REGULAMENTO DELEGADO (UE) 2017/571 DA COMISSÃO

de 2 de junho de 2016

que complementa a Diretiva 2014/65/UE do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação sobre a autorização, requisitos de organização e a publicação de transações no que respeita aos prestadores de serviços de comunicação de dados

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta a Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE ([1]), nomeadamente o artigo 61.º, n.º 4, o artigo 64.º, n.ºs 6 e 8, o artigo 65.º, n.ºs 6 e 8, e o artigo 66.º, n.º 5,

Considerando o seguinte:

(1) Em conformidade com a Diretiva 2014/65/UE, os prestadores de serviços de comunicação de dados abrangem três tipos diferentes de entidades: sistemas de reporte autorizados (ARM), sistemas de publicação autorizados (APA) e prestadores de informações consolidadas (CTP). Embora estes tipos de entidades desenvolvam atividades diferentes, a Diretiva 2014/65/UE prevê um processo de autorização semelhante para todas.

(2) O requerente de uma autorização como prestador de serviços de comunicação de dados deve fornecer no seu pedido de autorização um programa de atividades e um organograma. O organograma deve identificar quem é responsável pelas diferentes atividades, para que a autoridade competente possa avaliar se o prestador de serviços de comunicação de dados dispõe de recursos humanos suficientes e se as suas atividades são supervisionadas. O organograma deve abranger não só o âmbito dos serviços de comunicação de dados como também quaisquer outros serviços que a entidade preste, uma vez que assim se poderão evidenciar domínios suscetíveis de afetar a independência do prestador de serviços de comunicação de dados e de dar origem a um conflito de interesses. O requerente de uma autorização como prestador de serviços de comunicação de dados deve fornecer igualmente informações sobre a composição, o funcionamento e a independência dos seus órgãos diretivos, para que as autoridades competentes possam avaliar se as políticas, os procedimentos e a estrutura de governo societário asseguram a independência do prestador de serviços de comunicação de dados e evitam os conflitos de interesses.

(3) Podem surgir conflitos de interesses entre o prestador de serviços de comunicação de dados e os clientes que utilizam os seus serviços para cumprirem as suas obrigações regulamentares e outras entidades que adquirem dados aos prestadores de serviços de comunicação de dados. Em particular, esses conflitos podem surgir quando o prestador de serviços de comunicação de dados está envolvido noutras atividades, nomeadamente na qualidade de operador de mercado, empresa de investimento ou repositório de transações. Se os conflitos forem deixados por resolver, poderá ocorrer uma situação em que o prestador de serviços de comunicação de dados tem um incentivo para adiar a publicação ou a apresentação de dados ou para negociar com base em informações confidenciais que recebeu. O prestador de serviços de comunicação de dados deve, por conseguinte, adotar uma abordagem global para a identificação, prevenção e gestão dos conflitos de interesses existentes e potenciais, incluindo a preparação de um inventário dos conflitos de interesses e a implementação de políticas e procedimentos adequados para gerir esses conflitos e, quando necessário, deverá separar as funções e o pessoal envolvido por forma a limitar o fluxo de informações sensíveis entre as diferentes áreas comerciais do prestador de serviços de comunicação de dados.

(4) Todos os membros do órgão de administração de um prestador de serviços de comunicação de dados devem ter a idoneidade necessária e possuir conhecimentos, competências e experiência suficientes, uma vez que essas pessoas desempenham um papel fundamental na garantia de que o prestador de serviços de comunicação de dados respeita as suas obrigações regulamentares e contribuem para a definição da sua estratégia comercial. É, por conseguinte, importante que o prestador de serviços de comunicação de dados demonstre que possui um processo sólido de nomeação e avaliação do desempenho dos membros do órgão de administração e que existem canais de comunicação claros e uma apresentação regular de relatórios ao órgão de administração.

([1]) JO L 173 de 12.6.2014, p. 349.

(5) A externalização de atividades, em especial de funções críticas, é suscetível de constituir uma alteração significativa das condições de autorização de um prestador de serviços de comunicação de dados. Para garantir que a externalização de atividades não prejudica a capacidade do prestador de serviços de comunicação de dados para cumprir as suas obrigações ao abrigo da Diretiva 2014/65/UE nem conduz a conflitos de interesses, o prestador de serviços de comunicação de dados deve ser capaz de demonstrar a existência de uma supervisão e de um controlo suficientes dessas atividades.

(6) Os sistemas informáticos utilizados por um prestador de serviços de comunicação de dados devem ser adaptados aos diferentes tipos de atividades que essas entidades podem desempenhar, ou seja, publicar relatórios comerciais, apresentar comunicações de transações ou fornecer um sistema de prestação de informações consolidadas, e suficientemente sólidos para assegurar a continuidade e a regularidade da prestação dos referidos serviços. Tal inclui assegurar que os sistemas informáticos do prestador de serviços de comunicação de dados conseguem lidar com flutuações no volume de dados a tratar. Tais flutuações, designadamente aumentos inesperados no fluxo de dados, podem ter um impacto negativo na eficácia dos sistemas do prestador de serviços de comunicação de dados e, em consequência, na sua capacidade para publicar ou comunicar informações completas e exatas nos prazos exigidos. Para fazer face a este problema, um prestador de serviços de comunicação de dados deve testar periodicamente os seus sistemas, a fim de assegurar que sejam suficientemente robustos para lidar com alterações das condições operacionais e moduláveis.

(7) Os sistemas e as estruturas de salvaguarda estabelecidos por um prestador de serviços de comunicação de dados devem ser suficientes para permitir que continue a prestar os seus serviços, mesmo quando ocorram incidentes que perturbem as suas atividades. Um prestador de serviços de comunicação de dados deve definir os prazos máximos aceitáveis de recuperação de funções críticas, que serão aplicáveis em caso de incidente com perturbação das atividades e deverão permitir o cumprimento dos prazos para a apresentação de relatórios e a divulgação de informações.

(8) Para garantir que está em condições de prestar os serviços, o prestador de serviços de comunicação de dados deve analisar as tarefas e atividades que são críticas para essa prestação e os cenários possíveis que possam dar origem a um incidente com perturbação das atividades, incluindo a adoção de medidas para prevenir e atenuar essas situações.

(9) Quando ocorre uma perturbação do serviço, um prestador de serviços de comunicação de dados deve comunicar a situação à autoridade competente do seu Estado-Membro de origem, a quaisquer outras autoridades competentes relevantes, aos seus clientes e ao público, uma vez que a perturbação pode também significar que essas partes não serão capazes de cumprir as suas próprias obrigações regulamentares, nomeadamente o dever de remeter as comunicações de transações a outras autoridades competentes ou de tornar públicos os pormenores das transações efetuadas. A notificação deve permitir que essas partes adotem medidas alternativas para assegurar o cumprimento das suas obrigações.

(10) A implementação de atualizações dos sistemas informáticos poderá potencialmente afetar a eficácia e a solidez dos sistemas utilizados para a prestação de serviços de dados. Para evitar que o funcionamento do seu sistema informático seja, em qualquer momento, incompatível com as suas obrigações regulamentares, em particular com as obrigações de dispor de um mecanismo de segurança sólido e concebido de forma a garantir a segurança dos meios de transferência das informações, de minimizar o risco de corrupção dos dados e de evitar fugas de informação antes da publicação, um prestador de serviços de comunicação de dados deve utilizar metodologias de desenvolvimento e teste claramente delineadas a fim de assegurar que os controlos da conformidade e da gestão do risco integrados nos seus sistemas funcionam como previsto e que o sistema poderá continuar a funcionar eficazmente em qualquer situação. Se um prestador de serviços de comunicação de dados efetuar uma alteração importante do sistema, deve notificar a autoridade competente do respetivo Estado-Membro de origem e outras autoridades competentes, nos casos pertinentes, para que estas possam avaliar se a atualização terá um impacto sobre os seus próprios sistemas e se as condições da autorização continuam a estar cumpridas.

(11) A divulgação pública prematura, no caso dos relatórios comerciais, ou a divulgação não autorizada, no caso das comunicações de transações, poderão dar indicações quanto à estratégia de negociação ou revelar informações sensíveis, como a identidade dos clientes do prestador de serviços de comunicação de dados. Por conseguinte, o prestador de serviços de comunicação de dados deve implementar controlos físicos, tais como instalações trancadas, e controlos eletrónicos, incluindo *firewalls* e palavras-passe, para garantir que só o pessoal autorizado tenha acesso aos dados.

(12) As violações da segurança física ou eletrónica de um prestador de serviços de comunicação de dados constituem uma ameaça à confidencialidade dos dados dos clientes. Por conseguinte, sempre que ocorra uma tal violação, um prestador de serviços de comunicação de dados deve notificar imediatamente a autoridade competente relevante, bem como quaisquer clientes que tenham sido afetados. A notificação à autoridade competente do

Estado-Membro de origem é necessária para permitir que essa autoridade competente cumpra as suas responsabilidades de supervisão contínua no que diz respeito à questão de saber se o prestador de serviços de comunicação de dados está a manter devidamente mecanismos de segurança sólidos para garantir a segurança das informações e minimizar o risco de corrupção dos dados e de acesso não autorizado. Outras autoridades competentes que disponham de uma *interface* técnica com o prestador de serviços de comunicação de dados devem também ser notificadas, na medida em que podem ser negativamente afetadas, em especial se a violação estiver relacionada com os meios de transferência da informação entre o prestador de serviços de comunicação de dados e a autoridade competente.

(13) Uma empresa de investimento que tenha obrigações de informação sobre transações, conhecida como uma «empresa declarante», pode optar por recorrer a um terceiro para apresentar as comunicações de transações em seu nome a um ARM, que será a «empresa que apresenta a comunicação». Em virtude do papel que desempenha, a empresa que apresenta a comunicação terá acesso às informações confidenciais que apresenta. Contudo, a empresa que apresenta a comunicação não deve ter o direito de aceder a quaisquer outros dados sobre a empresa declarante ou sobre as transações da empresa declarante realizadas no âmbito do ARM. Tais dados podem dizer respeito a comunicações de transações que a própria empresa declarante enviou ao ARM ou a outra empresa, para posterior envio ao ARM. Estes dados não devem estar acessíveis à empresa que apresenta a comunicação, na medida em que podem conter informações confidenciais como a identidade dos clientes da empresa declarante.

(14) Um prestador de serviços de comunicação de dados deve assegurar-se de que os dados que está a publicar ou a apresentar são exatos e completos e deve garantir que dispõe de mecanismos para detetar erros ou omissões causados pelo cliente ou pelo próprio prestador. No caso de um ARM, tal pode incluir conciliações de uma amostra da população dos dados apresentados ao ARM por uma empresa de investimento ou gerados pelo ARM em nome da empresa de investimento com os dados correspondentes fornecidos pela autoridade competente. A frequência e a abrangência dessas conciliações devem ser proporcionadas ao volume de dados tratados pelo ARM e à medida em que este irá gerar comunicações de transações a partir dos dados dos clientes ou transmitir comunicações de transações preenchidas pelos clientes. A fim de assegurar uma comunicação atempada e isenta de erros e omissões, um ARM deve monitorizar continuamente o desempenho dos seus sistemas.

(15) Quando um ARM provocar um erro ou uma omissão, deve corrigir sem demora essa informação, bem como notificar esse erro ou omissão à autoridade competente do seu Estado-Membro de origem e a qualquer outra autoridade competente à qual apresente relatórios, uma vez que tais autoridades competentes são afetadas pela qualidade dos dados que lhes são apresentados. O ARM deve igualmente notificar o erro ou omissão ao seu cliente e fornecer-lhe informações atualizadas, de modo a que os registos internos do cliente possam ser alinhados com as informações que o ARM apresentou à autoridade competente em nome desse mesmo cliente.

(16) Os APA e os CTP devem poder apagar e alterar as informações que recebem de uma entidade que lhes faculte informações para lidarem com situações em que, em circunstâncias excecionais, a entidade que relata esteja a deparar-se com dificuldades técnicas e não possa apagar ou alterar ela própria essas informações. Contudo, os APA e os CTP não devem ser responsáveis pela correção de informações contidas nos relatórios publicados se o erro ou a omissão for imputável à entidade que faculta as informações. Tal deve-se ao facto de os APA e os CTP não poderem saber com certeza se uma omissão ou um erro observado está, de facto, incorreto, dado que não participaram na transação executada.

(17) Para facilitar uma comunicação fiável entre um APA e a empresa de investimento que comunica uma transação, nomeadamente no que diz respeito a anulações e alterações de transações específicas, o APA deverá incluir nas mensagens de confirmação enviadas às empresas de investimento que comunicam as transações o código de identificação da transação que foi atribuído pelo APA ao tornar pública a informação.

(18) Para efeitos de cumprimento das suas obrigações de comunicação ao abrigo do Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho ([1]), um ARM deve assegurar o fluxo regular de informação de e para uma autoridade competente, incluindo a capacidade de transferir relatórios e de lidar com relatórios rejeitados. O ARM deve, por conseguinte, estar em condições de demonstrar que pode cumprir as especificações técnicas estabelecidas pela autoridade competente no que se refere à interface entre o ARM e a autoridade competente.

([1]) Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativo aos mercados de instrumentos financeiros e que altera o Regulamento (UE) n.º 648/2012 (JO L 173 de 12.6.2014, p. 84).

(19) Um prestador de serviços de comunicação de dados deve também assegurar que armazena as informações de comunicação de transações e de comunicação comercial que trata durante um período suficiente para permitir a recuperação de informações históricas por parte das autoridades competentes. No caso específico dos APA e CTP, devem garantir que estabelecem os mecanismos organizativos necessários para conservar os dados pelo menos durante o período especificado no Regulamento (UE) n.º 600/2014 e que estão em condições de responder a qualquer pedido de prestação de serviços regulado pelo presente regulamento.

(20) O presente regulamento estabelece uma série de serviços adicionais que um CTP pode realizar e que aumentam a eficiência do mercado. Tendo em conta as possíveis evoluções do mercado, não é adequado apresentar uma lista exaustiva dos serviços adicionais que um CTP pode realizar. Um CTP deve, por conseguinte, ser capaz de fornecer outros serviços para além dos serviços adicionais especificamente previstos no presente regulamento, desde que esses outros serviços não coloquem qualquer risco para a independência do CTP ou para a qualidade do sistema de prestação de informações consolidadas.

(21) A fim de assegurar uma divulgação eficiente das informações publicadas pelos APA e CTP e um acesso e utilização simples dessas informações por parte dos participantes no mercado, a informação deve ser publicada num formato passível de leitura por máquina através de canais robustos que permitam o acesso automático aos dados. Embora nem sempre os sítios *web* possam oferecer uma arquitetura suficientemente robusta e modulável para permitir um acesso fácil e automático aos dados, essas limitações tecnológicas poderão ser ultrapassadas no futuro. Por conseguinte, não deve ser definida uma tecnologia específica, mas sim os critérios a cumprir pela tecnologia que será utilizada.

(22) No que diz respeito aos instrumentos de capital próprio e equivalentes, o Regulamento (UE) n.º 600/2014 não exclui a possibilidade de as empresas de investimento tornarem públicas as suas transações através de mais do que um APA. Contudo, deve existir um acordo específico para permitir que as partes interessadas consolidem as informações comerciais provenientes de diversos APA, nomeadamente CTP, a fim de identificar as potenciais transações duplicadas, uma vez que, se isso não for feito, uma mesma transação poderá ser consolidada várias vezes e repetidamente publicada pelos CTP. Tal poderia comprometer a qualidade e a utilidade do sistema de prestação de informações consolidadas.

(23) Aquando da publicação de uma transação, os APA devem, por conseguinte, publicar as transações comunicadas pelas empresas de investimento incluindo um campo de «reimpressão» que indique se uma comunicação representa um duplicado. A fim de permitir uma abordagem neutra em termos da tecnologia utilizada, é necessário prever diferentes formas possíveis de um APA conseguir identificar duplicados.

(24) Para assegurar que cada transação é incluída apenas uma vez no sistema de prestação de informações consolidadas, reforçando por conseguinte a fiabilidade das informações facultadas, os CTP não devem publicar informações relativas a uma transação publicada por um APA que esteja identificada como um duplicado.

(25) Os APA devem publicar informações sobre as transações, nomeadamente os carimbos de tempo relevantes, como a hora a que as transações foram executadas e a hora a que foram comunicadas. Além disso, a granularidade dos carimbos de tempo deve refletir a natureza do sistema de negociação em que a transação foi executada. Deve prever-se uma maior granularidade na publicação de informações sobre as transações executadas em sistemas eletrónicos do que para as transações executadas em sistemas não eletrónicos.

(26) Os CTP podem publicar informações sobre os instrumentos representativos de capital e os instrumentos não representativos de capital. Tendo em conta os diferentes requisitos para o funcionamento dos registos e, em particular, o âmbito significativamente mais vasto dos instrumentos financeiros não representativos de capital e a aplicação diferida das disposições da Diretiva 2014/65/UE para o sistema de prestação de informações consolidadas sobre esses instrumentos, o presente regulamento apenas especifica no seu âmbito os CTP que consolidam informações sobre instrumentos de capital.

(27) As disposições do presente regulamento estão estreitamente relacionadas, uma vez que lidam com a autorização, os requisitos de organização e a publicação das transações no que respeita aos prestadores de serviços de comunicação de dados. Para assegurar a coerência entre estas disposições, que devem entrar em vigor simultaneamente, e facilitar uma visão abrangente pelas partes interessadas e, em especial, pelas partes sujeitas às obrigações previstas, é necessário incluir estas normas técnicas de regulamentação num único regulamento.

(28) O presente regulamento especifica os requisitos de publicação de dados aplicáveis aos APA e CTP. Para garantir práticas coerentes na publicação de informações de negociação em todas as plataformas de negociação, APA e CTP, bem como para facilitar a consolidação de dados por parte dos CTP, o presente regulamento deve ser aplicável em conjugação com os Regulamentos Delegados (UE) 2017/587 ([1]) e (UE) 2017/583 ([2]) da Comissão, onde são definidos os requisitos pormenorizados aplicáveis à publicação de informações sobre transações.

(29) Por razões de coerência e a fim de assegurar o funcionamento eficiente dos mercados financeiros, é necessário que as disposições do presente regulamento e as correspondentes disposições nacionais de transposição da Diretiva 2014/65/UE sejam aplicáveis a partir da mesma data. Uma vez que o artigo 65.º, n.º 2, da Diretiva 2014/65/UE é aplicável a partir de 3 de setembro do ano seguinte ao ano de entrada em vigor do presente regulamento, determinadas disposições do presente regulamento deverão ser aplicáveis a partir dessa data posterior.

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

(31) A ESMA conduziu consultas públicas abertas sobre os projetos de normas técnicas de regulamentação que servem de base ao presente regulamento, analisou os seus potenciais custos e benefícios e solicitou o parecer do Grupo de Interessados do Setor dos Valores Mobiliários e dos Mercados criado pelo artigo 37.º do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([3]),

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

AUTORIZAÇÃO

(Artigo 61.º, n.º 2, da Diretiva 2014/65/UE)

Artigo 1.º

Informação às autoridades competentes

1. O requerente de uma autorização para prestar serviços de comunicação de dados deve apresentar à autoridade competente as informações mencionadas nos artigos 2.º, 3.º e 4.º e as informações respeitantes a todos os requisitos em matéria de organização estabelecidos nos capítulos II e III.

2. Um prestador de serviços de comunicação de dados deve informar de imediato a autoridade competente do seu Estado-Membro de origem de qualquer alteração significativa das informações fornecidas no momento da autorização e posteriormente.

Artigo 2.º

Informações sobre a organização

1. O requerente de uma autorização para prestar serviços de comunicação de dados deve incluir no seu pedido de autorização um programa de atividades como referido no artigo 61.º, n.º 2, da Diretiva 2014/65/UE. O programa de atividades deve incluir as seguintes informações:

a) Informações sobre a estrutura organizativa do requerente, incluindo um organograma e uma descrição dos recursos humanos, técnicos e jurídicos atribuídos às suas atividades comerciais;

([1]) Regulamento Delegado (UE) 2017/587 da Comissão, de 14 de julho de 2016, que complementa o Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho relativo aos mercados de instrumentos financeiros no que diz respeito às normas técnicas de regulamentação relativas aos requisitos de transparência aplicáveis às plataformas de negociação e às empresas de investimento relativamente a ações, certificados de depósito, fundos de índices cotados, certificados e outros instrumentos financeiros similares e às obrigações de execução das transações de certas ações numa plataforma de negociação ou por um internalizador sistemático (ver página 387 do presente Jornal Oficial).

([2]) Regulamento Delegado (UE) 2017/583 da Comissão, de 14 de julho de 2016, que complementa o Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho, relativo aos mercados de instrumentos financeiros, no que respeita às normas técnicas de regulamentação sobre os requisitos de transparência para as plataformas de negociação e empresas de investimento em matéria de obrigações, produtos financeiros estruturados, licenças de emissão e instrumentos derivados (ver página 229 do presente Jornal Oficial).

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

b) Informações sobre as políticas e procedimentos de garantia da conformidade do prestador de serviços de comunicação de dados, incluindo:

i) o nome da pessoa ou das pessoas responsáveis pela aprovação e manutenção dessas políticas,

ii) os mecanismos para monitorizar e aplicar as políticas e os procedimentos de garantia da conformidade,

iii) as medidas a tomar em caso de violação que possa conduzir ao incumprimento das condições da autorização inicial,

iv) uma descrição do procedimento a seguir para comunicar à autoridade competente qualquer violação que possa conduzir a um incumprimento das condições da autorização inicial;

c) Uma lista de todas as funções subcontratadas e dos recursos afetados ao controlo das funções subcontratadas.

2. Um prestador de serviços de comunicação de dados que ofereça serviços distintos da comunicação de dados deve descrever esses serviços no organograma.

Artigo 3.º

Governo das sociedades

1. O requerente de uma autorização para prestar serviços de comunicação de dados deve incluir no seu pedido de autorização informações sobre as políticas internas de governação e sobre os procedimentos que regem o seu órgão de administração, quadros superiores e, se estiverem estabelecidos, comités.

2. As informações referidas no n.º 1 devem incluir:

a) Uma descrição dos processos de seleção, nomeação, avaliação de desempenho e destituição dos quadros superiores e dos membros do órgão de administração;

b) Uma descrição dos canais de comunicação e da frequência da apresentação de relatórios aos quadros superiores e ao órgão de administração;

c) Uma descrição das políticas e procedimentos em matéria de acesso aos documentos por membros do órgão de administração.

Artigo 4.º

Informações sobre os membros do órgão de administração

1. O requerente de uma autorização para prestar serviços de comunicação de dados deve incluir no seu pedido de autorização as seguintes informações relativamente a cada membro do órgão de administração:

a) Nome, data e local de nascimento, número de identificação pessoal nacional ou equivalente, endereço e dados de contacto;

b) O cargo para o qual a pessoa está ou irá ser nomeada;

c) Um *curriculum vitae* que comprove experiência e conhecimentos suficientes para exercer adequadamente as suas responsabilidades;

d) O registo criminal, nomeadamente através de um certificado oficial ou, quando esse documento não estiver disponível no Estado-Membro em causa, uma autodeclaração de idoneidade e a autorização à autoridade competente para verificar se o membro foi condenado por qualquer infração penal relacionada com a prestação de serviços financeiros ou de serviços de dados ou com atos de fraude ou peculato;

e) Uma autodeclaração de idoneidade e a autorização à autoridade competente para verificar se o membro:

i) foi alvo de uma decisão desfavorável no âmbito de um processo de natureza disciplinar intentado por uma autoridade reguladora ou entidade administrativa ou é objeto de um processo dessa natureza ainda pendente,

ii) foi alvo de uma decisão judicial desfavorável no âmbito de um processo cível perante um tribunal, relacionada com a prestação de serviços financeiros ou de serviços de dados, ou por falta grave ou fraude na administração de uma empresa,

iii) fez parte do órgão de administração de uma empresa que tenha sido alvo de uma decisão desfavorável ou de uma sanção por parte de uma autoridade reguladora ou cujo registo ou autorização foi retirado por uma autoridade reguladora,

iv) lhe viu recusado o direito a exercer atividades que exigem registo ou autorização por parte de uma autoridade reguladora,

v) fez parte do órgão de administração de uma empresa que tenha entrado em insolvência ou liquidação enquanto a pessoa exercia tal cargo ou no prazo de um ano após a pessoa ter deixado de exercer tal cargo,

vi) foi sancionado com uma coima, suspenso, destituído ou alvo de qualquer outra sanção por motivo de fraude, peculato ou em relação com a prestação de serviços financeiros ou de serviços de dados, por um organismo profissional,

vii) foi interdito do exercício de funções de direção, de competências de gestão, demitido de um emprego ou de outra responsabilidade numa empresa na sequência de falta grave ou prática abusiva;

f) Uma indicação do tempo mínimo que deve ser dedicado ao desempenho das funções afetadas à pessoa no âmbito do prestador de serviços de comunicação de dados;

g) Uma declaração sobre qualquer potencial conflito de interesses que possa existir ou surgir no desempenho dessas funções e sobre a forma como esses conflitos serão geridos.

CAPÍTULO II

REQUISITOS EM MATÉRIA DE ORGANIZAÇÃO

(Artigo 64.º, n.os 3, 4 e 5, artigo 65.º, n.os 4, 5 e 6, e artigo 66.º, n.os 2, 3 e 4, da Diretiva 2014/65/UE)

Artigo 5.º

Conflitos de interesses

1. Um prestador de serviços de comunicação de dados deve operar e manter mecanismos administrativos eficazes, destinados a evitar conflitos de interesses com os clientes que utilizam os seus serviços para cumprimento das suas obrigações regulamentares e com outras entidades que adquirem dados a prestadores de serviços de comunicação de dados. Esses mecanismos devem incluir políticas e procedimentos para a identificação, gestão e divulgação dos conflitos de interesses, existentes e potenciais, e devem incluir:

a) Um inventário dos conflitos de interesses existentes e potenciais, estabelecendo a respetiva descrição, identificação, prevenção, gestão e divulgação;

b) A separação de tarefas e funções comerciais no seio do prestador de serviços de comunicação de dados, incluindo:

i) medidas destinadas a impedir ou controlar a troca de informações quando possa existir um risco de conflito de interesses,

ii) a supervisão distinta das pessoas relevantes cujas principais funções envolvam interesses que possam entrar em conflito com os interesses de um cliente;

c) Uma descrição da política de determinação dos honorários cobrados pelo prestador de serviços de comunicação de dados e pelas empresas com as quais esse prestador tem relações estreitas;

d) Uma descrição da política de remuneração dos membros do órgão de administração e dos quadros superiores;

e) As regras relativas à aceitação de numerário, presentes ou favores pelo pessoal do prestador de serviços de comunicação de dados e do seu órgão de administração.

2. O inventário dos conflitos de interesses referido no n.º 1, alínea a), deve incluir os conflitos de interesses resultantes de situações em que o prestador de serviços de comunicação de dados:

a) Possa obter um ganho financeiro ou evitar uma perda financeira em detrimento de um cliente;

b) Possa ter um interesse nos resultados de um serviço prestado a um cliente que não coincide com o interesse do cliente perante esses mesmos resultados;

c) Possa ter um incentivo para dar prioridade aos seus próprios interesses ou aos interesses de um outro cliente ou grupo de clientes e não aos interesses do cliente a quem o serviço é prestado;

d) Receba ou possa receber de qualquer pessoa que não seja cliente, em relação ao serviço prestado a um cliente, um incentivo sob a forma de numerário, bens ou serviços, para além da comissão ou dos honorários recebidos pelo serviço.

Artigo 6.º

Requisitos em matéria de organização no que diz respeito à externalização

1. Se um prestador de serviços de comunicação de dados decidir subcontratar os serviços de terceiros para realizarem as atividades em seu nome, incluindo empresas com as quais tenha relações estreitas, deve assegurar que esse terceiro prestador de serviços dispõe de competência e capacidade para realizar as atividades de forma fiável e profissional.

2. Um prestador de serviços de comunicação de dados deve especificar as atividades que irão ser subcontratadas, incluindo uma indicação do nível dos recursos técnicos e humanos necessários para realizar cada uma dessas atividades.

3. Um prestador de serviços de comunicação de dados que externaliza atividades deve garantir que essa externalização não reduza a capacidade ou os poderes para o exercício das funções dos quadros superiores ou do órgão de administração.

4. Um prestador de serviços de comunicação de dados continua a ser responsável por qualquer atividade externalizada e deve adotar medidas de caráter organizativo para garantir:

a) Que avalia se o prestador de serviços terceiro realiza as atividades objeto de subcontratação de modo eficaz e em cumprimento dos requisitos legislativos e regulamentares aplicáveis, dando uma resposta adequada às deficiências detetadas;

b) A identificação dos riscos relacionados com as atividades objeto de subcontratação e um acompanhamento periódico adequado;

c) Procedimentos de controlo adequados no que respeita às atividades subcontratadas, incluindo uma supervisão eficaz das atividades e dos seus riscos no âmbito do prestador de serviços de comunicação de dados;

d) Uma continuidade adequada das atividades subcontratadas;

Para efeitos da alínea d), o prestador de serviços de comunicação de dados deve obter informações sobre os planos de continuidade das atividades do terceiro prestador dos serviços, avaliar a sua qualidade e, se necessário, solicitar melhoramentos.

5. Um prestador de serviços de comunicação de dados deve assegurar que o terceiro prestador dos serviços coopera com a autoridade competente responsável pelo prestador de serviços de comunicação de dados no que respeita às atividades externalizadas.

6. Quando um prestador de serviços de comunicação de dados subcontratar qualquer função crítica, deve fornecer à autoridade competente do seu Estado-Membro de origem:

a) A identificação do terceiro prestador dos serviços;

b) As políticas e medidas organizacionais no que respeita à subcontratação e aos riscos que coloca, conforme especificado no n.º 4;

c) Relatórios internos ou externos sobre as atividades subcontratadas.

Para efeitos do primeiro parágrafo do n.º 6, uma função deve ser considerada crítica se uma deficiência ou falha no seu desempenho prejudicar significativamente o cumprimento continuado, pelo prestador de serviços de comunicação de dados, das condições e obrigações da sua autorização ou das suas outras obrigações decorrentes da Diretiva 2014/65/UE.

Artigo 7.º

Continuidade das atividades e mecanismos de salvaguarda

1. Um prestador de serviços de comunicação de dados deve utilizar sistemas e mecanismos adequados e suficientemente robustos para assegurar a continuidade e a regularidade da execução dos serviços prestados referidos na Diretiva 2014/65/UE.

2. Um prestador de serviços de comunicação de dados deve realizar análises periódicas, pelo menos anualmente, para avaliar as suas infraestruturas técnicas e as políticas e procedimentos associados, incluindo os planos de continuidade das atividades. Um prestador de serviços de comunicação de dados deve corrigir quaisquer deficiências detetadas durante a análise.

3. Um prestador de serviços de comunicação de dados deve dispor de planos de continuidade das atividades eficazes para fazer face a incidentes com perturbação das atividades, incluindo:

a) Os processos críticos para assegurar os serviços do prestador de serviços de comunicação de dados, incluindo procedimentos por fases para a resolução dos problemas, as atividades relevantes externalizadas ou as dependências em relação a prestadores externos;

b) Planos de continuidade específicos, que abranjam um conjunto adequado de cenários possíveis, a curto e a médio prazo, incluindo falhas do sistema, catástrofes naturais, perturbações nas comunicações, perda de pessoal fundamental e incapacidade para utilizar as instalações normalmente utilizadas;

c) Duplicação de componentes de equipamentos informáticos, por forma a permitir a comutação para uma infraestrutura de apoio, incluindo a conectividade de rede e os canais de comunicação;

d) Salvaguarda de dados fundamentais para a atividade comercial e informações atualizadas dos contactos necessários, a fim de garantir a comunicação no seio do prestador de serviços de comunicação de dados e entre este e os seus clientes;

e) Os procedimentos para a transição dos serviços de comunicação de dados para um sítio de salvaguarda e para a operação desses serviços a partir desse sítio;

f) Os prazos máximos aceitáveis de recuperação de funções críticas, que devem ser tão curtos quanto possível e, em qualquer caso, não superiores a seis horas, no caso dos sistemas de publicação autorizados (APA) e dos prestadores de informações consolidadas (CTP), e até ao fecho das operações do dia útil seguinte no caso dos sistemas de reporte autorizados (ARM);

g) Formação do pessoal em matéria do funcionamento dos planos de continuidade das atividades e funções dos indivíduos, incluindo o pessoal específico de segurança, que deverá estar pronto a reagir imediatamente a uma perturbação dos serviços.

4. Um prestador de serviços de comunicação de dados deve criar um programa para testar, analisar e, se necessário, alterar periodicamente os planos de continuidade das atividades.

5. Um prestador de serviços de comunicação de dados deve publicar no seu sítio *web* e informar de imediato a autoridade competente do seu Estado-Membro de origem e os seus clientes de quaisquer perturbações do serviço ou interrupções da ligação, bem como do prazo previsto para a retoma de um serviço regular.

6. No caso dos ARM, as notificações referidas no n.º 5 devem ser igualmente dirigidas a qualquer autoridade competente a quem o ARM apresente comunicações de transações.

Artigo 8.º

Testes e capacidade

1. Um prestador de serviços de comunicação de dados deve implementar metodologias de teste e desenvolvimento claramente delineadas, a fim de garantir que:

a) O funcionamento dos sistemas informáticos cumpre as obrigações regulamentares do prestador de serviços de comunicação de dados;

b) Os controlos da conformidade e de gestão do risco integrados nos sistemas informáticos funcionam como previsto;

c) Os sistemas informáticos podem continuar a funcionar eficazmente em qualquer momento.

2. Um prestador de serviços de comunicação de dados deve também utilizar as metodologias referidas no n.º 1 antes e após a implementação de eventuais atualizações dos sistemas informáticos.

3. Um prestador de serviços de comunicação de dados deve notificar de imediato a autoridade competente do seu Estado-Membro de origem de quaisquer alterações significativas planeadas do sistema informático, antes da sua implementação.

4. No caso dos ARM, as notificações referidas no n.º 3 devem ser igualmente dirigidas a qualquer autoridade competente a quem o ARM apresente comunicações de transações.

5. Um prestador de serviços de comunicação de dados deve criar um programa contínuo para rever periodicamente e, se necessário, modificar as metodologias de desenvolvimento e teste.

6. Um prestador de serviços de comunicação de dados deve realizar periodicamente testes de esforço, pelo menos anualmente. Um prestador de serviços de comunicação de dados deve incluir nos cenários adversos dos testes de esforço um comportamento imprevisível de elementos críticos constitutivos dos seus sistemas e linhas de comunicação. Os testes de esforço devem identificar de que forma os programas e equipamentos informáticos e as comunicações dão resposta às potenciais ameaças, especificando os sistemas incapazes de lidar com cenários adversos. Um prestador de serviços de comunicação de dados deve tomar as medidas necessárias para resolver as deficiências identificadas nesses sistemas.

7. Um prestador de serviços de comunicação de dados deve:

a) Ter capacidade suficiente para desempenhar as suas funções sem interrupções ou falhas, incluindo dados em falta ou incorretos;

b) Ser suficientemente modulável para responder, sem demora injustificada, a qualquer aumento da quantidade de informações a tratar e do número de pedidos de acesso por parte dos seus clientes.

Artigo 9.º

Segurança

1. Um prestador de serviços de comunicação de dados deve estabelecer e manter procedimentos e medidas de segurança física e eletrónica destinados a:

a) Proteger os seus sistemas informáticos contra a utilização abusiva ou o acesso não autorizado;

b) Minimizar os riscos de ataques aos sistemas informáticos, tal como definido no artigo 2.º, alínea a), da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho ([1]);

c) Impedir a divulgação não autorizada de informações confidenciais;

d) Garantir a segurança e a integridade dos dados.

2. Sempre que uma empresa de investimento («empresa declarante») utiliza um terceiro («empresa que apresenta a comunicação») para apresentar informações a um ARM em seu nome, o ARM deve ter em vigor procedimentos e medidas destinados a garantir que a empresa que apresenta a comunicação não tenha acesso a qualquer outra informação sobre a empresa declarante ou por esta apresentada ao ARM e que possa ter sido enviada pela empresa declarante ao ARM, diretamente ou através de outra empresa que apresenta a comunicação.

3. Um prestador de serviços de comunicação de dados deve estabelecer e manter as medidas e mecanismos necessários para identificar de imediato e gerir os riscos identificados no n.º 1.

4. No que respeita às violações das medidas de segurança física e eletrónica referidas nos n.ºs 1, 2 e 3, um prestador de serviços de comunicação de dados deve notificar imediatamente:

a) A autoridade competente do seu Estado-Membro de origem, fornecendo um relatório do incidente e indicando a sua natureza, as medidas adotadas para lidar com o mesmo e as iniciativas tomadas para evitar incidentes semelhantes;

b) Os seus clientes que tenham sido afetados pela quebra da segurança.

([1]) Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8).

5. No caso dos ARM, a notificação referida no n.º 4, alínea a), deve também ser efetuada a quaisquer outras autoridades competentes a quem o ARM apresente comunicações de transações.

Artigo 10.º

Gestão de informações incompletas ou potencialmente erróneas por parte dos APA e dos CTP

1. Os APA e os CTP devem estabelecer e manter mecanismos adequados para garantir que publicam com precisão os relatórios comerciais recebidos de empresas de investimento e, no caso dos CTP, de plataformas de negociação e APA, sem introduzirem quaisquer erros ou omitirem informações, e devem corrigir as informações sempre que tenham sido causadores desses erros ou omissões.

2. Os APA e os CTP devem monitorizar continuamente e em tempo real o desempenho dos seus sistemas informáticos, por forma a garantir que os relatórios comerciais recebidos foram corretamente publicados.

3. Os APA e os CTP devem executar conciliações periódicas entre os relatórios comerciais que recebem e os relatórios comerciais que publicam, verificando a correta publicação das informações.

4. Um APA deve acusar a receção de um relatório comercial à empresa de investimento declarante, incluindo o código de identificação da operação atribuído pelo APA. Um APA deve remeter para o código de identificação da operação em qualquer comunicação posterior com a empresa declarante relativa a um determinado relatório comercial.

5. Um APA deve estabelecer e manter mecanismos adequados para identificar, no momento da receção, relatórios comerciais que estejam incompletos ou que contenham informações que possam estar erradas. Estes mecanismos devem incluir alertas automáticos de preço e volume, tendo em conta:

a) O setor e o segmento em que o instrumento financeiro é negociado;

b) Os níveis de liquidez, incluindo os níveis de negociação históricos;

c) Índices de referência de preços e volume apropriados;

d) Se necessário, outros parâmetros, em função das características do instrumento financeiro.

6. Sempre que um APA determina que um relatório comercial que recebeu está incompleto ou contém informações que poderão ser erradas, não deve publicar esse relatório e deve alertar de imediato a empresa de investimento que apresentou o relatório comercial.

7. Em circunstâncias excecionais, os APA e os CTP devem apagar e alterar informações num relatório comercial a pedido da entidade que faculta as informações, quando essa entidade não puder apagar ou alterar as suas próprias informações por razões técnicas.

8. Os APA devem publicar políticas não discricionárias sobre o cancelamento de informações e alterações nos relatórios comerciais, que estabeleçam as sanções que os APA podem impor às empresas de investimento que fornecem relatórios comerciais nos casos em que as informações incompletas ou erróneas tenham conduzido ao cancelamento ou à alteração dos relatórios.

Artigo 11.º

Gestão de informações incompletas ou potencialmente erróneas por parte dos ARM

1. Um ARM deve estabelecer e manter mecanismos adequados para identificar relatórios comerciais que estejam incompletos ou que contenham erros manifestos causados pelos clientes. Um ARM deve efetuar a validação das comunicações de transações de acordo com os requisitos estabelecidos no artigo 26.º do Regulamento (UE) n.º 600/2014 relativamente aos campos, formatos e ao conteúdo dos campos em conformidade com o quadro 1 do anexo I do Regulamento Delegado (UE) 2017/590 da Comissão ([1]).

([1]) Regulamento Delegado (UE) 2017/590 da Comissão, de 28 de julho de 2016, que complementa o Regulamento (UE) n.o 600/2014 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação para a comunicação de informações sobre as transações às autoridades competentes (ver página 449 do presente Jornal Oficial).

2. Um ARM deve estabelecer e manter mecanismos adequados para identificar comunicações de transações que contenham erros ou omissões causados pelo próprio ARM e para corrigir, nomeadamente apagando ou alterando, tais erros ou omissões. Um ARM deve efetuar a validação do campo, do formato e do conteúdo dos campos em conformidade com o quadro 1 do anexo I do Regulamento Delegado (UE) 2017/590.

3. UM ARM deve monitorizar continuamente e em tempo real o desempenho dos seus sistemas de forma a garantir que uma comunicação de transação que recebeu foi devidamente enviada à autoridade competente em conformidade com o artigo 26.º do Regulamento (UE) n.º 600/2014.

4. Um ARM deve, a pedido da autoridade competente do seu Estado-Membro de origem ou da autoridade competente a quem o ARM apresenta comunicações de transações, executar conciliações periódicas entre as informações que recebe dos seus clientes ou que gera em nome desses clientes para fins de comunicação das transações e amostras de dados das informações fornecidas pela autoridade competente.

5. Quaisquer correções, incluindo anulações ou alterações das comunicações de transações, que não correspondam a uma correção de erros ou omissões causados por um ARM, só devem ser efetuadas a pedido de um cliente e em relação a uma determinada comunicação de transação. Sempre que um ARM anule ou altere uma comunicação de transação a pedido de um cliente, deve disponibilizar a comunicação atualizada ao cliente.

6. Sempre que um ARM, antes de apresentar a comunicação de transação, identifique um erro ou uma omissão causada por um cliente, não deve apresentar essa comunicação de transação e deve comunicar de imediato à empresa de investimento os pormenores do erro ou da omissão, por forma a permitir que o cliente envie um conjunto de informações corrigidas.

7. Sempre que um ARM tomar conhecimento de erros ou omissões causados pelo próprio ARM, deve enviar de imediato uma comunicação completa e correta.

8. Um ARM deve notificar imediatamente ao cliente os pormenores do erro ou da omissão e facultar-lhe uma comunicação de transação atualizada. Um ARM deve igualmente notificar imediatamente o erro ou a omissão à autoridade competente do seu Estado-Membro de origem e à autoridade competente a quem tenha enviado a comunicação de transação.

9. A obrigação de corrigir ou anular comunicações de transações incorretas ou de comunicar transações omissas não é extensível a erros ou omissões que tenham ocorrido mais de cinco anos antes da data em que o ARM teve conhecimento dos mesmos.

Artigo 12.º

Conectividade dos ARM

1. Um ARM deve dispor de políticas, mecanismos e capacidades técnicas para cumprir as especificações técnicas relativas à apresentação das comunicações de transações exigidas pela autoridade competente do seu Estado-Membro de origem e por outras autoridades competentes a quem o ARM envia comunicações de transações.

2. Um ARM deve dispor de políticas, mecanismos e capacidades técnicas adequadas para receber comunicações de transações de clientes e para transmitir informações de volta a esses mesmos clientes. O ARM deve fornecer ao cliente uma cópia das comunicações de transações que o ARM tenha apresentado à autoridade competente em nome do cliente.

Artigo 13.º

Outros serviços prestados pelos CTP

1. Um CTP pode prestar os seguintes serviços adicionais:

a) Fornecimento de dados relativos à transparência pré-negociação;

b) Fornecimento de dados históricos;

c) Fornecimento de dados de referência;

d) Prestação de serviços de investigação;

e) Tratamento, distribuição e comercialização de dados e estatísticas sobre instrumentos financeiros, plataformas de negociação e outros dados relacionados com o mercado;

f) Conceção, gestão, manutenção e comercialização de programas e equipamentos informáticos e de rede relacionados com a transmissão de dados e informações.

2. Um CTP pode prestar serviços diferentes dos especificados no n.º 1 que aumentem a eficiência do mercado, desde que tais serviços não impliquem riscos para a qualidade do sistema de prestação de informações consolidadas ou a independência do CTP que não possam ser adequadamente evitados ou atenuados.

CAPÍTULO III

MECANISMOS DE PUBLICAÇÃO

(Artigo 64.º. n.ºs 1 e 2, e artigo 65.º, n.º 1, da Diretiva 2014/65/UE)

Artigo 14.º

Leitura por máquina

1. Os APA e os CTP devem publicar as informações a disponibilizar ao público nos termos dos artigos 64.º, n.º 1, e 65.º, n.º 1, da Diretiva 2014/65/UE, num formato passível de leitura por máquina.

2. Os CTP devem publicar as informações a disponibilizar nos termos do artigo 65.º, n.º 2, da Diretiva 2014/65/UE, num formato passível de leitura por máquina.

3. As informações só são consideradas publicadas num formato passível de leitura por máquina se estiverem preenchidas todas as seguintes condições:

a) As informações estão num formato eletrónico destinado a ser direta e automaticamente lido por um computador;

b) As informações estão armazenadas numa arquitetura informática adequada nos termos do artigo 8.º, n.º 7, que permite o acesso automático;

c) A arquitetura é suficientemente robusta para assegurar a continuidade e regularidade da execução dos serviços prestados e assegura um acesso adequado em termos de rapidez;

d) As informações podem ser acedidas, lidas, utilizadas e copiadas por um programa informático gratuito e disponível ao público.

Para efeitos da alínea a) do primeiro parágrafo, o formato eletrónico deve ser especificado através de normas livres, genéricas e abertas.

4. Para efeitos do n.º 3, alínea a), o formato eletrónico deve incluir o tipo de ficheiros ou de mensagens, as regras para a respetiva identificação, bem como o nome e o tipo de dados dos campos que contêm.

5. Os APA e os CTP devem:

a) Disponibilizar ao público instruções que expliquem como e onde aceder e utilizar facilmente os dados, incluindo a identificação do formato eletrónico;

b) Tornar públicas quaisquer alterações das instruções referidas na alínea a), pelo menos três meses antes da sua entrada em vigor, exceto se existir uma necessidade urgente e devidamente justificada de que essas alterações das instruções entrem em vigor mais rapidamente;

c) Incluir uma ligação para as instruções referidas na alínea a) na página inicial do seu sítio *web*.

Artigo 15.º

Âmbito de aplicação do sistema de prestação de informações consolidadas para ações, certificados de depósito, ETF, certificados e outros instrumentos financeiros similares

1. Um CTP deve incluir no seu fluxo eletrónico de dados os dados tornados públicos em aplicação dos artigos 6.º e 20.º do Regulamento (UE) n.º 600/2014 relativos a todos os instrumentos financeiros referidos nesses artigos.

2. Quando um novo APA ou uma nova plataforma de negociação entrar em funcionamento, um CTP deve incluir os dados tornados públicos por esse APA ou plataforma de negociação no fluxo eletrónico de dados do seu sistema de prestação de informações consolidadas o mais rapidamente possível e, em qualquer caso, o mais tardar seis meses após o início das operações do APA ou da plataforma de negociação.

Artigo 16.º

Identificação de relatórios comerciais originais e duplicados em relação a ações, certificados de depósito, ETF, certificados e outros instrumentos financeiros similares

1. Quando um APA publica um relatório comercial que é um duplicado, deve inserir o código «DUPL» num campo de reimpressão, para permitir que os destinatários dos dados distingam entre o relatório comercial original e quaisquer duplicados desse mesmo relatório.

2. Para efeitos do n.º 1, um APA deve exigir que cada empresa de investimento cumpra uma das seguintes condições:

a) Declarar que apenas comunica transações de um determinado instrumento financeiro através desse APA;

b) Utilizar um mecanismo de identificação que assinala um relatório como original («ORGN») e todos os outros relatórios relativos à mesma operação como duplicados («DUPL»).

Artigo 17.º

Publicação de relatórios originais em relação a ações, certificados de depósito, ETF, certificados e outros instrumentos financeiros similares

Um CTP não deve consolidar os relatórios comerciais com o código «DUPL» no campo de reimpressão.

Artigo 18.º

Dados que devem ser publicados pelo APA

1. Um APA deve tornar públicos:

a) No caso de operações executadas relativamente a ações, certificados de depósito, fundos de índices cotados (ETF), certificados e outros instrumentos financeiros similares, os dados de uma transação especificados no quadro 2 do anexo I do Regulamento Delegado (UE) 2017/587, utilizando os códigos adequados enunciados no quadro 3 do anexo 1 do Regulamento Delegado (UE) 2017/587;

b) No caso de operações executadas relativamente a obrigações, produtos financeiros estruturados, licenças de emissão e derivados, os dados de uma transação especificados no quadro 1 do anexo II do Regulamento Delegado (UE) 2017/583, utilizando os códigos adequados enunciados no quadro 2 do anexo II do Regulamento Delegado (UE) 2017/583.

2. Em caso de publicação de informações sobre o momento em que a transação foi comunicada, um APA deve incluir a data e a hora, ao segundo, em que publica a operação.

3. Em derrogação do n.º 2, um APA que publica informações relativas a uma transação executada num sistema eletrónico deve incluir a data e a hora, ao milissegundo, da publicação dessa transação no seu relatório comercial.

4. Para efeitos do n.º 3, entende-se por «sistema eletrónico» um sistema em que as ordens são negociáveis por via eletrónica ou são negociáveis fora do sistema, desde que sejam publicitadas através do sistema.

5. Os carimbos de data/hora referidos nos n.ºs 2 e 3 não devem divergir em mais do que um segundo ou milissegundo, respetivamente, do Tempo Universal Coordenado (UTC) emitido e mantido por um dos centros de definição do tempo listados no último relatório anual sobre atividades de tempo do *Bureau International des Poids et Mesures*.

Artigo 19.º

Não discriminação

Os APA e os CTP devem assegurar que as informações que devem ser tornadas públicas são enviadas através de todos os canais de distribuição ao mesmo tempo, nomeadamente quando as informações são tornadas públicas de forma tão próxima do tempo real quanto tecnicamente possível ou 15 minutos após a primeira publicação.

Artigo 20.º

Dados que devem ser publicados pelo CTP

Um CTP deve tornar públicos:

a) No caso de transações executadas relativamente a ações, certificados de depósito, ETF, certificados e outros instrumentos financeiros similares, os pormenores de uma transação especificados no quadro 2 do anexo I do Regulamento Delegado (UE) 2017/587 e utilizar os códigos adequados enunciados no quadro 3 do anexo I do Regulamento Delegado (UE) 2017/587;

b) No caso de transações executadas relativamente a obrigações, produtos financeiros estruturados, licenças de emissão e derivados, os pormenores de uma transação especificados no quadro 1 do anexo II do Regulamento Delegado (UE) 2017/583 e utilizar os códigos adequados enunciados no quadro 2 do anexo II do Regulamento Delegado (UE) 2017/583.

Artigo 21.º

Entrada em vigor e aplicação

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

O presente regulamento é aplicável a partir da data que consta do artigo 93.º, n.º 1, segundo parágrafo, da Diretiva 2014/65/UE.

No entanto, o artigo 14.º, n.º 2, e o artigo 20.º, alínea b), são aplicáveis a partir do primeiro dia do nono mês a contar da data de entrada em aplicação da Diretiva 2014/65/UE.

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

Feito em Bruxelas, em 2 de junho de 2016.

Pela Comissão

O Presidente

Jean-Claude JUNCKER