Journal officiel
de l'Union européenne

FR
Série L

2025/885

20.8.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/885 DE LA COMMISSION

du 29 avril 2025

complétant le règlement (UE) 2023/1114 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les dispositifs, systèmes et procédures permettant de prévenir, de détecter et de signaler les abus de marché, les modèles à utiliser pour signaler les abus de marché présumés et les procédures de coordination entre les autorités compétentes en vue de la détection et de la répression des abus de marché comportant une dimension transfrontière

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) nº 1093/2010 et (UE) nº 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 ([1]), et notamment son article 92, paragraphe 2, troisième alinéa,

considérant ce qui suit:

(1) Des exigences doivent être établies en ce qui concerne les dispositifs, procédures et systèmes que les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs doivent mettre en place pour la déclaration des ordres, des transactions et d'autres aspects du fonctionnement de la technologie des registres distribués (DLT), y compris le mécanisme de consensus, lorsque des circonstances pourraient indiquer qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis. Ces exigences sont essentielles et devraient contribuer à la prévention et à la détection des abus de marché. Elles devraient également contribuer à faire en sorte que les signalements adressés aux autorités compétentes faisant état de soupçons raisonnables concernant des ordres, des transactions et d'autres aspects du fonctionnement de la technologie des registres distribués (STOR) soient pertinents, complets et utiles.

(2) Afin de garantir l'efficacité de la prévention et de la détection des abus de marché, des systèmes appropriés devraient être mis en place pour surveiller les ordres, les transactions et d'autres aspects du fonctionnement de la DLT, en fonction de l'échelle, du volume et de la nature de l'activité de la personne qui organise ou exécute des transactions à titre professionnel. Ces systèmes devraient prévoir une analyse humaine effectuée par du personnel dûment formé, sur la base des informations objectives à la disposition de l'entité déclarante. L'entité ne devrait collecter des données à caractère personnel supplémentaires que pour garantir une analyse humaine appropriée. Afin de permettre une analyse plus approfondie des éventuelles opérations d'initiés, manipulations de marché ou tentatives d'opération d'initié ou de manipulation de marché, les systèmes de surveillance des abus de marché devraient être à même d'émettre des alertes selon des paramètres prédéfinis. L'accès à ces alertes devrait être enregistré afin de garantir qu'elles ne sont utilisées que pour détecter les abus de marché. Il est probable que l'ensemble du processus nécessite un certain niveau d'automatisation.

(3) Pour déterminer si les dispositifs, systèmes et procédures de prévention et de détection des abus de marché sont appropriés, il est nécessaire d'évaluer l'incidence que la personne qui exécute ou organise des transactions à titre professionnel est susceptible d'avoir sur le marché. Dans le cadre de cette évaluation, ces personnes devraient déterminer si elles occupent une position importante ou dominante sur un segment d'actifs du marché des crypto-actifs, auquel cas ces dispositifs, systèmes et procédures devraient être proportionnés à leur position.

(4) La prévention et la détection des abus de marché nécessitent une surveillance continue de tous les ordres et toutes les transactions organisés ou exécutés par des personnes qui organisent ou exécutent des transactions à titre professionnel, que ces ordres et transactions soient exécutés dans le registre distribué («sur chaîne») ou en dehors du registre distribué («hors chaîne»), y compris les transferts de crypto-actifs vers ou depuis les comptes de clients d'un même prestataire de services sur crypto-actifs.

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

(5) Afin de faciliter et de promouvoir une approche et des pratiques uniformes dans toute l'Union en matière de prévention, de détection et de répression des abus de marché, il est nécessaire d'établir des dispositions détaillées harmonisant le contenu, le modèle et le délai de déclaration des ordres et transactions suspects et autres aspects suspects du fonctionnement de la DLT.

(6) Afin de partager les ressources, de mettre en place et de maintenir des systèmes de surveillance au niveau central et d'acquérir une expertise en matière de surveillance des ordres et des transactions suspects, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs devraient pouvoir déléguer la prévention et la détection de ces ordres, transactions et autres aspects du fonctionnement de la DLT au sein d'un groupe, ou déléguer l'analyse des données et l'émission d'alertes, sous réserve de conditions appropriées. Cette délégation ne devrait pas empêcher les autorités compétentes d'évaluer, à tout moment, si les dispositifs, systèmes et procédures mis en place par le délégataire des fonctions sont effectivement conformes à l'obligation de prévention et de détection des abus de marché. L'obligation de déclaration, ainsi que la responsabilité d'appliquer le présent règlement et l'article 92 du règlement (UE) 2023/1114, continuent d'incomber au délégateur.

(7) Les prestataires de services sur crypto-actifs qui exploitent une plate-forme de négociation devraient avoir des règles de négociation appropriées qui contribuent à la prévention des abus de marché. Ces entités devraient également être dotées de dispositifs permettant de revoir («*replay*») le carnet d'ordres afin d'analyser l'activité de négociation.

Un modèle unique et harmonisé pour la transmission électronique de déclarations de transactions et d'ordres suspects («STOR») devrait faciliter l'échange efficace d'informations sur les ordres et transactions suspects entre les autorités compétentes lors d'enquêtes transfrontières.

(8) Les champs d'information figurant dans ce modèle de STOR, s'ils sont complétés de manière claire, complète, objective et précise, devraient aider les autorités compétentes à évaluer rapidement ces ordres et transactions suspects et à prendre les mesures qui s'imposent. Ce modèle de STOR devrait donc permettre aux personnes qui effectuent la STOR de fournir les informations jugées pertinentes par les autorités compétentes au sujet des ordres et transactions suspects ou autres aspects suspects du fonctionnement de la technologie des registres distribués qu'elles déclarent et d'expliquer les motifs de la suspicion. Le modèle de STOR devrait également permettre aux personnes qui effectuent la STOR de communiquer des données à caractère personnel permettant d'identifier les personnes impliquées dans l'activité suspecte et d'aider les autorités compétentes dans la conduite de leurs enquêtes. Ces informations devraient être fournies dès le départ, afin que l'intégrité de l'enquête ne soit pas compromise par la nécessité éventuelle, pour une autorité compétente, de revenir en cours d'enquête vers la personne qui lui a adressé la STOR. Tout traitement de données à caractère personnel au titre du présent règlement devrait être effectué conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil [2] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le principe de minimisation des données, en particulier, devrait être respecté lorsque des données à caractère personnel sont collectées afin de garantir le respect du présent règlement.

(9) Pour faciliter la transmission d'une STOR, le modèle devrait permettre de joindre les documents et pièces nécessaires pour étayer la notification, y compris sous la forme d'une annexe énumérant les ordres ou transactions suspects et détaillant leur prix et leur volume. En outre, le modèle de STOR devrait permettre de signaler les comportements suspects liés au fonctionnement de la DLT.

(10) Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs ne devraient pas notifier tous les ordres reçus, ou toutes les transactions effectuées, qui ont déclenché une alerte interne. Une telle exigence serait incompatible avec l'obligation d'apprécier au cas par cas s'il existe des motifs raisonnables de suspicion.

(11) L'analyse des ordres, transactions et autres aspects du fonctionnement de la DLT ne devrait pas seulement tenir compte des informations internes de la personne qui organise ou exécute à titre professionnel des transactions portant sur des crypto-actifs, mais de toutes les informations accessibles au public, y compris celles relatives aux transactions intégrées dans un système de registre public.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Les STOR devraient être transmises sans retard à l'autorité compétente dès lors qu'il existe des motifs raisonnables de suspecter l'existence d'un abus de marché. L'analyse visant à déterminer s'il y a lieu de considérer comme suspect un ordre ou une transaction donné devrait s'appuyer sur des faits, et non sur une spéculation ou une présomption, et devrait être effectuée aussi rapidement que possible en pratique. Reporter la soumission d'une notification afin d'y incorporer d'autres ordres ou transactions suspects ou autres aspects suspects du fonctionnement de la DLT ou accumuler plusieurs STOR serait inconciliable avec l'obligation d'agir sans retard, lorsqu'il existe déjà des soupçons raisonnables. En tout état de cause, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs devraient apprécier au cas par cas si plusieurs ordres, transactions ou autres aspects du fonctionnement de la DLT peuvent être notifiés dans une même STOR.

(13) Dans certaines circonstances, des motifs raisonnables de suspecter un abus de marché peuvent apparaître après que l'activité suspecte a eu lieu, en raison d'événements ultérieurs ou d'informations disponibles ultérieurement. Cela ne devrait pas être une raison pour ne pas déclarer l'activité suspecte à l'autorité compétente. Afin de démontrer le respect des exigences déclaratives dans ces circonstances spécifiques, la personne qui effectue la STOR devrait être en mesure de justifier le temps écoulé entre la survenance de l'activité suspecte et la conception des soupçons raisonnables qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis.

(14) Afin d'aider les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs à exercer leur jugement lors de l'examen d'ordres ou de transactions suspects ultérieurs, il convient de leur permettre de reprendre et de réexaminer l'analyse des STOR qui ont été transmises, ainsi que des ordres et transactions suspects et comportements suspects liés au fonctionnement de la DLT qui ont été analysés, mais à propos desquels l'autorité compétente a conclu que les motifs de suspicion n'étaient pas raisonnables.

(15) Afin de prévenir autant que possible les abus de marché, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs devraient être en mesure de perfectionner leurs systèmes de surveillance et de détecter des schémas de comportement répétés, dont l'accumulation, envisagée dans son ensemble, pourrait déboucher sur des soupçons raisonnables d'abus de marché. Ces personnes devraient donc être tenues d'analyser les ordres, transactions, comportements et autres aspects liés au fonctionnement de la technologie des registres distribués qui sont suspects et n'ont pas donné lieu à une STOR, et d'enregistrer ces analyses. Ces dossiers devraient également aider ces personnes à prouver le respect de l'article 92 du règlement (UE) 2023/1114 et devraient faciliter l'exercice, par les autorités compétentes, de leurs fonctions de surveillance, d'enquête et d'application au titre de l'article 92 du règlement (UE) 2023/1114.

(16) Étant donné que les marchés de crypto-actifs sont intrinsèquement transfrontières, il est nécessaire de préciser les procédures de coordination entre les autorités compétentes en vue de la détection et de la répression des abus de marché dans les situations d'abus de marché comportant une dimension transfrontière. Ces procédures de coordination devraient garantir qu'il n'y a pas de conflit entre plusieurs enquêtes ou activités répressives. Dans ce contexte, les situations d'abus de marché comportant une dimension transfrontière devraient comprendre les cas dans lesquels un crypto-actif admis à la négociation dans un État membre fait l'objet de transactions suspectes dans un autre État membre et les cas dans lesquels le prestataire de services sur crypto-actifs concerné exerce ses activités dans plus d'un État membre.

(17) Il est nécessaire de prévoir des dispositions pour la transmission des STOR entre les autorités compétentes. Ces exigences sont essentielles, en l'absence d'un régime de déclaration des transactions, pour garantir l'efficacité de la surveillance du marché et l'application de la législation tout en évitant la transmission d'un flux massif d'informations qui ne seraient pas utiles à l'autorité destinataire.

(18) Le présent règlement se fonde sur le projet de normes techniques de réglementation soumis à la Commission par l'Autorité européenne des marchés financiers (ci-après l'«AEMF»).

(19) L'AEMF a procédé à des consultations publiques ouvertes sur le projet de normes techniques de réglementation sur lequel se fonde le présent règlement, analysé les coûts et avantages potentiels qu'il implique et sollicité l'avis du groupe des parties intéressées au secteur financier institué par l'article 37 du règlement (UE) nº 1095/2010 du Parlement européen et du Conseil ([3]).

([3]) Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([4]) et a rendu son avis le 22 janvier 2025,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Définitions

Aux fins du présent règlement, on entend par:

1) «déclaration de transactions et d'ordres suspects» (STOR — *suspicious transaction and order report*): la déclaration d'ordres ou de transactions suspects, y compris de toute annulation ou modification les concernant, et d'autres aspects du fonctionnement de la DLT lorsque des circonstances pourraient indiquer qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis;

2) «moyens électroniques»: les moyens électroniques de traitement (y compris la compression numérique), de stockage et de transmission de données par câble, ondes radio, technologie optique ou tout autre moyen électromagnétique;

3) «groupe»: un groupe au sens de l'article 2, point 11, de la directive 2013/34/UE du Parlement européen et du Conseil ([5]);

4) «ordre»: tout ordre, y compris toute cotation, que sa finalité soit la soumission initiale, la modification, l'actualisation ou l'annulation d'un ordre, et quel qu'en soit le type.

Article 2

Exigences générales

1. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs établissent et maintiennent des dispositifs, systèmes et procédures qui garantissent:

a) une surveillance effective et constante, aux fins de la prévention, de la détection et de l'identification des ordres et des transactions pour lesquels des circonstances pourraient indiquer qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis, de tous les ordres reçus et transmis et de toutes les transactions sur crypto-actifs exécutées;

b) une surveillance effective et constante des aspects du fonctionnement de la DLT, aux fins de la détection et de l'identification d'autres aspects du fonctionnement de la technologie des registres distribués, y compris le mécanisme de consensus, pour lesquels des circonstances pourraient indiquer qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis;

c) la transmission de STOR aux autorités compétentes conformément aux exigences énoncées dans le présent règlement et suivant le modèle joint en annexe.

([4]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises, modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (JO L 182 du 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

2. Les obligations visées au paragraphe 1 s'appliquent aux ordres, transactions et autres aspects du fonctionnement de la DLT susceptibles de constituer des abus de marché et s'appliquent indépendamment:

a) du titre auquel l'ordre est passé ou la transaction exécutée;

b) des types de clients concernés;

c) du fait que les ordres ont été passés, ou les transactions exécutées, sur ou en dehors d'une plate-forme de négociation.

3. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs veillent à ce que les dispositifs, systèmes et procédures visés au paragraphe 1:

a) soient adaptés et proportionnés à l'échelle, au volume et à la nature de leurs activités;

b) soient régulièrement évalués, au moins dans le cadre d'un audit et d'un réexamen interne annuels, et mis à jour si nécessaire;

c) fassent l'objet d'une documentation écrite claire, indiquant leurs modifications ou mises à jour éventuelles, aux fins du présent règlement, et à ce que les informations figurant dans cette documentation soient conservées pendant une période de cinq ans.

4. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs fournissent à l'autorité compétente, sur demande, les informations relatives à l'évaluation visée au paragraphe 3, y compris des informations sur le niveau d'automatisation mis en place.

Article 3

Prévention, surveillance et détection

1. Les dispositifs, systèmes et procédures visés à l'article 92, paragraphe 1,du règlement (UE) 2023/1114:

a) couvrent toute la gamme des activités de négociation exercées par les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs;

b) émettent des alertes indiquant les activités qui requièrent une analyse plus approfondie aux fins de la détection d'éventuels abus de marché;

c) permettent aux prestataires de services sur crypto-actifs qui exploitent une plate-forme de négociation:

   i) d'effectuer une analyse individuelle et comparative de chaque transaction exécutée, et de chaque ordre passé, modifié, annulé ou rejeté dans les systèmes de la plate-forme de négociation;

   ii) de prévenir l'apparition de comportements répétés observés sur cette même plate-forme de négociation;

d) permettent aux personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs d'effectuer une analyse individuelle et comparative de chaque transaction exécutée et de chaque ordre passé, modifié, annulé ou rejeté dans ou en dehors d'une plate-forme de négociation, que ces ordres et transactions soient ou non passés et exécutés au moyen du registre distribué, et des aspects du fonctionnement de la DLT qui pourraient constituer des abus de marché.

2. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs mettent en place et maintiennent des dispositifs et des procédures qui garantissent un niveau approprié d'analyse humaine dans la prévention, la surveillance, la détection et l'identification des transactions, ordres et autres aspects du fonctionnement de la technologie des registres distribués qui indiquent la probabilité ou l'existence de comportements d'abus de marché. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs ne collectent des données à caractère personnel supplémentaires que dans le seul but de garantir une analyse humaine appropriée.

3. Aux fins de l'article 92, paragraphe 1, du règlement (UE) 2023/1114, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs utilisent, dans une mesure adaptée et proportionnée à l'échelle, au volume et à la nature de leurs activités, des systèmes de TIC.

Les systèmes de TIC visés au premier alinéa comprennent des systèmes informatiques permettant de procéder à une lecture automatique différée, de revoir et d'analyser les données du carnet d'ordres. Ces systèmes disposent d'une capacité suffisante pour opérer dans un environnement de trading algorithmique.

Aux fins du deuxième alinéa, on entend par «trading algorithmique» la négociation de crypto-actifs dans laquelle un algorithme informatique détermine automatiquement les différents paramètres des ordres, notamment la décision de lancer l'ordre, la date et l'heure, le prix ou la quantité de l'ordre, ou la manière de gérer l'ordre après sa soumission, avec une intervention humaine limitée ou sans intervention humaine, ce qui ne comprend pas les systèmes utilisés uniquement pour acheminer des ordres vers une ou plusieurs plates-formes de négociation ou pour le traitement d'ordres n'impliquant la détermination d'aucun paramètre de négociation ou pour la confirmation des ordres ou pour exécuter les ordres de clients ou pour le traitement post-négociation des transactions exécutées.

4. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs peuvent, par un accord écrit, externaliser auprès d'un tiers ou déléguer à une personne morale faisant partie du même groupe, au sens de l'article 2, point 11, de la directive 2013/34/UE du Parlement européen et du Conseil ([6]) (ci-après les «prestataires») les fonctions liées à la prévention, à la surveillance, à la détection et à l'identification des ordres, transactions et autres aspects du fonctionnement de la DLT qui pourraient constituer des abus de marché, dont l'analyse des données, y compris les données des ordres et des transactions, et l'émission des alertes. Les personnes qui délèguent ou externalisent ces fonctions demeurent pleinement responsables du respect de toutes les obligations qui leur incombent en vertu du présent règlement et de l'article 92 du règlement (UE) 2023/1114. Lorsque ces fonctions sont externalisées auprès d'un tiers, les personnes qui procèdent à cette externalisation respectent à tout moment les exigences suivantes:

(a) elles conservent l'expertise et les ressources nécessaires pour:

i) évaluer la qualité des services fournis et l'adéquation organisationnelle des prestataires;

ii) superviser les services externalisés;

iii) gérer en permanence les risques associés à l'externalisation de ces fonctions;

(b) elles disposent d'un accès direct à toutes les informations pertinentes concernant l'analyse de données et l'émission d'alertes.

L'accord écrit visé au premier alinéa décrit les droits et obligations de la personne qui délègue ou externalise les fonctions et ceux du prestataire. Il indique aussi les motifs sur la base desquels la personne déléguant ou externalisant les fonctions peut mettre un terme à cet accord.

5. Dans le cadre des dispositifs, systèmes et procédures visés aux premier et deuxième alinéas, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs conservent pendant une période de cinq ans les informations qui documentent l'analyse des ordres, transactions et aspects du fonctionnement de la DLT susceptibles de constituer des abus de marché. Ces informations comprennent l'analyse effectuée et les raisons de la transmission ou non d'une STOR. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs communiquent ces informations à l'autorité compétente sur demande.

([6]) Directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises, modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (JO L 182 du 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

Article 4

Formation

Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs organisent et dispensent une formation efficace et complète au personnel chargé de la prévention, de la surveillance, de la détection et de l'identification des ordres, transactions et autres aspects du fonctionnement de la DLT qui pourraient indiquer l'existence d'abus de marché, notamment au personnel participant au traitement d'ordres et de transactions ou chargé du fonctionnement de la DLT. Cette formation a lieu régulièrement et est adaptée et proportionnée à l'échelle, au volume et à la nature des activités.

Article 5

Déclaration des ordres ou transactions suspects

1. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs établissent et maintiennent des dispositifs, systèmes et procédures efficaces qui leur permettent d'évaluer, aux fins de la transmission d'une STOR, si, en ce qui concerne un ordre, une transaction ou d'autres aspects de la DLT, des circonstances pourraient indiquer qu'un abus de marché a été commis, est en train d'être commis ou est susceptible d'être commis. Ces dispositifs, systèmes et procédures comportent un niveau approprié d'analyse humaine.

2. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs communiquent une STOR:

(a) en utilisant le modèle de STOR figurant en annexe et en complétant d'une manière claire et précise les champs d'information concernant les ordres, transactions ou autres aspects du fonctionnement de la DLT déclarés, en incluant les éventuels documents justificatifs ou pièces jointes;

(b) en utilisant les moyens électroniques indiqués par cette autorité compétente.

Aux fins du premier alinéa, point b), l'autorité compétente précise sur son site internet les moyens électroniques à utiliser et veille à ce que ces moyens électroniques permettent de préserver le caractère complet, l'intégrité et la confidentialité des informations pendant la transmission.

La STOR visée au premier alinéa se fonde sur des faits et une analyse tenant compte de toutes les informations dont disposent les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs.

3. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs garantissent et maintiennent la confidentialité des informations figurant dans la déclaration d'ordres ou de transactions suspects et veillent à ce que la personne sur laquelle porte la STOR, et toute personne ne devant pas avoir connaissance de la transmission d'une STOR en raison de ses fonctions ou de son poste chez la personne déclarante, ne soient pas informées:

(a) de l'émission des alertes visées à l'article 3, paragraphe 1, point b);

(b) de l'évaluation susceptible de conduire à la transmission d'une STOR;

(c) du fait que la personne déclarante complétera la STOR sans envoyer, à la personne au sujet de laquelle la STOR pourrait être transmise, de demandes d'informations pour remplir certains champs;

(d) de la transmission d'une STOR à l'autorité compétente, ou de l'intention d'en transmettre une.

Article 6

Délai de transmission des STOR

1. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs veillent à mettre en place des dispositifs, systèmes et procédures efficaces permettant de transmettre une STOR sans retard, dès lors qu'il existe des soupçons raisonnables d'abus de marché.

2. Les dispositifs, systèmes et procédures visés au paragraphe 1 comportent la possibilité de transmettre des STOR se rapportant à des transactions, à des ordres ou à d'autres aspects du fonctionnement de la DLT qui sont survenus dans le passé, si les soupçons sont apparus à la lumière d'événements ou d'informations ultérieurs. Dans ce cas, les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs expliquent, dans la STOR, les raisons du délai écoulé entre l'infraction suspectée et la transmission de la STOR, en fonction des circonstances spécifiques du dossier.

3. Les personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs communiquent à l'autorité compétente toutes les informations supplémentaires pertinentes venant à leur connaissance après la transmission de la STOR et lui fournissent toute information ou tout document dont elle fait la demande.

Article 7

Échange de déclarations entre les autorités compétentes

1. Les autorités compétentes transmettent les STOR au moyen du formulaire pour la communication non sollicitée d'informations figurant à l'annexe IV du règlement d'exécution (UE) 2024/2545 de la Commission ([7]).

2. L'autorité compétente à l'origine de la transmission joint la STOR au formulaire visé au paragraphe 1, sans être tenue de le traduire dans la langue de l'autorité compétente destinataire. L'autorité compétente à l'origine de la transmission inclut tout document supplémentaire fourni dans la STOR, en précisant la base juridique de la fourniture des informations.

Article 8

Procédures de coordination en vue de la détection et de la répression des abus de marché comportant une dimension transfrontière

1. Une autorité compétente qui soupçonne un abus de marché d'avoir été commis, d'avoir pu être commis ou d'être en train d'être commis communique, dans les plus brefs délais, aux autres autorités compétentes, y compris, le cas échéant, aux autorités compétentes des plates-formes de négociation sur lesquelles le crypto-actif est admis à la négociation, le statut de son évaluation préliminaire.

Lorsqu'elles sont informées de situations d'abus de marché comportant une dimension transfrontière, les autorités compétentes destinataires partagent, sans délai injustifié, des informations sur la planification ou l'existence de toute activité ou mesure de surveillance ou, le cas échéant et lorsque ces informations sont à leur disposition, sur l'existence d'une enquête pénale relative à la même affaire.

2. Les autorités compétentes concernées:

(a) s'informent périodiquement des situations d'abus de marché comportant une dimension transfrontière;

(b) s'informent mutuellement des développements importants survenus dans l'intervalle concernant des situations d'abus de marché comportant une dimension transfrontière;

(c) coordonnent leurs actions de surveillance et d'application.

([7]) Règlement d'exécution (UE) 2024/2545 de la Commission du 24 septembre 2024 définissant, pour l'application du règlement (UE) 2023/1114 du Parlement européen et du Conseil, des normes techniques d'exécution établissant des formulaires, modèles et procédures normalisés pour la coopération et l'échange d'informations entre les autorités compétentes (JO L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

3. Une autorité compétente qui a formellement lancé une enquête ou une activité répressive ou, le cas échéant, qui a connaissance d'une enquête pénale en informe les autres autorités compétentes concernées, y compris, le cas échéant, les autorités compétentes des plates-formes de négociation sur lesquelles le crypto-actif est admis à la négociation. L'autorité compétente à l'origine de la communication peut informer l'AEMF.

4. Les autorités compétentes qui ont lancé une enquête ou une activité répressive, ou qui y participent, dans le contexte d'une situation comportant une dimension transfrontière peuvent demander une coordination par l'AEMF.

5. Aux fins du présent article, on entend par "situation d'abus de marché comportant une dimension transfrontière" l'une des situations suivantes:

(a) une situation dans laquelle plusieurs autorités sont compétentes pour détecter un cas potentiel d'abus de marché, enquêter à son sujet ou le sanctionner;

(b) une situation dans laquelle une coopération entre deux autorités compétentes ou plus est nécessaire pour détecter un cas potentiel d'abus de marché, enquêter à son sujet ou le sanctionner.

Article 9

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 29 avril 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Modèle de STOR (déclaration de transactions et d'ordres suspects)

*Veuillez noter que **tous** les champs des sections 1 à 4 sont obligatoires. Lorsque des informations ne peuvent pas être fournies pour un champ spécifique, veuillez indiquer «S.O.» et en expliquer brièvement les raisons.*

SECTION 1 — IDENTITÉ DE L'ENTITÉ/DE LA PERSONNE DÉCLARANTE

Personnes qui organisent ou exécutent à titre professionnel des transactions portant sur des crypto-actifs — Préciser, dans chaque cas:

Nom de la personne physique	[Prénom(s) et nom de la personne physique chargée d'effectuer la déclaration au sein de l'entité déclarante.]
Poste dans l'entité déclarante	[Poste occupé par la personne physique chargée d'effectuer la déclaration au sein de l'entité déclarante.]
Nom de l'entité déclarante	[Nom complet de l'entité déclarante, y compris, pour les personnes morales: — la forme juridique prévue dans le registre du pays selon le droit duquel elle est constituée, le cas échéant, et — le code identifiant d'entité légale (code LEI — Legal Entity Identifier), selon la norme ISO 17442.]
Adresse de l'entité déclarante	[Adresse complète (par exemple: rue, numéro, code postal, ville, État/province) et pays.]
Titre auquel l'entité agit à l'égard des ordres, transactions ou comportements liés au fonctionnement de la DLT susceptibles de constituer un abus de marché	[Expliquer à quel titre l'entité déclarante agissait en ce qui concerne les ordres, transactions ou comportements liés au fonctionnement de la technologie des registres distribués qui pourraient indiquer l'existence d'un abus de marché, par exemple: exécution d'ordres pour le compte de clients, exploitation d'une plate-forme de négociation, etc.]
Type d'activité de négociation (tenue de marché, arbitrage, etc.) et type de crypto-actif négocié par l'entité déclarante	[Description des éventuelles dispositions, circonstances ou relations d'entreprise, contractuelles ou organisationnelles.]
Contact pour les demandes d'informations complémentaires	[Personne à contacter dans l'entité déclarante pour les demandes d'informations complémentaires relatives à cette déclaration (par exemple, le responsable de la conformité) et coordonnées de contact utiles, si ce n'est pas la même personne que celle chargée de transmettre la STOR: — prénom(s) et nom de famille, — poste occupé par la personne de contact au sein de l'entité déclarante, — adresse de courrier électronique professionnelle, — numéro de téléphone professionnel.]
Les faits ont-ils déjà été signalés aux autorités publiques?	Veuillez indiquer si les faits ont déjà été signalés aux autorités publiques (et, dans ce cas, indiquer le nom de l'autorité).

SECTION 2 — TRANSACTION/ORDRE/COMPORTEMENT ET AUTRES ASPECTS LIÉS AU FONCTIONNEMENT DE LA TECHNOLOGIE DES REGISTRES DISTRIBUÉS

Description du crypto-actif:	Décrire le ou les crypto-actifs qui font l'objet de la STOR, en précisant: — l'intitulé complet [y compris l'identifiant de jeton numérique (DTI) selon la norme ISO 24165-2 ou un identifiant unique équivalent comme indiqué à l'article 15 du règlement délégué (UE) 2025/1140 de la Commission ([1]) précisant les enregistrements devant être conservés de tous les services, activités, ordres et transactions sur crypto-actifs effectués] ou, en l'absence de DTI, la description du crypto-actif. Lorsque le comportement suspect implique une paire de transactions, veuillez indiquer les deux crypto-actifs de la paire, — le type de crypto-actif [jeton se référant à un ou des actifs (ART), jeton de monnaie électronique (EMT), autre crypto-actif] et, pour les ART et les EMT, la valeur, le droit ou la monnaie officielle (ou la combinaison de ceux-ci) auxquels se réfère le crypto-actif afin de maintenir une valeur stable.
Nom(s) du ou des registres distribués:	[Indiquer le nom complet du ou des registres distribués dans lequel le comportement suspect a été observé.]
Plate-forme de négociation sur laquelle l'ordre a été passé ou la transaction a été exécutée	[Préciser le nom et le code d'identification de marché (MIC) selon la norme ISO 10383 permettant d'identifier la plate-forme de négociation sur laquelle l'ordre a été passé ou la transaction a été exécutée. Lorsque l'ordre ou la transaction n'a pas été identifié(e) sur une plate-forme de négociation, veuillez indiquer «en dehors d'une plate-forme de négociation» ainsi que le LEI du prestataire de services sur crypto-actifs qui a effectué la transaction, le cas échéant.]
Lieu (pays)	[Nom complet du pays et code de pays à deux caractères ISO 3166-1.] [Préciser où: — l'ordre a été donné, — la transaction a été exécutée, — le comportement lié au fonctionnement de la technologie des registres distribués a été observé.]
Description de l'ordre, de la transaction ou du comportement suspect lié au fonctionnement de la DLT	[Décrire au moins les caractéristiques suivantes des ordre(s), transaction(s) ou comportement(s) déclaré(s): — date(s) et heure(s) des ordre(s), transaction(s) ou comportement(s). (Les dates et heures doivent être exprimées en TUC selon le format ISO 8601), — numéro de référence de la transaction ou numéro de référence de l'ordre ou hachage de transaction, — date et heure du règlement, — prix d'achat/prix de vente, — volume/quantité de crypto-actifs, — uniquement pour les ordres, type d'ordre (par exemple, «achat à cours limité à x EUR»)], [Si la suspicion d'abus de marché vise plusieurs ordres ou transactions, les prix et volumes de ces ordres et transactions peuvent être communiqués à l'autorité compétente dans une annexe à la STOR.]

	— informations concernant l'annulation ou la modification de l'ordre, y compris: — la nature de la modification (par exemple, changement de prix ou de quantité) et l'étendue de la modification, [Si la suspicion d'opération d'initié, de manipulation de marché ou de tentative d'opération d'initié ou de manipulation de marché vise plusieurs ordres ou transactions, les prix et volumes de ces ordres et transactions peuvent être communiqués à l'autorité compétente dans une annexe à la STOR.] — le moyen par lequel l'ordre a été modifié (courrier électronique, téléphone, etc.). En cas de déclaration d'un comportement suspect lié au fonctionnement du registre distribué, veuillez fournir le plus de détails possible, y compris l'incidence du comportement sur la validation des transactions et la méthode utilisée pour altérer le fonctionnement de la DLT.
SECTION 3 — DESCRIPTION DE LA NATURE DE LA SUSPICION	
Nature de la suspicion	[Préciser le type d'infraction sur la base de laquelle le ou les ordres, transactions et comportements liés au fonctionnement de la DLT pourraient constituer des abus de marché.]
Motifs de la suspicion	[Décrire l'activité (transactions et ordres, manière de passer les ordres ou d'exécuter les transactions et caractéristiques des ordres et transactions qui les rendent suspects, comportements liés au fonctionnement de la DLT), en indiquant comment l'attention de la personne déclarante a été attirée, et préciser les motifs de suspicion. Pour les crypto-actifs admis à la négociation/négociés sur une plate-forme de négociation, une description de la nature des interactions du carnet d'ordre/transactions qui pourraient constituer un abus de marché.]
SECTION 4 — IDENTIFICATION DE LA OU DES PERSONNES RESPONSABLES DES ORDRES, TRANSACTIONS OU COMPORTEMENTS LIÉS AU FONCTIONNEMENT DE LA TECHNOLOGIE DES REGISTRES DISTRIBUÉS SUSCEPTIBLES DE CONSTITUER UN ABUS DE MARCHÉ («PERSONNE SUSPECTÉE»)	
Nom	[Pour les personnes physiques: prénom(s) et nom de famille.] [Pour les personnes morales: nom complet, y compris la forme juridique prévue dans le registre du pays selon le droit duquel elle est constituée, le cas échéant, et le code identifiant d'entité légale (LEI), selon la norme ISO 17442.]
Numéro national d'identification	[Numéro et/ou texte.] [Lorsque le numéro national d'identification n'est pas applicable ou connu, indiquer la date de naissance (uniquement pour les personnes physiques) au format ISO 8601.]
Adresse	[Adresse complète (par exemple: rue, numéro, code postal, ville, État/province) et pays.]
Informations concernant la situation professionnelle: — Lieu — poste	[Informations concernant la situation professionnelle de la personne suspectée, provenant de sources d'information internes de l'entité déclarante (par exemple, documentation relative au compte dans le cas de clients, système d'information sur le personnel dans le cas d'un salarié de l'entité déclarante).]
Numéro(s) de compte et adresse(s) de portefeuille	[Numéros des comptes de dépôt, des éventuels comptes communs ou des procurations établies sur les comptes que détient l'entité/la personne suspectée. Adresse(s) de portefeuille concernée(s) par la transaction ou le comportement suspect.]
Identifiant du client	[Si la personne suspectée est un client de l'entité déclarante.]
Relation avec l'émetteur du crypto-actif concerné	[Description des éventuelles dispositions, circonstances ou relations d'entreprise, contractuelles ou organisationnelles.]

SECTION 5 — INFORMATIONS SUPPLÉMENTAIRES

Autres informations pertinentes pour la déclaration, en fonction de l'activité

[La liste suivante est indicative et non exhaustive. D'autres informations jugées utiles par la personne déclarante peuvent être fournies, lorsqu'elles sont pertinentes pour la STOR.]

— Situation de la personne suspectée (par exemple, client de détail, institution).
— Nature de l'intervention de l'entité/la personne suspectée (pour compte propre, pour le compte d'un client, validateur de transactions dans un système de registres distribués, autre).
— Lorsque le comportement suspect est commis dans une DLT, les autres informations pertinentes peuvent comprendre:
  — une mention indiquant si la transaction a transité par une file d'attente publique ou privée (cryptée) de transactions (c'est-à-dire le «mempool») avant d'être validée dans la DLT,
  — une mention indiquant si la DLT est publique (non soumise à permission) ou privée (soumise à permission),
  — les interactions potentielles avec les contrats intelligents, y compris la spécification de l'adresse du contrat et de la fonction appelée.
— La taille du portefeuille de l'entité/la personne suspectée.
— La date à laquelle la relation d'affaires avec le client a commencé, si l'entité/la personne suspectée est un client de la personne/l'entité déclarante.
— Le type d'activités de la salle des marchés de l'entité suspectée, si disponible.
— Les schémas de comportement de négociation de l'entité/la personne suspectée. À titre indicatif, les exemples d'informations qui suivent peuvent être utiles:
  — les habitudes de comportement de négociation de l'entité/la personne suspectée,
  — la comparabilité de la taille de l'ordre ou de la transaction déclaré(e) avec la taille moyenne des ordres soumis ou des transactions exécutées par l'entité/la personne suspectée au cours des 12 derniers mois,
  — les habitudes de l'entité/la personne suspectée en ce qui concerne les crypto-actifs qu'elle a négociés au cours des 12 derniers mois, notamment le fait que l'ordre/la transaction déclaré(e) se rapporte ou non à un crypto-actif qu'elle a négocié au cours de l'année écoulée.
— Les autres entités/personnes dont on sait qu'elles ont été impliquées dans la négociation des ordres ou transactions qui pourraient constituer des abus de marché:
  — nom.
— Activité (par exemple, exécution d'ordres pour le compte de clients, négociation pour compte propre, exploitation d'une plate-forme de négociation, validation des transactions).

SECTION 6 — DOCUMENTATION JOINTE

[Liste des pièces et documents justificatifs joints à la présente déclaration.]

[Cette documentation peut consister, par exemple, en courriers électroniques, enregistrements de conversations, enregistrements d'ordres/de transactions, enregistrements de DLT, confirmations, rapports de courtiers, procurations et commentaires des médias, le cas échéant.

Lorsque les informations détaillées concernant les ordres/transactions/comportements liés au fonctionnement de la technologie des registres distribués visées à la section 2 sont jointes dans une annexe séparée, indiquer l'intitulé de cette annexe.]

([1]) Règlement délégué (UE) 2025/1140 de la Commission du 27 février 2025 complétant le règlement (UE) 2023/1114 du Parlement européen et du Conseil par des normes techniques de réglementation qui précisent les enregistrements devant être conservés de tous les services, activités, ordres et transactions sur crypto-actifs effectués (JO L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).