Este texto constitui um instrumento de documentação e não tem qualquer efeito jurídico. As Instituições da União não assumem qualquer responsabilidade pelo respetivo conteúdo. As versões dos atos relevantes que fazem fé, incluindo os respetivos preâmbulos, são as publicadas no Jornal Oficial da União Europeia e encontram-se disponíveis no EUR-Lex. É possível aceder diretamente a esses textos oficiais através das ligações incluídas no presente documento

►**B**

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)

(JO L 87 de 31.3.2017, p. 126)

Alterado por:

		Jornal Oficial		
		n.°	página	data
►**M1**	Regulamento Delegado (UE) 2018/63 da Comissão de 26 de setembro de 2017	L 12	2	17.1.2018

▼B

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)

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;

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,

▼B

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;

▼B

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.

▼B

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

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;

▼B

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

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

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

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.

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.

([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).

▼B

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.

▼B

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]).

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.

([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).

▼B

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.

▼B

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

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.

▼M1

Artigo 15.º-A

Âmbito de aplicação do sistema de prestação de informações consolidadas para obrigações, produtos financeiros estruturados, licenças de emissão e derivados

1. Um CTP deve incluir no seu fluxo eletrónico de dados os dados relativos a uma ou mais das seguintes categorias de ativos:

a) Obrigações, excluindo mercadorias negociadas em bolsa (ETC) e notas negociadas em bolsa (ETN);

b) Tipos de obrigações ETC e ETN;

c) Produtos financeiros estruturados (SFP);

d) Derivados titularizados;

e) Derivados de taxas de juro;

f) Derivados cambiais;

g) Derivados de instrumentos de capital próprio;

h) Derivados de mercadorias;

i) Derivados de crédito;

▼**M1**

j) Contratos sobre diferenças;

k) Derivados C10;

l) Derivados de licenças de emissão;

m) Licenças de emissão.

2. Um CTP deve incluir no seu fluxo eletrónico de dados os dados tornados públicos em aplicação dos artigos 10.º e 21.º do Regulamento (UE) n.º 600/2014 por forma a cumprir ambos os seguintes rácios de cobertura:

a) O número das transações publicadas pelo CTP numa das categoria de ativos enumeradas no n.º 1 representa, pelo menos, 80 % do número total das transações na categoria de ativos relevante publicadas na União por todos os APA e todas as plataformas de negociação durante o período de cálculo a que se refere o n.º 3;

b) O volume das transações publicadas pelo CTP numa das categoria de ativos enumeradas no n.º 1 representa, pelo menos, 80 % do volume total das transações na categoria de ativos relevante publicadas na União por todos os APA e todas as plataformas de negociação durante o período de avaliação a que se refere o n.º 3.

Para efeitos da alínea b), o volume de transações é calculado de acordo com a medida de volume indicada no quadro 4 do anexo II do Regulamento Delegado (UE) 2017/583 da Comissão ([1]).

3. Um CTP deve calcular os rácios de cobertura estabelecidos no n.º 2 semestralmente, com base em dados que cubram os 6 meses anteriores. Os períodos de cálculo têm início em 1 de janeiro e 1 de julho de cada ano. O primeiro período cobre os seis primeiros meses do ano de 2019.

4. Um CTP deve assegurar que cumpre os rácios mínimos de cobertura estabelecidos no n.º 2 o mais rapidamente possível, e, em qualquer caso, o mais tardar:

a) no dia 31 de janeiro do ano civil que se segue ao período entre 1 de janeiro e 30 de junho;

b) no dia 31 de julho do ano civil que se segue ao período entre 1 de julho e 31 de dezembro.

([1]) 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 (JO L 87 de 31.3.2017, p. 229).

▼B

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.

▼B

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.

▼**M1**

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 de 3 de janeiro de 2018.

No entanto, o artigo 15.º-A, n.º 4, é aplicável a partir de 1 de janeiro de 2019, e os artigos 14.º, n.º 2, 15.º, n.ºs 1, 2 e 3, e 20.º, alínea b), são aplicáveis a partir de 3 de setembro de 2019.

▼**B**

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