RÈGLEMENT DÉLÉGUÉ (UE) 2017/571 DE LA COMMISSION

du 2 juin 2016

complétant la directive 2014/65/UE du Parlement européen et du Conseil par des normes techniques de réglementation sur l'agrément, les exigences organisationnelles et la publication des transactions pour les prestataires de services de communication de données

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

LA COMMISSION EUROPÉENNE,

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

vu la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE [1], et notamment son article 61, paragraphe 4, son article 64, paragraphes 6 et 8, son article 65, paragraphes 6 et 8, et son article 66, paragraphe 5,

considérant ce qui suit:

(1) Conformément à la directive 2014/65/UE, les prestataires de services de communication de données correspondent à trois types d'entités: les mécanismes de déclaration agréés (ARM), les dispositifs de publication agréés (APA) et les fournisseurs de système consolidé de publication (CTP). Bien que ces différents types d'entités n'exercent par les mêmes activités, la procédure d'agrément prévue par la directive 2014/65/UE pour chacun d'entre eux est similaire.

(2) Une entité qui demande à être agréée en tant que prestataire de services de communication de données devrait fournir dans sa demande d'agrément un programme d'activité et un organigramme. Cet organigramme devrait identifier les personnes responsables des différentes activités pour permettre à l'autorité compétente de déterminer si le prestataire de services de communication de données dispose de ressources humaines et de capacités de supervision des activités suffisantes. L'organigramme devrait couvrir non seulement toute l'étendue des services de communication de données, mais également tous les autres services que l'entité fournit, afin de mettre en évidence les éventuels domaines dans lesquels l'indépendance du prestataire de services de communication de données pourrait être compromise et où un conflit d'intérêts pourrait apparaître. Une entité qui demande à être agréée en tant que prestataire de services de communication de données devrait également fournir des informations sur la composition, le fonctionnement et l'indépendance de ses organes de direction, afin que les autorités compétentes soient en mesure d'évaluer si les politiques, les procédures et la structure de la gouvernance d'entreprise du prestataire de services de communication de données garantissent son indépendance et permettent d'éviter les conflits d'intérêts.

(3) Il peut y avoir des conflits d'intérêts entre un prestataire de services de communication de données et les clients qui recourent à ses services pour satisfaire à leurs obligations réglementaires et d'autres entités qui achètent des données à de tels prestataires. Ces conflits peuvent notamment exister lorsque le prestataire de services de communication de données exerce d'autres activités, par exemple d'opérateur de marché, d'entreprise d'investissement ou de référentiel central. Si ces conflits ne sont pas réglés, cela peut créer une situation dans laquelle le prestataire de services de communication de données est incité à retarder la publication ou la communication de données ou à effectuer des transactions en se fondant sur des informations confidentielles qu'il a reçues. Le prestataire de services de communication de données devrait donc adopter une approche globale pour identifier, prévenir et gérer les conflits d'intérêts existants et potentiels, et notamment en faire l'inventaire et mettre en œuvre des politiques et procédures appropriées pour les gérer et, au besoin, pour séparer les fonctions opérationnelles et les membres du personnel afin de limiter la circulation des informations sensibles entre ses différents secteurs d'activité.

(4) Tous les membres de l'organe de direction d'un prestataire de services de communication de données devraient être des personnes jouissant d'une honorabilité suffisante et possédant les connaissances, les compétences et l'expérience nécessaires, car ils jouent un rôle clé, qui est de veiller à ce que ce prestataire respecte ses obligations réglementaires et de contribuer à sa stratégie d'entreprise. Il importe donc que le prestataire de services de communication de données montre qu'il a mis en place un solide processus de nomination des membres de son organe de direction et d'évaluation de leur performance, ainsi que des lignes hiérarchiques claires et l'obligation de faire régulièrement rapport à l'organe de direction.

[1] JO L 173 du 12.6.2014, p. 349.

(5) L'externalisation d'activités, en particulier de fonctions critiques, peut modifier de façon sensible les conditions d'agrément d'un prestataire de services de communication de données. Pour garantir que l'externalisation d'activités ne compromet pas la capacité du prestataire de services de communication de données à remplir ses obligations au titre de la directive 2014/65/UE ou n'entraîne pas de conflits d'intérêt, ce prestataire devrait être en mesure de démontrer qu'il exerce une supervision et un contrôle suffisants sur lesdites activités.

(6) Les systèmes informatiques utilisés par les prestataires de services de communication de données devraient être adaptés aux différents types d'activités que ces entités peuvent exercer, à savoir publier des rapports de négociation, déposer des déclarations de transactions ou fournir un système consolidé de publication. Ils devraient également être suffisamment solides pour garantir la continuité et la régularité de la fourniture de ces services, et notamment être capables de faire face aux fluctuations du volume de données à traiter. Ces fluctuations, en particulier les augmentations inattendues des flux de données, peuvent altérer l'efficacité des systèmes du prestataire de services de communication de données, et partant, sa capacité à publier ou communiquer des informations exactes et complètes dans les délais requis. Pour y remédier, un prestataire de services de communication de données devrait tester périodiquement ses systèmes pour s'assurer qu'ils sont suffisamment robustes pour faire face aux variations des conditions d'exploitation et suffisamment modulables.

(7) Les mécanismes et dispositifs de sauvegarde mis en place par un prestataire de services de communication de données devraient être suffisants pour lui permettre de fournir ses services même en cas d'incident perturbateur. Un prestataire de services de communication de données devrait définir des délais maximaux acceptables pour le rétablissement de ses fonctions critiques après un incident perturbateur, de manière à permettre le respect des délais de communication et de publication des informations.

(8) Afin d'être certain de pouvoir fournir ses services, le prestataire de services de communication de données devrait examiner quelles tâches et activités sont indispensables à leur prestation et analyser les scénarios susceptibles de donner lieu à un incident perturbateur, et prendre des mesures pour prévenir ces situations ou y remédier.

(9) En cas de perturbation de ses services, le prestataire de services de communication de données devrait en aviser l'autorité compétente de son État membre d'origine, toute autre autorité compétente concernée, ses clients et le public, dans la mesure où ces parties pourraient, du fait de cette perturbation, ne pas être en mesure de satisfaire à leurs propres obligations réglementaires, telles que l'obligation de transmettre des déclarations de transactions à d'autres autorités compétentes ou de rendre public le détail des transactions exécutées. Cette notification devrait permettre à ces parties de prendre d'autres dispositions pour remplir leurs obligations.

(10) Les mises à jour des systèmes informatiques sont susceptibles d'altérer l'efficacité et la solidité des systèmes utilisés pour la prestation de services de données. Afin d'éviter à tout moment que le fonctionnement de son système informatique soit incompatible avec ses obligations réglementaires, notamment avec l'obligation de disposer d'un mécanisme de sécurité solide permettant de garantir la sécurité des moyens de transfert de l'information, de réduire au minimum le risque de corruption des données et d'empêcher les fuites d'informations avant leur publication, un prestataire de services de communication de données devrait employer des méthodes de développement et de test clairement définies pour garantir que les contrôles de conformité et de gestion des risques intégrés dans le système fonctionnent comme prévu et que le système peut continuer à fonctionner efficacement dans toutes les circonstances. Lorsqu'un prestataire de services de communication de données entreprend de modifier sensiblement son système, il devrait en informer l'autorité compétente de son État membre d'origine et les autres autorités compétentes, le cas échéant, afin qu'elles puissent évaluer si la mise à jour aura des répercussions sur leurs propres systèmes et si les conditions d'agrément sont toujours remplies.

(11) La divulgation prématurée au public dans le cas des rapports de négociation, ou la divulgation non autorisée dans le cas des déclarations de transactions, est susceptible de fournir des indications sur la stratégie de négociation ou de révéler des informations sensibles telles que l'identité des clients du prestataire de services de communication de données. Celui-ci devrait donc mettre en place des moyens de contrôle physiques, tels que le verrouillage des installations, et des moyens de contrôle électroniques, notamment des pare-feu et des mots de passe, afin que seules les personnes autorisées puissent avoir accès aux données.

(12) Les failles dans les systèmes physiques ou électroniques de sécurité d'un prestataire de services de communication de données sont une menace pour la confidentialité des données des clients. Par conséquent, lorsqu'une telle faille apparaît, il convient que le prestataire de services de communication de données en avise dans les meilleurs délais

l'autorité compétente concernée ainsi que les clients touchés par la faille. Il est nécessaire que l'autorité compétente de l'État membre d'origine en soit informée afin qu'elle puisse exercer ses responsabilités en matière de surveillance en ce qui concerne le respect par le prestataire de services de communication de données de son obligation de disposer de mécanismes de sécurité solides pour garantir la sécurité des informations, et réduire au minimum le risque de corruption des données et d'accès non autorisé. Les autres autorités compétentes qui disposent d'une interface technique avec le prestataire de services de communication de données devraient aussi être avisées de la faille, puisque celle-ci est susceptible d'avoir pour elles des conséquences négatives, notamment lorsqu'elle concerne les moyens de transfert des informations entre le prestataire et elles.

(13) Une entreprise d'investissement soumise à des obligations de déclaration des transactions, dite «entreprise déclarante», peut choisir d'avoir recours à un tiers, dit «entreprise déposante», pour déposer en son nom des déclarations de transactions auprès d'un ARM. En tant qu'entreprise déposante, ce tiers aura accès aux informations confidentielles qu'il sera chargé de transmettre. Toutefois, il ne devrait pas avoir le droit d'accéder aux autres données sur l'entreprise déclarante, ou sur les transactions de cette dernière, qui sont conservées par l'ARM. De telles données peuvent correspondre à des déclarations de transactions que l'entreprise déclarante a elle-même déposées auprès de l'ARM ou qu'elle a envoyées à une autre entreprise déposante pour que celle-ci les envoie à l'ARM. L'entreprise déposante ne devrait pas avoir accès à ces données, celles-ci étant susceptibles de contenir des informations confidentielles, telles que l'identité des clients de l'entreprise déclarante.

(14) Un prestataire de services de communication de données devrait vérifier que les données qu'il publie ou qu'il dépose sont exactes et complètes et veiller à disposer de mécanismes qui lui permettent de détecter les erreurs ou omissions que le client ou lui-même ont commises. Dans le cas d'un ARM, il peut s'agir de vérifier la concordance entre un échantillon des données soumises à l'ARM par une entreprise d'investissement ou générées par l'ARM pour le compte de cette entreprise d'investissement et les données correspondantes fournies par l'autorité compétente. La fréquence et l'étendue de ces vérifications de concordance devraient être proportionnelles au volume de données traitées par l'ARM et à son activité de production de rapports de transactions à partir des données des clients ou de transmission des rapports de transactions remplis par les clients. Afin que les déclarations respectent les délais et soient exemptes d'erreurs et omissions, un ARM devrait constamment surveiller le fonctionnement de ses systèmes.

(15) Lorsqu'un ARM est lui-même à l'origine d'une erreur ou d'une omission, il devrait corriger sans délai l'information concernée et avertir de cette erreur ou omission l'autorité compétente de son État membre d'origine et toute autorité compétente à laquelle il soumet des déclarations, ces autorités compétentes étant concernées par la qualité des données qui leur sont soumises. L'ARM devrait également avertir son client de l'erreur ou de l'omission et lui fournir des informations actualisées afin qu'il puisse aligner ses registres internes sur les informations que l'ARM a soumises pour son compte à l'autorité compétente.

(16) Les APA et les CTP devraient pouvoir supprimer ou modifier les informations reçues d'une entité déclarante afin de remédier aux situations dans lesquelles, dans des circonstances exceptionnelles, cette dernière rencontre des difficultés techniques l'empêchant de supprimer ou modifier elle-même ces informations. Cependant, en dehors de ces situations, les APA et les CTP ne devraient pas être chargés de la correction des informations contenues dans les rapports publiés si l'erreur ou l'omission est attribuable à l'entité qui fournit les informations. En effet, les APA et les CTP ne peuvent pas savoir avec certitude si une erreur ou omission apparente est avérée, puisqu'ils n'étaient pas partie à la transaction exécutée.

(17) Pour favoriser une communication fiable entre un APA et l'entreprise d'investissement qui déclare une transaction, notamment en ce qui concerne les annulations et modifications de transactions, l'APA devrait inclure dans les messages de confirmation envoyés aux entreprises d'investissement le code d'identification qu'il a attribué à la transaction lors de la publication de l'information.

(18) Pour se conformer à son obligation de déclaration en vertu du règlement (UE) nº 600/2014 du Parlement européen et du Conseil ([1]), un ARM devrait veiller à la fluidité de circulation des informations entre l'autorité compétente et lui, notamment du point de vue des capacités de transfert de rapports et de traitement des rapports rejetés. L'ARM devrait donc être en mesure de démontrer sa capacité à respecter les spécifications techniques définies par l'autorité compétente en ce qui concerne leur interface commune.

([1]) Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84).

(19) Un prestataire de services de communication de données devrait également veiller à conserver pendant une période suffisamment longue les informations relatives aux déclarations de transaction et aux rapports de négociation qu'il traite, afin de faciliter la recherche d'informations historiques par les autorités compétentes. Dans le cas spécifique des APA et des CTP, ces derniers devraient veiller à prendre les dispositions organisationnelles nécessaires pour conserver les données au minimum pendant la période fixée par le règlement (UE) nº 600/2014 et être en mesure de répondre à toute demande de prestation de services régie par le présent règlement.

(20) Le présent règlement définit un certain nombre de services supplémentaires qu'un CTP pourrait fournir et qui augmentent l'efficience du marché. Compte tenu de l'évolution possible des marchés, il n'est pas opportun de fournir une liste exhaustive de ces services. Un CTP devrait donc pouvoir fournir d'autres services supplémentaires que ceux explicitement énumérés dans le présent règlement, à condition toutefois que ces autres services ne compromettent pas son indépendance ou la qualité du système consolidé de publication.

(21) Afin d'assurer une bonne diffusion des informations rendues publiques par les APA et les CTP et de faciliter l'accès à ces informations et leur utilisation par les acteurs du marché, elles devraient être publiées dans un format lisible par machine à travers des canaux solides permettant l'accès automatique aux données. Si les sites web n'ont pas toujours une architecture suffisamment robuste et modulable qui permette un accès automatisé aisé aux données, ces contraintes technologiques pourraient être surmontées à l'avenir. Il ne s'agit donc pas de prescrire une technologie particulière, mais de définir des critères que la technologie à utiliser doit remplir.

(22) En ce qui concerne les actions et les instruments assimilables à des actions, le règlement (UE) nº 600/2014 n'exclut pas que les entreprises d'investissement rendent leurs transactions publiques au moyen de plusieurs APA. Toutefois, il convient qu'un mécanisme spécifique soit mis en place afin de permettre aux parties intéressées qui consolident les informations de négociation provenant de plusieurs APA, et notamment aux CTP, de repérer les éventuels doublons, afin d'éviter que la même transaction soit consolidée plusieurs fois et publiée à plusieurs reprises par les CTP. Cela nuirait à la qualité et à l'utilité du système consolidé de publication.

(23) Les APA devraient donc publier les transactions déclarées par les entreprises d'investissement en prévoyant un champ «réédition» permettant de signaler les déclarations qui sont des doubles. Afin de permettre une approche neutre du point de vue de la technologie utilisée, il est nécessaire de prévoir différentes manières possibles pour un APA de repérer les doublons.

(24) Afin de garantir que chaque transaction n'est introduite qu'une seule fois dans le système consolidé de publication et d'accroître ainsi la fiabilité des informations fournies, les CTP ne devraient pas publier les informations relatives à une transaction publiée par un APA qui constitue un double.

(25) Les APA devraient publier des informations sur les transactions, y compris les horodatages pertinents, par exemple le moment où elles ont été exécutées et le moment où elles ont été déclarées. En outre, la granularité de l'horodatage devrait refléter la nature du système de négociation sur lequel la transaction a été exécutée. La granularité devrait être plus fine lorsque les informations concernent des transactions exécutées sur des systèmes électroniques que lorsqu'elles concernent des transactions exécutées sur des systèmes non électroniques.

(26) Les CTP peuvent publier des informations sur des actions ou instruments assimilés et sur d'autres types d'instruments. Étant donné les différentes exigences applicables à l'exploitation de ces systèmes consolidés de publication, notamment l'éventail nettement plus large d'instruments financiers couverts qui ne sont pas des actions ou des instruments assimilés, et l'application différée des dispositions de la directive 2014/65/UE en ce qui concerne les CTP pour ces instruments, le présent règlement précise seulement l'étendue des informations à consolider par les CTP pour les actions et instruments assimilés.

(27) Les dispositions du présent règlement sont étroitement liées entre elles, puisqu'elles concernent l'agrément, les exigences organisationnelles et la publication des transactions pour les prestataires de services de communication de données. Pour assurer la cohérence de ces différentes dispositions, qui doivent entrer en vigueur en même temps, et pour que les parties prenantes, et en particulier celles soumises à ces obligations, en aient d'emblée une vision globale, il est nécessaire de regrouper ces normes techniques de réglementation dans un règlement unique.

(28) Le présent règlement définit les exigences de publication de données applicables aux APA et aux CTP. Afin d'assurer la cohérence des pratiques de publication d'informations de négociation entre les plates-formes de négociation, les APA et les CTP et de faciliter la consolidation des données par les CTP, le présent règlement devrait s'appliquer en conjonction avec les règlements délégués de la Commission (UE) 2017/587 ([1]) et (UE) 2017/583 ([2]) qui définissent des exigences concernant la publication d'informations de négociation.

(29) Dans un souci de cohérence et afin de garantir le bon fonctionnement des marchés financiers, il convient que les dispositions du présent règlement et les dispositions nationales correspondantes transposant la directive 2014/65/UE s'appliquent à compter de la même date. Étant donné que l'article 65, paragraphe 2, de la directive 2014/65/UE s'applique à partir du 3 septembre de l'année suivant celle d'entrée en vigueur du présent règlement, certaines dispositions du présent règlement devraient elles aussi s'appliquer à partir de cette date plus tardive.

(30) Le présent règlement se fonde sur les projets de normes techniques de réglementation soumis à la Commission par l'Autorité européenne des marchés financiers (AEMF).

(31) L'AEMF a procédé à des consultations publiques ouvertes sur les projets de normes techniques de réglementation sur lesquels se fonde le présent règlement, analysé les coûts et avantages potentiels qu'ils impliquent 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]),

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

AGRÉMENT

(Article 61, paragraphe 2, de la directive 2014/65/UE)

Article premier

Communication d'informations aux autorités compétentes

1. Un demandeur sollicitant un agrément pour la prestation de services de communication de données communique à l'autorité compétente les informations visées aux articles 2, 3 et 4 ainsi que les informations concernant toutes les exigences organisationnelles définies aux chapitres II et III.

2. Un prestataire de services de communication de données informe sans délai l'autorité compétente de son État membre d'origine de toute modification importante des informations fournies au moment de l'agrément et ultérieurement.

Article 2

Informations sur l'organisation

1. Un demandeur sollicitant un agrément pour la prestation de services de communication de données inclut dans sa demande d'agrément un programme d'activité tel que visé à l'article 61, paragraphe 2, de la directive 2014/65/UE. Le programme d'activité contient les informations suivantes:

a) des informations sur la structure organisationnelle du demandeur, y compris un organigramme et une description des ressources humaines, techniques et juridiques affectées à ses activités opérationnelles;

([1]) Règlement délégué (UE) 2017/587 de la Commission du 14 juillet 2016 complétant le règlement (UE) nº 600/2014 du Parlement européen et du Conseil concernant les marchés d'instruments financiers par des normes techniques de réglementation relatives aux obligations de transparence applicables aux plates-formes de négociation et aux entreprises d'investissement pour les actions, certificats représentatifs, fonds cotés, certificats préférentiels et instruments financiers analogues, et aux obligations d'exécution des transactions sur certaines actions via une plate-forme de négociation ou par un internalisateur systématique (voir page 387 du présent Journal officiel).

([2]) Règlement délégué (UE) 2017/583 de la Commission du 14 juillet 2016 complétant le règlement (UE) nº 600/2014 du Parlement européen et du Conseil concernant les marchés d'instruments financiers par des normes techniques de réglementation relatives aux obligations de transparence applicables aux plates-formes de négociation et aux entreprises d'investissement pour les obligations, produits financiers structurés, quotas d'émission et instruments dérivés (voir page 229 du présent Journal officiel).

([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).

b) des informations sur les politiques et procédures de conformité mises en place par le prestataire de services de communication de données, y compris:

i) le nom de la personne ou des personnes chargées de l'approbation et de l'actualisation de ces politiques;

ii) les dispositifs visant à surveiller et faire appliquer les politiques et procédures en matière de conformité;

iii) les mesures à prendre en cas de faille susceptible d'aboutir à un non-respect des conditions de l'agrément initial;

iv) une description de la procédure de déclaration à l'autorité compétente de toute faille susceptible d'aboutir à un non-respect des conditions de l'agrément initial;

c) une liste de toutes les fonctions externalisées et de toutes les ressources affectées à leur contrôle.

2. Un prestataire de services de communication de données qui offre des services autres que des services de communication de données décrit ces services dans l'organigramme.

Article 3

Gouvernance d'entreprise

1. Un demandeur sollicitant un agrément pour la prestation de services de communication de données inclut dans sa demande d'agrément des informations sur ses politiques internes de gouvernance d'entreprise et sur les procédures qui régissent son organe de direction, sa direction générale, et, s'il en a institué, ses comités.

2. Les informations visées au paragraphe 1 comprennent:

a) une description des processus de sélection, de nomination, d'évaluation de la performance et de révocation de la direction générale et des membres de l'organe de direction;

b) une description des lignes hiérarchiques et l'indication de la fréquence de communication de rapports à la direction générale et à l'organe de direction;

c) une description des politiques et procédures d'accès des membres de l'organe de direction aux documents.

Article 4

Informations sur les membres de l'organe de direction

1. Un demandeur sollicitant un agrément pour la prestation de services de communication de données inclut dans sa demande d'agrément les informations suivantes concernant chacun des membres de l'organe de direction:

a) le nom, la date et le lieu de naissance, le numéro d'identification national ou un équivalent, l'adresse et les coordonnées;

b) la fonction à laquelle le membre est ou sera nommé;

c) un curriculum vitæ attestant qu'il possède une expérience et des connaissances suffisantes pour exercer correctement ses responsabilités;

d) le casier judiciaire, présenté au moyen d'un certificat officiel, ou, lorsqu'un tel document n'est pas disponible dans l'État membre concerné, une déclaration solennelle d'honorabilité incluant l'autorisation, pour l'autorité compétente, de vérifier si le membre en question a déjà été reconnu coupable d'une infraction pénale en rapport avec la prestation de services financiers ou de services de données ou en rapport avec une fraude ou un détournement;

e) dans tous les cas, une déclaration solennelle d'honorabilité incluant l'autorisation, pour l'autorité compétente, de vérifier si le membre en question:

i) a déjà fait l'objet d'une décision lui faisant grief à la suite d'une procédure disciplinaire engagée par une autorité réglementaire ou une administration publique, ou si une telle procédure est actuellement en cours à son égard;

ii) a déjà fait l'objet d'une décision lui faisant grief dans une procédure civile devant un tribunal, portant sur la prestation de services financiers ou de services de données ou sur une faute ou une fraude commises dans la gestion d'une entreprise;

iii) a fait partie de l'organe de direction d'une entreprise qui a fait l'objet d'une décision lui faisant grief ou d'une sanction infligée par une autorité réglementaire ou dont l'enregistrement ou l'agrément a été retiré par une autorité réglementaire;

iv) s'est vu refuser le droit d'exercer des activités soumises à une obligation d'enregistrement ou d'agrément par une autorité réglementaire;

v) a fait partie de l'organe de direction d'une entreprise qui a fait faillite ou a été placée en liquidation alors qu'il était en fonction ou dans un délai d'un an après qu'il a cessé d'être en fonction;

vi) s'est vu infliger par un organisme professionnel une amende, une mesure de suspension ou de révocation ou toute autre sanction en rapport avec une fraude ou un détournement ou avec la prestation de services financiers ou de services de données;

vii) a déjà été révoqué comme administrateur, déchu du droit d'exercer des fonctions de direction ou de gestion ou licencié d'un poste de salarié ou d'un autre poste occupé dans une entreprise pour inconduite ou abus;

f) une indication du temps minimal qu'il doit consacrer à l'exercice de ses fonctions au sein du prestataire de services de communication de données;

g) une déclaration des éventuels conflits d'intérêts pouvant exister ou naître du fait de l'exercice de ses fonctions, et de la manière dont ces conflits sont gérés.

CHAPITRE II

EXIGENCES ORGANISATIONNELLES

(Article 64, paragraphes 3, 4 et 5, article 65, paragraphes 4, 5 et 6, et article 66, paragraphes 2, 3 et 4, de la directive 2014/65/UE)

Article 5

Conflits d'intérêt

1. Un prestataire de services de communication de données met en œuvre et maintient des dispositifs administratifs efficaces destinés à prévenir les conflits d'intérêts avec les clients qui utilisent ses services pour satisfaire à leurs obligations réglementaires et d'autres entités qui achètent des données auprès de prestataires de services de communication de données. Ces dispositifs comprennent des politiques et procédures pour l'identification, la gestion et la divulgation des conflits d'intérêts existants et potentiels, et comportent:

a) un inventaire des conflits d'intérêts existants et potentiels, présentant leur description, identification, prévention, gestion et divulgation;

b) la séparation des tâches et des fonctions opérationnelles au sein du prestataire de services de communication de données, y compris:

i) les mesures destinées à empêcher ou contrôler l'échange d'informations lorsqu'un risque de conflits d'intérêts est susceptible d'apparaître;

ii) une surveillance distincte des personnes pertinentes dont les principales fonctions comportent des intérêts susceptibles d'être en conflit avec ceux d'un client;

c) une description de la politique tarifaire appliquée pour déterminer les frais facturés par le prestataire de services de communication de données et les entreprises auxquelles il est étroitement lié;

d) une description de la politique de rémunération applicable aux membres de l'organe de direction et de la direction générale;

e) les règles concernant l'acceptation de sommes d'argent, de cadeaux ou de faveurs par le personnel du prestataire de services de communication de données et son organe de direction.

2. L'inventaire des conflits d'intérêts visé au paragraphe 1, point a), inclut les conflits d'intérêts créés par les situations dans lesquelles le prestataire de services de communication de données:

a) peut, au détriment du client, réaliser un gain financier ou éviter une perte financière;

b) peut avoir un intérêt dans le résultat d'un service fourni à un client qui ne coïncide pas avec l'intérêt de ce client dans ce résultat;

c) peut être incité à privilégier ses propres intérêts, ou ceux d'un autre client ou groupe de clients, au détriment de ceux du client à qui le service est fourni;

d) reçoit ou est susceptible de recevoir de la part d'une personne autre que le client, en rapport avec le service fourni à ce dernier, une incitation, sous forme d'argent, de biens ou de services, autre que la commission ou les frais perçus pour le service en question.

Article 6

Exigences organisationnelles en matière d'externalisation

1. Lorsqu'un prestataire de services de communication de données confie des activités à des tiers pour qu'ils les exercent pour son compte, y compris des entreprises avec lesquelles il a des liens étroits, il veille à ce que le prestataire de service tiers ait l'aptitude et la capacité d'exercer ces activités de manière fiable et professionnelle.

2. Un prestataire de services de communication de données précise quelles activités seront externalisées, ainsi que les ressources humaines et techniques nécessaires à l'exercice de chacune de ces activités.

3. Un prestataire de services de communication de données qui externalise des activités veille à ce que cette externalisation ne diminue pas son aptitude à exercer ou son pouvoir d'exercer des fonctions de direction générale ou d'organe de direction.

4. Un prestataire de services de communication de données conserve la responsabilité de toutes les activités externalisées et adopte des mesures organisationnelles garantissant:

a) qu'il évalue si le prestataire de services tiers exerce les activités externalisées de manière efficace et conforme aux dispositions législatives et aux exigences réglementaires applicables et remédie de manière adéquate aux défaillances constatées;

b) l'identification des risques relatifs aux activités externalisées et un suivi périodique adéquat;

c) des procédures de contrôle adéquates des activités externalisées, incluant une surveillance effective des activités et de leurs risques au sein du prestataire de services de communication de données;

d) une continuité suffisante des activités externalisées.

Aux fins du point d), le prestataire de services de communication de données obtient des informations sur les mécanismes de continuité des activités du prestataire de services tiers, en évalue la qualité et, au besoin, en demande l'amélioration.

5. Un prestataire de services de communication de données veille à ce que le prestataire de services tiers coopère avec l'autorité compétente du prestataire de services de communication de données en ce qui concerne les activités externalisées.

6. Lorsqu'un prestataire de services de communication de données externalise des fonctions critiques, il communique à l'autorité compétente de son État membre d'origine:

a) l'identité du prestataire de services tiers;

b) les mesures et politiques organisationnelles régissant l'externalisation et les risques qu'elle pose définies au paragraphe 4;

c) des rapports internes ou externes sur les activités externalisées.

Aux fins du premier alinéa du paragraphe 6, une fonction est considérée comme critique lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement à la capacité du prestataire de services de communication de données de se conformer en permanence aux conditions et aux obligations de son agrément ou à ses autres obligations au titre de la directive 2014/65/UE.

Article 7

Mécanismes de continuité des activités et de sauvegarde

1. Un prestataire de services de communication de données utilise des systèmes et des mécanismes appropriés et suffisamment solides pour garantir la continuité et la régularité des services visés dans la directive 2014/65/UE.

2. Un prestataire de services de communication de données procède à des examens périodiques, au moins une fois par an, pour évaluer ses infrastructures techniques et ses politiques et procédures connexes, y compris ses mécanismes de continuité des activités. Il remédie à toute insuffisance constatée pendant l'examen.

3. Un prestataire de services de communication de données a mis en place des mécanismes de continuité des activités efficaces pour faire face à des incidents perturbateurs, notamment:

a) les processus indispensables à la fourniture de ses services, y compris des procédures d'intervention par paliers, l'externalisation d'activités pertinentes ou le recours à des prestataires externes;

b) des mécanismes de continuité spécifiques, couvrant un éventail adéquat de scénarios possibles, à court et moyen termes, y compris de défaillances des systèmes, de catastrophe naturelle, de rupture de communication, de perte de collaborateurs clés et d'impossibilité d'utiliser les locaux normalement utilisés;

c) la duplication des composants du matériel informatique, pour permettre de basculer vers une infrastructure de sauvegarde, tout en maintenant la connectivité des réseaux et les canaux de communication;

d) la sauvegarde des données cruciales pour l'entreprise et des informations actualisées sur les contacts nécessaires, de manière à assurer la communication au sein du prestataire de services de communication de données et avec les clients;

e) les procédures relatives au passage à un site de sauvegarde et à l'exploitation des services de communication de données depuis un tel site;

f) le délai cible maximal de rétablissement des fonctions critiques, qui doit être aussi court que possible et, en tout état de cause, ne pas dépasser six heures dans le cas de dispositifs de publication agréés (APA) et de fournisseurs de systèmes consolidés de publication (CTP), ni l'heure de clôture des activités le jour ouvrable suivant dans le cas de mécanismes de déclaration agréés (ARM);

g) une formation du personnel sur le fonctionnement des mécanismes de continuité des activités, définissant le rôle de chacun, et notamment de membres du personnel spécifiquement chargés des opérations de sécurité et prêts à réagir immédiatement en cas de perturbation des services.

4. Un prestataire de services de communication de données met en place un programme en vue de périodiquement tester, réexaminer et, au besoin, modifier les mécanismes de continuité des activités.

5. Un prestataire de services de communication de données informe immédiatement l'autorité compétente de son État membre d'origine et ses clients de toute interruption des services ou de toute perturbation des connexions, ainsi que du délai estimé pour le rétablissement de services normaux, et publie ces informations sur son site web.

6. Dans le cas d'un ARM, les notifications visées au paragraphe 5 sont également effectuées auprès de toute autorité compétente à laquelle l'ARM soumet des déclarations de transactions.

Article 8

Tests et capacités

1. Un prestataire de services de communication de données applique des méthodes de développement et de test clairement définies garantissant que:

a) l'exploitation des systèmes informatiques est conforme aux obligations réglementaires du prestataire de services de communication de données;

b) les mécanismes de contrôle de conformité et de gestion des risques intégrés dans les systèmes informatiques fonctionnent comme prévu;

c) les systèmes informatiques peuvent continuer à fonctionner efficacement en toutes circonstances.

2. Un prestataire de services de communication de données applique également les méthodes visées au paragraphe 1 avant et après toute mise à jour des systèmes informatiques.

3. Un prestataire de services de communication de données informe sans délai l'autorité compétente de son État membre d'origine de tout projet de modification importante du système informatique avant sa mise en œuvre.

4. Dans le cas d'un ARM, les notifications visées au paragraphe 3 sont également effectuées auprès de toute autorité compétente à laquelle l'ARM soumet des déclarations de transactions.

5. Un prestataire de services de communication de données met en place un programme permanent de réexamen périodique et, au besoin, de modification des méthodes de développement et de test.

6. Un prestataire de services de communication de données effectue périodiquement des tests de résistance, au moins une fois par an. Il inclut parmi les scénarios défavorables du test de résistance un comportement inattendu des composants essentiels de ses systèmes et des lignes de communication. Les tests de résistance mettent en évidence la manière dont le matériel informatique, les logiciels et les communications réagissent aux menaces potentielles, en indiquant les systèmes qui sont incapables de faire face aux scénarios défavorables. Le prestataire de services de communication de données prend des mesures pour remédier aux lacunes constatées de ces systèmes.

7. Un prestataire de services de communication de données dispose:

a) d'une capacité suffisante pour s'acquitter de ses fonctions sans interruption ou défaillance, liée notamment à des données manquantes ou incorrectes;

b) d'une flexibilité suffisante pour s'adapter, sans délai excessif, à toute augmentation de la quantité d'informations à traiter et du nombre de demandes d'accès de ses clients.

Article 9

Sécurité

1. Un prestataire de services de communication de données met en place et maintient des procédures et dispositifs de sécurité physique et électronique conçus pour:

a) protéger ses systèmes informatiques contre toute utilisation abusive ou tout accès non autorisé;

b) minimiser les risques d'attaques contre les systèmes d'information au sens de l'article 2, point a), de la directive 2013/40/UE du Parlement européen et du Conseil ([1]);

c) empêcher la divulgation non autorisée d'informations confidentielles;

d) garantir la sécurité et l'intégrité des données.

2. Lorsqu'une entreprise d'investissement («entreprise déclarante») a recours à un tiers («entreprise déposante») pour soumettre en son nom des informations à un ARM, l'ARM dispose de procédures et de dispositifs pour garantir que l'entreprise déposante n'a accès à aucune autre information concernant l'entreprise déclarante ou soumise par cette dernière à l'ARM, qui a pu être envoyée par l'entreprise déclarante à l'ARM directement ou par l'intermédiaire d'une autre entreprise déposante.

3. Un prestataire de services de communication de données met en place et maintient des mesures et des dispositifs permettant de repérer et gérer rapidement les risques visés au paragraphe 1.

4. S'agissant des failles dans les mesures de sécurité physique ou électronique prévues aux paragraphes 1, 2 et 3, le prestataire de services de communication de données en informe dans les plus brefs délais:

a) l'autorité compétente de son État membre d'origine et lui fournit un rapport d'incident indiquant la nature de l'incident, les mesures adoptées pour y remédier et les initiatives prises pour empêcher de tels incidents de se reproduire;

b) ceux de ses clients qui ont été touchés par la faille de sécurité.

([1]) Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

5. Dans le cas d'un ARM, la notification visée au paragraphe 4, point a), est également effectuée auprès de toute autorité compétente à laquelle l'ARM soumet des déclarations de transactions.

Article 10

Gestion par les APA et les CTP des informations incomplètes ou susceptibles d'être erronées

1. Les APA et les CTP mettent en place et maintiennent les dispositifs nécessaires pour garantir qu'ils publient avec exactitude les rapports de négociation reçus de la part d'entreprises d'investissement et, dans le cas de CTP, de la part de plates-formes de négociation et d'APA, sans eux-mêmes introduire d'erreur ou omettre d'informations, et ils corrigent les informations lorsqu'ils sont eux-mêmes à l'origine de l'erreur ou de l'omission.

2. Les APA et les CTP surveillent constamment en temps réel la performance de leurs systèmes informatiques en s'assurant que les rapports de négociation qu'ils ont reçus ont bien été publiés.

3. Les APA et les CTP vérifient périodiquement la concordance entre les rapports de négociation qu'ils reçoivent et ceux qu'ils publient, en vérifiant la bonne publication des informations.

4. Un APA qui reçoit un rapport de négociation en accuse réception auprès de l'entreprise d'investissement déclarante et lui confirme le code d'identification de transaction qu'il a attribué. Dans toute communication ultérieure avec l'entreprise déclarante au sujet d'un rapport de négociation spécifique, l'APA indique le code d'identification de transaction.

5. Un APA établit et maintient les dispositifs nécessaires pour détecter dès leur réception les rapports de négociation qui sont incomplets ou qui contiennent des informations susceptibles d'être erronées. Ces dispositifs comprennent des mécanismes automatiques d'alerte de prix et de volume, tenant compte:

a) du secteur et du segment sur lequel l'instrument financier est négocié;

b) des niveaux de liquidité, incluant les niveaux de négociation historiques;

c) de prix et de volumes de référence appropriés;

d) si nécessaire, d'autres paramètres qui dépendent des caractéristiques de l'instrument financier.

6. Lorsqu'un APA constate qu'un rapport de négociation qu'il a reçu est incomplet ou contient des informations susceptibles d'être erronées, il ne le publie pas et avertit rapidement l'entreprise d'investissement qui soumet ce rapport.

7. Dans des circonstances exceptionnelles, les APA et CTP suppriment ou modifient des informations dans un rapport de négociation à la demande de l'entité qui fournit ces informations lorsque pour des raisons techniques, cette dernière ne peut pas supprimer ou modifier ses propres informations.

8. Les APA publient des politiques non discrétionnaires en matière de suppression et de modification des informations contenues dans les rapports de négociation, qui fixent les sanctions qu'ils peuvent imposer aux entreprises d'investissement ayant fourni des rapports de négociation dont les informations incomplètes ou erronées ont conduit à la suppression ou à la modification de ces rapports.

Article 11

Gestion par les ARM des informations incomplètes ou susceptibles d'être erronées

1. Un ARM établit et maintient les dispositifs nécessaires pour détecter les déclarations de transactions qui sont incomplètes ou qui contiennent des erreurs manifestes dont des clients sont à l'origine. Un ARM effectue la validation des déclarations de transactions au regard des obligations prévues par l'article 26 du règlement (UE) n° 600/2014 en ce qui concerne les champs, le format et le contenu des champs conformément au tableau 1 de l'annexe I du règlement délégué (UE) 2017/590 de la Commission ([1]).

([1]) Règlement délégué (UE) 2017/590 de la Commission du 28 juillet 2016 complétant le règlement (UE) n° 600/2014 du Parlement européen et du Conseil par des normes techniques de réglementation pour la déclaration de transactions aux autorités compétentes (voir page 449 dur présent Journal officiel).

2. Un ARM met en place et maintient les dispositifs nécessaires pour détecter les déclarations de transactions qui comportent des erreurs ou des omissions dont il est lui-même à l'origine et pour corriger, y compris par des suppressions ou des modifications, ces erreurs ou omissions. Un ARM effectue la validation pour les champs, le format et le contenu des champs conformément au tableau 1 de l'annexe I du règlement délégué (UE) 2017/590.

3. Un ARM surveille constamment en temps réel la performance de ses systèmes en s'assurant que les déclarations de transactions qu'il reçoit sont bien transmises à l'autorité compétente, conformément à l'article 26 du règlement (UE) nº 600/2014.

4. Un ARM vérifie périodiquement, à la demande de l'autorité compétente de son État membre d'origine ou de l'autorité compétente à laquelle il transmet des déclarations de transactions, la concordance entre, d'une part, les informations qu'il reçoit de son client ou qu'il génère pour le compte de celui-ci aux fins de la déclaration de transactions, et d'autre part, des échantillons de données extraits des informations fournies par l'autorité compétente.

5. Les corrections, y compris les suppressions ou modifications de déclarations de transactions, qui ne corrigent pas des erreurs ou omissions dont l'ARM est à l'origine, ne sont faites qu'à la demande d'un client et pour une déclaration de transaction donnée. Lorsqu'un ARM supprime ou modifie une déclaration de transaction à la demande d'un client, il fournit cette déclaration de transaction actualisée à ce client.

6. Lorsqu'un ARM, avant de transmettre la déclaration de transaction, détecte une erreur ou une omission dont un client est à l'origine, il ne soumet pas cette déclaration de transaction et avertit sans délai l'entreprise d'investissement des détails de cette erreur ou omission pour permettre au client de soumettre des informations corrigées.

7. Lorsqu'un ARM prend connaissance d'erreurs ou d'omissions dont il est lui-même à l'origine, il transmet sans délai une déclaration exacte et complète.

8. L'ARM avertit sans délai le client des détails de l'erreur ou de l'omission et lui fournit une déclaration de transaction actualisée. L'ARM avertit également sans délai de cette erreur ou omission l'autorité compétente de son État membre d'origine et l'autorité compétente à laquelle il a transmis la déclaration de transaction.

9. L'obligation de corriger ou supprimer les déclarations de transaction erronées ou de signaler les transactions omises ne concerne pas les erreurs ou omissions qui ont eu lieu plus de cinq ans avant la date à laquelle l'ARM en a pris connaissance.

Article 12

Connectivité des ARM

1. Un ARM dispose des politiques, dispositifs et capacités techniques nécessaires pour se conformer aux spécifications techniques fixées par l'autorité compétente de son État membre d'origine et par les autres autorités compétentes auxquelles il adresse des déclarations de transactions pour la transmission de ces déclarations.

2. Un ARM dispose des politiques, dispositifs et capacités techniques nécessaires pour recevoir les déclarations de transactions de clients et leur transmettre des informations en retour. L'ARM fournit au client une copie de la déclaration de transaction qu'il a transmise pour son compte à l'autorité compétente.

Article 13

Autres services fournis par les CTP

1. Un CTP peut fournir les services supplémentaires suivants:

a) fourniture de données pour la transparence pré-négociation;

b) fourniture de données historiques;

c) fourniture de données de référence;

d) fourniture de services de recherche;

e) traitement, distribution et commercialisation de données et de statistiques sur les instruments financiers et les plates-formes de négociation, ainsi que d'autres données relatives au marché;

f) conception, gestion, maintenance et commercialisation de logiciels, de matériel informatique et de réseaux pour la transmission de données et d'informations.

2. Un CTP peut fournir des services améliorant l'efficience du marché, autres que ceux indiqués au paragraphe 1, à condition que ces services ne génèrent pas un risque pour la qualité de la consolidation ou l'indépendance du CTP qui ne puisse pas être efficacement évité ou circonscrit.

CHAPITRE III

DISPOSITIFS DE PUBLICATION

(Article 64, paragraphes 1 et 2, et article 65, paragraphe 1, de la directive 2014/65/UE)

Article 14

Lisibilité par machine

1. Les APA et les CTP publient sous une forme lisible par machine les informations qui doivent être rendues publiques conformément à l'article 64, paragraphe 1, et à l'article 65, paragraphe 1, de la directive 2014/65/UE.

2. Les CTP publient sous une forme lisible par machine les informations qui doivent être rendues publiques conformément à l'article 65, paragraphe 2, de la directive 2014/65/UE.

3. Les informations ne sont réputées publiées sous une forme lisible par machine que si toutes les conditions suivantes sont remplies:

a) elles se présentent sous un format électronique conçu pour être directement et automatiquement lu par un ordinateur;

b) elles sont stockées dans une architecture informatique appropriée, conformément à l'article 8, paragraphe 7, laquelle permet un accès automatique;

c) elles sont suffisamment solides pour garantir la continuité et la régularité des services fournis et sont accessibles suffisamment rapidement;

d) elles sont accessibles, lisibles, utilisables et copiables par des logiciels informatiques publiquement disponibles et gratuits.

Aux fins du premier alinéa, point a), le format électronique est précisé par des normes libres, non propriétaires et ouvertes.

4. Aux fins du paragraphe 3, point a), le format électronique comprend le type de fichiers ou messages, les règles pour les identifier, et le nom et le type de données des champs qu'ils contiennent.

5. Les APA et les CTP:

a) mettent à la disposition du public des instructions expliquant où et comment obtenir et utiliser facilement les données, y compris l'indication du format électronique;

b) rendent publiques toutes les modifications apportées aux instructions visées au point a) au moins trois mois avant qu'elles ne prennent effet, sauf en cas d'urgence dûment justifiée nécessitant qu'elles prennent effet plus rapidement;

c) font figurer sur la page d'accueil de leur site web un lien vers les instructions visées au point a).

Article 15

Données à inclure dans le système consolidé de publication pour les actions, les certificats représentatifs, les fonds cotés, les certificats préférentiels et autres instruments financiers similaires

1. Un CTP inclut dans ses flux électroniques de données les données rendues publiques conformément aux articles 6 et 20 du règlement (UE) n° 600/2014 concernant tous les instruments financiers visés dans lesdits articles.

2. Lorsqu'un nouvel APA ou une nouvelle plate-forme de négociation entre en activité, un CTP inclut les données rendues publiques par cet APA ou cette plate-forme de négociation dans le flux électronique de données de son système consolidé de publication le plus tôt possible, et en tout état de cause au plus tard six mois après l'entrée en activité de l'APA ou de la plate-forme de négociation.

Article 16

Identification des rapports de négociation originaux et de leurs doubles pour les actions, les certificats représentatifs, les fonds cotés, les certificats préférentiels et autres instruments financiers similaires

1. Lorsqu'un APA publie un rapport de négociation qui constitue un double, il inscrit le code «DUPL» dans un champ de réédition afin de permettre aux destinataires des données de distinguer le rapport de négociation original de ses éventuels doubles.

2. Aux fins du paragraphe 1, un APA exige de chaque entreprise d'investissement qu'elle se conforme à l'une des conditions suivantes:

a) certifier qu'elle ne passe que par cet APA pour déclarer les transactions portant sur un instrument financier donné;

b) utiliser un mécanisme d'identification qui signale une déclaration comme étant l'originale («ORGN») et toutes les autres déclarations de la même transaction comme des doubles («DUPL»).

Article 17

Publication des rapports originaux pour les actions, les certificats représentatifs, les fonds cotés, les certificats préférentiels et autres instruments financiers similaires

Un CTP ne consolide pas les rapports de négociation pour lesquels le code «DUPL» figure dans le champ de réédition.

Article 18

Renseignements à publier par l'APA

1. Un APA publie:

a) pour les transactions exécutées portant sur des actions, des certificats représentatifs, des fonds cotés, des certificats préférentiels ou d'autres instruments financiers similaires, les détails d'une transaction précisés dans le tableau 2 de l'annexe I du règlement délégué (UE) 2017/587 et utilise les codes signalétiques appropriés énumérés dans le tableau 3 de l'annexe I du règlement délégué (UE) 2017/587;

b) pour les transactions exécutées portant sur des obligations, des produits financiers structurés, des quotas d'émission ou des instruments dérivés, les détails d'une transaction précisés dans le tableau 1 de l'annexe II du règlement délégué (UE) 2017/583 et utilise les codes signalétiques appropriés énumérés dans le tableau 2 de l'annexe II du règlement délégué (UE) 2017/583.

2. Lorsqu'il publie des informations sur le moment où la transaction a été déclarée, l'APA indique la date et l'heure, à la seconde près, où il publie la transaction.

3. Par dérogation au paragraphe 2, un APA qui publie des informations concernant une transaction exécutée sur un système électronique indique la date et l'heure, à la milliseconde près, de la publication de cette transaction dans son rapport de négociation.

4. Aux fins du paragraphe 3, on entend par «système électronique» un système dans lequel les ordres peuvent être exécutés électroniquement ou dans lequel les ordres peuvent être exécutés en dehors du système pour autant qu'ils soient signalés au moyen du système en question.

5. Les horodatages visés aux paragraphes 2 et 3 ne s'écartent pas, respectivement, de plus d'une seconde ou de plus d'une milliseconde du temps universel coordonné (TUC) émis et géré par l'un des centres horaires énumérés dans le dernier rapport annuel sur les activités relatives à la mesure du temps *(Annual Report on Time Activities)* du Bureau international des poids et mesures (BIPM).

Article 19

Non-discrimination

Les APA et les CTP veillent à ce que les informations qui doivent être rendues publiques soient envoyées simultanément à travers tous les canaux de distribution, y compris lorsque ces informations sont rendues publiques dans un délai aussi proche du temps réel que le permettent les moyens techniques ou 15 minutes après la première publication.

Article 20

Renseignements à publier par le CTP

Un CTP publie:

a) pour les transactions exécutées portant sur des actions, des certificats représentatifs, des fonds cotés, des certificats préférentiels ou d'autres instruments financiers similaires, les détails d'une transaction précisés dans le tableau 2 de l'annexe I du règlement délégué (UE) 2017/587 et utilise les codes signalétiques appropriés énumérés dans le tableau 3 de l'annexe I du règlement délégué (UE) 2017/587;

b) pour les transactions exécutées portant sur des obligations, des produits financiers structurés, des quotas d'émission ou des instruments dérivés, les détails d'une transaction précisés dans le tableau 1 de l'annexe II du règlement délégué (UE) 2017/583 et utilise les codes signalétiques appropriés énumérés dans le tableau 2 de l'annexe II du règlement délégué (UE) 2017/583.

Article 21

Entrée en vigueur et application

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

Il s'applique à compter de la première date visée à l'article 93, paragraphe 1, deuxième alinéa, de la directive 2014/65/UE.

Cependant, l'article 14, paragraphe 2, et l'article 20, point b), s'appliquent à compter du premier jour du neuvième mois suivant la date d'entrée en application de la directive 2014/65/UE.

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

Fait à Bruxelles, le 2 juin 2016.

Par la Commission

Le président

Jean-Claude JUNCKER