros aspetos do funcionamento da tecnologia de registo distribuído comunicados e expliquem as razões da suspeita. O modelo STOR deve também permitir que as pessoas que apresentam a STOR forneçam dados pessoais que possibilitem a identificação das pessoas envolvidas na atividade suspeita e apoiem as autoridades competentes nas suas investigações. Essas informações devem ser facultadas no início, para que a integridade da investigação não seja comprometida pela eventualidade de a autoridade competente ter de voltar a contactar, no decurso de uma investigação, a pessoa que apresentou a STOR. Qualquer tratamento de dados pessoais ao abrigo do presente regulamento deve ser efetuado em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O princípio da minimização dos dados, em particular, deve ser respeitado sempre que sejam recolhidos dados pessoais, a fim de assegurar o cumprimento do referido regulamento.

(9) Para facilitar a apresentação de uma STOR, o modelo deve permitir que sejam anexados documentos e outros elementos necessários para apoiar a notificação efetuada, nomeadamente sob a forma de um anexo que enumere as ordens ou transações suspeitas e especifique os respetivos preços e volumes. Além disso, o modelo STOR deve permitir a comunicação de condutas suspeitas relacionadas com o funcionamento da DLT.

(10) As pessoas que, a título profissional, organizam ou executam transações de criptoativos não devem notificar todas as ordens recebidas ou transações realizadas que desencadearam um alerta interno. Um tal requisito seria incompatível com o requisito de avaliar, caso a caso, se existem motivos razoáveis para suspeitas.

(11) A análise das ordens, transações ou outros aspetos do funcionamento da DLT deve ter em conta não só as informações internas da pessoa que, a título profissional, organiza ou executa transações de criptoativos, mas também todas as informações publicamente disponíveis, incluindo informações sobre transações integradas num sistema de registo público.

([2]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) As STOR devem ser apresentadas de imediato à autoridade competente, assim que se forme uma suspeita razoável da existência de abuso de mercado. A análise com vista a determinar se uma dada ordem ou transação deverá ser considerada suspeita deve basear-se em factos, e não em especulações ou pressuposições, e deve ser realizada com a maior celeridade possível. Adiar a apresentação de uma comunicação no intuito de incorporar outras suspeitas em relação a ordens, transações ou outros aspetos do funcionamento da DLT ou de acumular várias STOR seria incompatível com a obrigação de atuar de imediato, caso já se tenha formado uma suspeita razoável. De qualquer forma, as pessoas que, a título profissional, organizam ou executam transações de criptoativos devem avaliar caso a caso se várias ordens, transações ou outros aspetos do funcionamento da DLT podem ser comunicados numa única STOR.

(13) Podem surgir circunstâncias em que uma suspeita razoável de abuso de mercado ou de tentativa de abuso de informação privilegiada ou de manipulação de mercado se forme depois da ocorrência da atividade suspeita, na sequência de acontecimentos ou informações que surjam posteriormente. Este facto não deve justificar a não comunicação da atividade suspeita à autoridade competente. A fim de demonstrar conformidade com os requisitos em matéria de comunicação de informações nessas circunstâncias específicas, a pessoa que apresenta a STOR deve estar apta a justificar a discrepância temporal entre a ocorrência da atividade suspeita e a formação da suspeita razoável de que foi, está a ser ou poderá ser praticado abuso de mercado.

(14) A fim de ajudar as pessoas que, a título profissional, organizam ou executam transações de criptoativos a exercer juízos quando analisam novas ordens ou transações suspeitas, essas pessoas devem ter a possibilidade de recuperar e rever as análises realizadas a STOR que tenham sido apresentadas, bem como as ordens, transações e condutas suspeitas relacionadas com o funcionamento da DLT analisadas, mas em relação às quais a autoridade competente em causa tenha concluído que não existiam motivos razoáveis para suspeitas.

(15) A fim de prevenir, tanto quanto possível, o abuso de mercado, as pessoas que, a título profissional, organizam ou executam transações de criptoativos devem poder aperfeiçoar os seus sistemas de controlo e detetar padrões de comportamento repetidos, podendo o conjunto destes dados, analisados como um todo, resultar numa suspeita razoável de abuso de mercado. Por conseguinte, essas pessoas devem ter a obrigação de analisar as suspeitas ligadas a ordens, transações, condutas e outros aspetos relacionados com o funcionamento da tecnologia de registo distribuído que não tenham resultado na apresentação de uma STOR e de registar essas análises. Esses registos devem também ajudar essas pessoas a comprovar o cumprimento do artigo 92.º do Regulamento (UE) 2023/1114 e facilitar o desempenho, por parte das autoridades competentes, das suas funções de supervisão, investigação e aplicação da lei decorrentes do mesmo artigo.

(16) Tendo em conta que os mercados de criptoativos são intrinsecamente transfronteiriços, é necessário especificar procedimentos de coordenação entre as autoridades competentes para detetar e sancionar o abuso de mercado em situações transfronteiriças dessa natureza. Esses procedimentos de coordenação devem assegurar que não existam investigações ou atividades de aplicação da lei contraditórias. Nesse contexto, as situações transfronteiriças de abuso de mercado devem incluir os casos em que são efetuadas transações suspeitas num Estado-Membro relativas a um criptoativo admitido à negociação noutro Estado-Membro e os casos em que o prestador de serviços de criptoativos em causa opera em mais do que um Estado-Membro.

(17) É necessário estabelecer disposições para a transmissão das STOR entre as autoridades competentes. Estes requisitos são fundamentais, na ausência de um regime de comunicação das transações, para assegurar que o mercado seja objeto de uma supervisão e aplicação da lei eficientes, evitando simultaneamente a transmissão de um fluxo maciço de informação que não seria útil para a autoridade recetora.

(18) O presente regulamento tem por base os projetos de normas técnicas de regulamentação apresentados à Comissão pela Autoridade Europeia dos Valores Mobiliários e dos Mercados («ESMA»).

(19) A ESMA realizou consultas públicas abertas sobre os projetos de normas técnicas de regulamentação em que se baseia o presente regulamento, analisou os potenciais custos e benefícios associados e solicitou o parecer do Grupo de Interessados do Setor dos Valores Mobiliários e dos Mercados criado em conformidade com o artigo 37.º do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([3]).

([3]) Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/77/CE da Comissão (JO L 331 de 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 ([4]) e emitiu parecer em 22 de janeiro de 2025.

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Comunicação de transações ou ordens suspeitas» (STOR), a comunicação de ordens ou transações suspeitas, incluindo qualquer cancelamento ou modificação das mesmas, e outros aspetos do funcionamento da DLT, caso existam circunstâncias que indiciem que foi, está a ser ou poderá ser praticado abuso de mercado;

2) «Meios eletrónicos», meios eletrónicos para o processamento (incluindo a compressão digital), armazenamento e transmissão de dados por cabo, ondas rádio, tecnologias óticas ou quaisquer outros meios eletromagnéticos;

3) «Grupo», um grupo na aceção do artigo 2.º, ponto 11, da Diretiva 2013/34/UE do Parlamento Europeu e do Conselho ([5]);

4) «Ordem», todas as ordens, incluindo todas as cotações, independentemente de terem por objetivo a apresentação inicial, modificação, atualização ou cancelamento de uma ordem, e independentemente do seu tipo.

Artigo 2.º

Requisitos gerais

1. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem estabelecer e manter mecanismos, sistemas e procedimentos que assegurem:

a) Um acompanhamento eficaz e contínuo para efeitos de prevenção, deteção e identificação de ordens e transações, caso existam circunstâncias que indiciem que foi, está a ser ou poderá ser praticado abuso de mercado, de todas as ordens recebidas e transmitidas e de todas as transações de criptoativos executadas;

b) Um acompanhamento eficaz e contínuo dos aspetos do funcionamento da DLT, a fim de detetar e identificar outros aspetos desse mesmo funcionamento, incluindo o mecanismo de consenso, caso existam circunstâncias que indiciem que foi, está a ser ou poderá ser praticado abuso de mercado;

c) A transmissão de STOR às autoridades competentes em conformidade com os requisitos previstos no presente regulamento e utilizando o modelo apresentado no anexo.

([4]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Diretiva 2013/34/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa às demonstrações financeiras anuais, às demonstrações financeiras consolidadas e aos relatórios conexos de certas formas de empresas, que altera a Diretiva 2006/43/CE do Parlamento Europeu e do Conselho e revoga as Diretivas 78/660/CEE e 83/349/CEE do Conselho (JO L 182 de 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

2. As obrigações a que se refere o n.º 1 aplicam-se às ordens, transações e outros aspetos do funcionamento da DLT que possam constituir abuso de mercado e são aplicáveis independentemente:

a) Do título a que a ordem é colocada ou a transação é executada;

b) Do tipo de clientes em causa;

c) De as ordens terem ou não sido colocadas, ou de as transações terem ou não sido executadas, numa plataforma de negociação.

3. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem assegurar que os mecanismos, sistemas e procedimentos referidos no n.º 1 são:

a) Adequados e proporcionados em relação à escala, dimensão e natureza da sua atividade económica;

b) Avaliados regularmente, pelo menos através de uma auditoria e revisão interna realizadas anualmente, e atualizados sempre que necessário;

c) Documentados claramente por escrito, incluindo as suas eventuais alterações ou atualizações, para efeitos de cumprimento do presente regulamento, e que as informações documentadas são conservadas durante um período de cinco anos.

4. As pessoas que, a título profissional, organizam ou executam transações de criptoativos facultam à autoridade competente, a pedido desta, as informações sobre a avaliação a que se refere o n.º 3, incluindo informações sobre o nível de automatização aplicado.

Artigo 3.º

Prevenção, controlo e deteção

1. Os mecanismos, sistemas e procedimentos a que se refere o artigo 92.º, n.º 1, do Regulamento (UE) 2023/1114:

a) Abrangem toda a gama de atividades de negociação realizadas pelas pessoas que, a título profissional, organizam ou executam transações de criptoativos;

b) Emitem alertas que indicam as atividades que requerem uma análise mais aprofundada para se detetar um potencial abuso de mercado;

c) Permitem que os prestadores de serviços de criptoativos que operam uma plataforma de negociação:

   i) efetuem uma análise, individual e comparativa, de todas as transações executadas e de todas as ordens colocadas, modificadas, canceladas ou rejeitadas nos sistemas da plataforma de negociação,

   ii) previnam a ocorrência de condutas repetidas observadas na mesma plataforma de negociação;

d) Permitem que as pessoas que, a título profissional, organizam ou executam transações de criptoativos efetuem uma análise individual e comparativa de todas as transações executadas e de todas as ordens colocadas, modificadas, canceladas ou rejeitadas dentro e fora de uma plataforma de negociação, independentemente de serem ou não colocadas e executadas através do registo distribuído, bem como dos aspetos do funcionamento da DLT suscetíveis de constituir abuso de mercado.

2. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem estabelecer e manter mecanismos e procedimentos destinados a assegurar um nível adequado de análise humana para efeitos de prevenção, controlo, deteção e identificação de transações, ordens e aspetos do funcionamento da tecnologia de registo distribuído que indiciem a probabilidade ou a existência de condutas de abuso de mercado. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem recolher dados pessoais adicionais, com o único objetivo de assegurar um nível adequado de análise humana.

3. Para efeitos do artigo 92.º, n.º 1, do Regulamento (UE) 2023/1114, as pessoas que, a título profissional, organizam ou executam transações de criptoativos utilizam sistemas de TIC na medida adequada e proporcionada em relação à escala, dimensão e natureza da sua atividade económica.

Os sistemas de TIC a que se refere o primeiro parágrafo incluem sistemas de TIC que permitam, de forma automatizada e *a posteriori*, a leitura, reprodução e análise de dados do livro de ordens. Esses sistemas devem ter capacidade suficiente para funcionar num ambiente de negociação algorítmica.

Para efeitos do segundo parágrafo, entende-se por negociação algorítmica a negociação de criptoativos em que um algoritmo informático determina automaticamente os parâmetros individuais das ordens, incluindo se deverá ou não ser acionada, o calendário, o preço ou a quantidade da ordem ou o modo de gestão após a sua introdução, com pouca ou nenhuma intervenção humana. Esta definição não inclui qualquer sistema utilizado apenas para fins de encaminhamento de ordens para uma ou mais plataformas de negociação, para o processamento de ordens que não envolvam a determinação de parâmetros de negociação ou para a confirmação das ordens ou o processamento pós-negociação das transações executadas.

4. As pessoas que, a título profissional, organizam ou executam transações de criptoativos podem, mediante acordo escrito, subcontratar a terceiros ou delegar numa pessoa coletiva que faça parte do mesmo grupo, na aceção do artigo 2.º, ponto 11, da Diretiva 2013/34/UE do Parlamento Europeu e do Conselho ([6]), («prestadores de serviços»), as funções relacionadas com a prevenção, controlo, deteção e identificação de ordens, transações ou outros aspetos do funcionamento da DLT que possam constituir abuso de mercado, incluindo a análise de dados, nomeadamente respeitantes a ordens e transações, e o lançamento de alertas. As pessoas que delegam ou subcontratam essas funções continuam a ser plenamente responsáveis pelo cumprimento de todas as obrigações que lhes incumbem por força do presente regulamento e do artigo 92.º do Regulamento (UE) 2023/1114. Caso essas funções sejam subcontratadas a terceiros, as pessoas que subcontratam essas funções devem cumprir em permanência os seguintes requisitos:

a) Conservar as competências e os recursos necessários para:

   i) avaliar a qualidade dos serviços prestados e a adequação organizativa dos prestadores de serviços,

   ii) controlar os serviços subcontratados,

   iii) gerir os riscos associados à subcontratação dessas funções, de forma contínua;

b) Dispor de acesso direto a todas as informações relevantes sobre a análise de dados e a emissão de alertas.

O acordo escrito a que se refere o primeiro parágrafo deve conter a descrição dos direitos e obrigações da pessoa que delega ou subcontrata as funções e do prestador de serviços. Deve, além disso, estipular os fundamentos com base nos quais a pessoa que delega ou subcontrata as funções pode rescindir o acordo.

5. No âmbito dos mecanismos, sistemas e procedimentos a que se referem o primeiro e o segundo parágrafos, as pessoas que, a título profissional, organizam ou executam transações de criptoativos devem conservar, por um período de cinco anos, as informações relativas à análise realizada no que respeita às ordens, transações e aspetos do funcionamento da DLT que possam constituir abuso de mercado. Essas informações devem incluir a análise efetuada e as razões para a apresentação ou não de uma STOR. As pessoas que, a título profissional, organizam ou executam transações de criptoativos facultam essas informações à autoridade competente, a pedido desta.

([6]) Diretiva 2013/34/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa às demonstrações financeiras anuais, às demonstrações financeiras consolidadas e aos relatórios conexos de certas formas de empresas, que altera a Diretiva 2006/43/CE do Parlamento Europeu e do Conselho e revoga as Diretivas 78/660/CEE e 83/349/CEE do Conselho (JO L 182 de 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

Artigo 4.º

Formação

As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem organizar e proporcionar formação eficaz e abrangente ao pessoal envolvido no controlo, deteção e identificação de ordens, transações e outros aspetos do funcionamento da DLT que possam indiciar a existência de abuso de mercado, incluindo o pessoal envolvido no processamento das ordens e transações ou responsável pelo funcionamento da DLT. Essa formação deve ter lugar regularmente e ser adequada e proporcionada à escala, dimensão e natureza da atividade em questão.

Artigo 5.º

Comunicação de ordens ou transações suspeitas

1. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem estabelecer e manter mecanismos, sistemas e procedimentos eficazes que lhes permitam avaliar, para efeitos da apresentação de uma STOR, se, com referência a uma ordem, transação ou outros aspetos da DLT, existem circunstâncias que indiciem que foi, está a ser ou poderá ser praticado abuso de mercado. Esses mecanismos, sistemas e procedimentos devem incluir um nível adequado de análise humana.

2. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem comunicar uma STOR:

a) Utilizando o modelo STOR constante do anexo e preenchendo os campos de informação relevantes para as ordens, transações ou outros aspetos do funcionamento da DLT comunicados, de forma clara e precisa, incluindo quaisquer documentos comprovativos ou anexos;

b) Através dos meios eletrónicos especificados por essa autoridade competente.

Para efeitos da alínea b) do primeiro parágrafo, a autoridade competente especifica no seu sítio Web os meios eletrónicos a utilizar e assegura que esses meios eletrónicos garantem a exaustividade, integridade e confidencialidade das informações durante a transmissão.

A STOR a que se refere o primeiro parágrafo será baseada em factos e análises, tendo em conta todas as informações de que dispõem as pessoas que, a título profissional, organizam ou executam transações de criptoativos.

3. As pessoas que, a título profissional, organizam ou executam transações de criptoativos asseguram e mantêm a confidencialidade das informações constantes da comunicação sobre ordens ou transações suspeitas e asseguram que a pessoa relativamente à qual foi apresentada uma STOR, bem como todas as pessoas que não tenham necessidade de ter conhecimento da apresentação dessa STOR em virtude da sua função ou cargo junto da pessoa que apresenta a STOR, não sejam informadas:

a) Da emissão dos alertas a que se refere o artigo 3.º, n.º 1, alínea b);

b) Da avaliação que pode conduzir à apresentação de uma STOR;

c) Do facto de que a pessoa que apresenta a declaração irá preencher a STOR sem enviar pedidos de informação à pessoa a respeito da qual a STOR pode ser apresentada, no sentido de que preencha determinados campos do modelo;

d) Da apresentação de uma STOR à autoridade competente ou da intenção de a apresentar.

Artigo 6.º

Prazos para apresentação das STOR

1. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem assegurar que dispõem de mecanismos, sistemas e procedimentos eficazes para efeitos da apresentação sem demora de uma STOR, assim que surjam suspeitas razoáveis de abuso de mercado.

2. Os mecanismos, sistemas e procedimentos mencionados no n.º 1 implicam a possibilidade de comunicar STOR relativamente a transações, ordens ou outros aspetos do funcionamento da DLT que tenham ocorrido no passado, caso a suspeita tenha surgido em virtude de acontecimentos ou informações posteriores. Nesses casos, as pessoas que, a título profissional, organizam ou executam transações de criptoativos devem justificar, na STOR, o tempo decorrido entre a suspeita de fuga de informação e a apresentação da STOR, de acordo com as circunstâncias específicas do caso.

3. As pessoas que, a título profissional, organizam ou executam transações de criptoativos devem apresentar à autoridade competente qualquer informação adicional de que tomem conhecimento depois de a STOR ter sido apresentada, devendo facultar a essa autoridade qualquer informação ou documento que esta lhes solicite.

Artigo 7.º

Troca de informações entre autoridades competentes

1. As autoridades competentes transmitem as STOR utilizando o formulário de comunicação de informações não solicitadas definido no anexo IV do Regulamento de Execução (UE) 2024/2545 da Comissão ([7]).

2. A autoridade competente remetente deve anexar a STOR ao formulário referido no n.º 1, sem ser obrigada a traduzi-lo para a língua da autoridade competente recetora. A autoridade competente remetente deve incluir quaisquer documentos adicionais apresentados na STOR, especificando a base jurídica para a prestação das informações.

Artigo 8.º

Procedimentos de coordenação para detetar e sancionar situações transfronteiriças de abuso de mercado

1. Uma autoridade competente que suspeite que ocorreu, pode ter ocorrido ou pode vir a ocorrer uma situação transfronteiriça de abuso de mercado comunica o estado da sua avaliação preliminar às outras autoridades competentes em causa, sem demora injustificada, incluindo, se for caso disso, às autoridades competentes das plataformas de negociação em que o criptoativo se encontra admitido à negociação.

Quando forem informadas sobre situações transfronteiriças de abuso de mercado, as autoridades competentes recetoras partilham, sem demora injustificada, informações sobre o planeamento ou a existência de qualquer atividade ou medida de supervisão ou, se for caso disso, e se a autoridade competente recetora dispuser dessas informações, sobre uma investigação criminal em curso sobre o mesmo caso.

2. As autoridades competentes em causa:

a) Mantêm-se mutuamente informadas, de forma periódica, sobre as situações transfronteiriças de abuso de mercado;

b) Informam-se mutuamente sobre evoluções intercalares significativas relacionadas com situações transfronteiriças de abuso de mercado;

c) Coordenam as suas ações de supervisão e de aplicação da lei.

([7]) Regulamento de Execução (UE) 2024/2545 da Comissão, de 24 de setembro de 2024, que estabelece normas técnicas de execução para a aplicação do Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho no que diz respeito aos formulários, modelos e procedimentos normalizados para a cooperação e troca de informações entre autoridades competentes (JO L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

3. Uma autoridade competente que tenha iniciado formalmente uma investigação, uma atividade de aplicação da lei ou, se for o caso, que tenha conhecimento de uma investigação criminal informa desse facto as outras autoridades competentes em causa, incluindo, se for caso disso, as autoridades competentes das plataformas de negociação em que o criptoativo se encontra admitido à negociação. A autoridade competente que comunica as informações pode informar a ESMA.

4. As autoridades competentes que tenham iniciado ou participado numa investigação ou numa atividade de aplicação da lei no contexto de situações transfronteiriças podem solicitar a coordenação da ESMA.

5. Para efeitos do presente artigo, entende-se por «situações transfronteiriças de abuso de mercado» qualquer uma das seguintes situações:

a) Uma situação em que mais do que uma autoridade é competente para detetar, investigar ou sancionar um potencial caso de abuso de mercado;

b) Uma situação em que é necessária a cooperação entre duas ou mais autoridades competentes para detetar, investigar ou sancionar um potencial caso de abuso de mercado.

Artigo 9.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 29 de abril de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

Modelo de STOR

*Chama-se a atenção para o facto de que **todos** os campos das secções 1 a 4 são obrigatórios. Se não for possível fornecer informações relativamente a um campo específico, indicar «NA» e explicar sucintamente as razões para tal.*

SECÇÃO 1 — IDENTIDADE DA ENTIDADE/PESSOA QUE APRESENTA A STOR

Pessoas que, a título profissional, organizam ou executam transações de criptoativos — Especificar em cada caso:

Nome da pessoa singular	[Nome(s) próprio(s) e apelido(s) da pessoa singular, dentro da entidade autora da comunicação, que é encarregada de apresentar a STOR.]
Cargo junto da entidade autora da comunicação	[Cargo, na entidade autora da comunicação, da pessoa singular que é encarregada de apresentar a STOR.]
Designação da entidade autora da comunicação	[Designação completa da entidade autora da comunicação, incluindo, caso se trate de uma pessoa coletiva: — a sua forma jurídica, tal como consta do registo do país ao abrigo de cuja lei foi constituída, se aplicável, e — o código identificador de entidade jurídica (LEI) em conformidade com a norma ISO 17442.]
Endereço da entidade autora da comunicação	[Endereço completo (por exemplo, rua, número de porta, código postal, localidade, distrito/província) e país.]
Título a que atua a entidade relativamente às ordens, transações ou condutas relacionadas com o funcionamento da DLT que possam constituir abuso de mercado	[Descrição do título a que a entidade autora da comunicação atuava relativamente à ou às ordens, transações ou condutas relacionadas com o funcionamento da tecnologia de registo distribuído suscetíveis de indiciar a existência de abuso de mercado, por exemplo, execução de ordens em nome de clientes, operação de uma plataforma de negociação...]
Tipo de atividade de negociação (criação de mercado, arbitragem, etc.) e tipo de criptoativo negociado pela entidade autora da comunicação	[Descrição de quaisquer acordos, circunstâncias ou relações de natureza comercial, contratual ou organizativa.]
Contacto para pedido de informações adicionais	[Pessoa a contactar, junto da entidade autora da comunicação, para eventuais pedidos de informações adicionais relacionadas com esta comunicação (por exemplo, responsável pela conformidade), bem como os respetivos dados de contacto, se não for a mesma pessoa responsável pela apresentação da STOR: — nome(s) próprio(s) e apelido(s), — cargo da pessoa de contacto na entidade autora da comunicação, — endereço de correio eletrónico profissional, — número de telefone profissional.]
Os factos já foram comunicados às autoridades públicas?	Indicar se os factos já foram comunicados a uma autoridade pública (e, nesse caso, indicar o nome da autoridade).

SECÇÃO 2 — TRANSAÇÃO/ORDEM/CONDUTA E OUTROS ASPETOS RELACIONADOS COM O FUNCIONAMENTO DA TECNOLOGIA DE REGISTO DISTRIBUÍDO

Descrição do criptoativo:	Descrever o(s) criptoativo(os) que é(são) objeto da STOR, especificando: — o nome completo [incluindo o identificador de criptoficha digital (DTI) em conformidade com a norma ISO 24165-2 ou um identificador único equivalente a que se refere o artigo 15.º do Regulamento Delegado (UE) 2025/1140 da Comissão ([1]), que especifica os registos a manter para todos os serviços, atividades, ordens e transações de criptoativos realizadas] ou a descrição do criptoativo, na ausência do DTI. Sempre que a conduta suspeita envolver um par de negociação, indicar ambos os criptoativos desse par, — o tipo de criptoativo [criptoficha referenciada a ativos (ART), criptoficha de moeda eletrónica (EMT), outro criptoativo] e, para as criptofichas referenciadas a ativos e as criptofichas em moeda eletrónica, o valor, direito ou moeda oficial (ou a combinação dos mesmos) a que o criptoativo faz referência a fim de manter um valor estável.
Nome(s) do(s) registo(s) distribuído(s):	[Indicar o(s) nome(s) completa(s) do(s) registo(s) distribuído(s) onde foi observada a conduta suspeita.]
Plataforma de negociação em que a ordem foi colocada ou a transação foi executada	[Especificar o nome e o código de identificação do mercado (MIC), de acordo com a norma ISO 10383, para identificar a plataforma de negociação em que a ordem foi colocada ou a transação foi executada. Se a ordem/transação não foi identificada numa plataforma de negociação, indicar «fora de uma plataforma de negociação» e o identificador de entidade jurídica do prestador de serviços de criptoativos que realizou a transação, se for caso disso.]
Localização (país)	[Nome completo do país e código de país com dois carateres conforme definido na ISO 3166-1.] [Especificar onde: — a ordem é emitida, — a transação é executada, — tem lugar a conduta relacionada com o funcionamento da tecnologia de registo distribuído.]
Descrição da ordem, transação ou conduta suspeita relacionada com o funcionamento da DLT	[Descrever pelo menos as seguintes características da(s) ordem(ns), transação(ões) ou conduta(s) comunicada(s): — a(s) data(s) e hora(s) da(s) ordem(ns), transação(ões) ou conduta(s). (As datas e as horas têm de ser comunicadas em UTC, de acordo com o formato previsto na norma ISO 8601), — o número de referência da transação ou o número de referência da ordem ou *hash* da transação, — a data e hora da liquidação, — o preço de compra/preço de venda, — o volume/quantidade de criptoativos, — apenas para as ordens, o tipo de ordem (por exemplo, «compra com limite de x EUR»)], [Caso existam várias ordens ou transações que possam constituir abuso de mercado, os dados relativos aos preços e volumes dessas ordens ou transações podem ser facultados à autoridade competente num anexo à STOR.]

	— Informação sobre o cancelamento ou alteração da ordem, incluindo: — a natureza da alteração (por exemplo, alteração do preço ou da quantidade) e a respetiva extensão, [Caso existam várias ordens ou transações que possam constituir abuso de informação privilegiada, manipulação de mercado ou tentativa de abuso de informação privilegiada ou de manipulação de mercado, os dados relativos aos preços e volumes dessas ordens ou operações podem ser facultados à autoridade competente num anexo à STOR.] — o meio pelo qual é feita a alteração da ordem (por exemplo, correio eletrónico, telefone, etc.). Em caso de comunicação de um comportamento suspeito relacionado com o funcionamento do registo distribuído, forneça informações o mais pormenorizadas possível, incluindo o seu impacto na validação das transações e o método utilizado para alterar o funcionamento da DLT.
SECÇÃO 3 — DESCRIÇÃO DA NATUREZA DA SUSPEITA	
Natureza da suspeita	[Especificar o tipo de infração com base na qual a(s) ordem(ns), transação(ões) ou conduta(s) relacionada(s) com o funcionamento da DLT pode(m) constituir abuso de mercado].
Fundamentação da suspeita	[Descrever a atividade (transações e ordens, modo de colocação das ordens ou de execução da operação e características das ordens ou operações que as tornam suspeitas, condutas relacionadas com o funcionamento da DLT) e o modo como o assunto chegou ao conhecimento do autor da comunicação, especificando os motivos para a suspeita. Para criptoativos admitidos à negociação/negociados numa plataforma de negociação, uma descrição da natureza das operações e interações no seio do livro de ordens que podem constituir abuso de mercado.]
SECÇÃO 4 — IDENTIFICAÇÃO DA PESSOA OU PESSOAS RESPONSÁVEIS PELAS ORDENS, TRANSAÇÕES OU CONDUTAS RELACIONADAS COM O FUNCIONAMENTO DA TECNOLOGIA DE REGISTO DISTRIBUÍDO QUE PODEM CONSTITUIR ABUSO DE MERCADO («PESSOA SUSPEITA»)	
Nome	[Caso se trate de uma pessoa singular: nome(s) próprio(s) e apelido(s).] [Caso se trate de uma pessoa coletiva: denominação completa, incluindo a forma jurídica tal como consta do registo do país ao abrigo de cuja legislação foi constituída, se aplicável, e o código identificador de entidade jurídica (LEI) em conformidade com a norma ISO 17442,]
Número de identificação nacional	[Número e/ou texto]. [Se o número de identificação nacional não for aplicável ou conhecido, indicar uma data de nascimento (apenas para as pessoas singulares) no formato ISO 8601]
Endereço	[Endereço completo (por exemplo, rua, número de porta, código postal, localidade, distrito/província) e país.]
Informações sobre o emprego: — Local — Cargo	[Informações sobre o emprego da pessoa suspeita, provenientes de fontes de informação disponíveis internamente para a entidade autora da comunicação (por exemplo, documentação da conta no caso de clientes, sistema de informação sobre o pessoal no caso de um trabalhador da entidade autora da comunicação).]
Número(s) de conta e endereço(s) de carteira	[Número(s) da(s) conta(s) em numerário, eventuais contas conjuntas ou eventuais procurações relativas à conta da entidade/pessoa suspeita. Endereço(s) de carteira envolvido(s) na transação ou na conduta suspeita]
Identificador do cliente	[Caso a pessoa suspeita seja um cliente da entidade autora da comunicação.]
Relação com o emitente do criptoativo em causa	[Descrição de quaisquer acordos, circunstâncias ou relações de natureza comercial, contratual ou organizativa]

SECÇÃO 5 — INFORMAÇÕES ADICIONAIS

Outras informações pertinentes para a comunicação, em função da atividade

[A lista que se segue é indicativa e não exaustiva. A pessoa que apresenta a comunicação pode fornecer outras informações que considere úteis, se tal for pertinente para a STOR.]

— a situação da pessoa suspeita (por exemplo, cliente de retalho, instituição),
— a natureza da intervenção da entidade/pessoa suspeita (por conta própria, em nome de um cliente, validador de transações num sistema de registo distribuído, outra).
— Quando a conduta suspeita é praticada numa DLT, as outras informações pertinentes podem incluir:
  — se a transação passou por uma fila pública ou privada (encriptada) de transações (o chamado *mempool*) antes de ser validada na DLT,
  — se a DLT é pública (sem autorização) ou privada (com autorização),
  — potenciais interações com contratos inteligentes, incluindo a especificação do endereço do contrato e da função invocada,
— a dimensão da carteira da entidade/pessoa suspeita,
— a data em que teve início a relação comercial com o cliente, se a entidade/pessoa suspeita for um cliente da pessoa/entidade autora da comunicação,
— o tipo de atividade da sala de negociação, se disponível, da entidade suspeita,
— padrões de negociação da entidade/pessoa suspeita. A título de orientação, seguem-se exemplos de informações que podem ser úteis:
  — hábitos de negociação da entidade/pessoa suspeita,
  — comparabilidade da dimensão da ordem/transação comunicada com a dimensão média das ordens colocadas/operações efetuadas pela entidade/pessoa suspeita nos últimos 12 meses,
  — hábitos da entidade/pessoa suspeita no que diz respeito aos criptoativos negociados nos últimos 12 meses, em particular se a ordem/transação comunicada diz respeito a um criptoativo que foi negociado pela entidade/pessoa suspeita no último ano.
— Outras entidades/pessoas que se saiba estarem envolvidas nas ordens ou transações que podem constituir abuso de mercado:
  — nomes,
— atividade (por exemplo, execução de ordens em nome de clientes, negociação por conta própria, exploração de uma plataforma de negociação, validação de transações.)

SECÇÃO 6 — DOCUMENTAÇÃO EM ANEXO

[Enumerar os anexos e elementos de apoio fornecidos juntamente com esta STOR.]

[Trata-se, por exemplo, de mensagens de correio eletrónico, registos de conversas, registos de ordens/transações, registos de tecnologia de registo distribuído, confirmações, relatórios de corretores, procurações e observações dos meios de comunicação social, se for caso disso.

Se as informações pormenorizadas relativas às ordens/transações/condutas relacionadas com o funcionamento da tecnologia de registo distribuído referida na secção 2 forem fornecidas num anexo separado, indicar o título desse anexo.]

([1]) Regulamento Delegado (UE) 2025/1140 da Comissão, de 27 de fevereiro de 2025, que complementa o Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os registos a manter para todos os serviços, atividades, ordens e transações de criptoativos realizadas (JO L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).