Jornal Oficial
da União Europeia

PT
Série L

2024/1942

20.12.2024

REGULAMENTO DE EXECUÇÃO (UE) 2024/1942 DA COMISSÃO

de 5 de julho de 2024

que estabelece procedimentos comuns e regras detalhadas para o acesso e o tratamento de informações eletrónicas sobre o transporte de mercadorias pelas autoridades competentes em conformidade com o Regulamento (UE) 2020/1056 do Parlamento Europeu e do Conselho

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) 2020/1056 do Parlamento Europeu e do Conselho, de 15 de julho de 2020, relativo a informações eletrónicas sobre o transporte de mercadorias ([1]), nomeadamente o artigo 8.º,

Considerando o seguinte:

(1) O Regulamento (UE) 2020/1056 exige que os Estados-Membros assegurem que todas as suas autoridades competentes tenham acesso a informações eletrónicas sobre o transporte de mercadorias («eFTI»), em conformidade com procedimentos comuns e regras detalhadas, incluindo especificações técnicas comuns e procedimentos para o tratamento de informações regulamentares e para a comunicação com os operadores económicos no que respeita a essas informações.

(2) A fim de estabelecer estes procedimentos e regras comuns, nos termos do artigo 8.º do Regulamento (UE) 2020/1056, a Comissão deve enumerar os principais componentes de tecnologias da informação e comunicação («TIC») do ambiente de intercâmbio eFTI a fornecer pelos Estados-Membros e indicar as suas especificações funcionais e técnicas.

(3) Para assegurar flexibilidade na aplicação destes procedimentos comuns e regras detalhadas, os Estados-Membros devem poder decidir como organizar o fornecimento dos componentes de TIC, desde que esses componentes cumpram as respetivas especificações funcionais e técnicas estabelecidas no presente regulamento. Mais especificamente, os Estados-Membros podem decidir criar componentes separados, componentes integrados num único componente ou ainda vários componentes diferentes que executem as respetivas funcionalidades. Podem também criar vários componentes que executem o mesmo conjunto de funções.

(4) Os Estados-Membros devem poder reutilizar componentes de TIC existentes que já tenham desenvolvido para outros serviços públicos digitais, na medida em que esses componentes já forneçam ou sejam ajustados para fornecer as funcionalidades necessárias em conformidade com as especificações, incluindo os requisitos técnicos, se for caso disso, estabelecidos no presente regulamento. Os Estados-Membros deverão também poder optar por criar, desenvolver e manter um ou vários componentes de TIC previstos no presente regulamento em conjunto com outros Estados-Membros.

(5) Cada Estado-Membro deverá ser responsável por garantir a manutenção e a segurança dos componentes de TIC por si criados ou pelos quais são responsáveis, nomeadamente garantir a segurança e a confidencialidade das informações tratadas por esses componentes. Se vários Estados-Membros decidirem criar e gerir conjuntamente alguns destes componentes, devem assegurar que as suas responsabilidades respetivas são estabelecidas em acordos ou memorandos de entendimento adequados.

(6) Nos termos do Regulamento (UE) 2020/1056, todas as comunicações no ambiente de intercâmbio eFTI devem ser efetuadas através de ligações seguras entre partes devidamente identificadas e autorizadas. Por conseguinte, as especificações funcionais e técnicas comuns estabelecidas no presente regulamento devem assegurar o cumprimento desses requisitos para todas as comunicações realizadas entre os participantes no ambiente de intercâmbio eFTI através de componentes de TIC, incluindo com as plataformas eFTI.

([1]) JO L 249 de 31.7.2020, p. 33.

(7) Prevê-se que o número de participantes no ambiente de intercâmbio eFTI seja elevado, tanto a nível das autoridades competentes como a nível dos operadores económicos interessados, que terão a liberdade de escolher que plataformas eFTI decidem utilizar. Por conseguinte, seria necessário estabelecer e manter um número adequado de ligações seguras, autenticadas e autorizadas entre os componentes de TIC do ambiente de intercâmbio eFTI. Para reduzir os custos associados a um número tão elevado de ligações, alguns dos componentes de TIC do ambiente de intercâmbio eFTI a estabelecer pelos Estados-Membros deverão mediar esse intercâmbio desempenhando uma função de porta de acesso, mantendo simultaneamente um elevado nível de segurança e o cumprimento das autorizações aplicáveis.

(8) Estas portas, ou «portas eFTI» (*eFTI Gate*), devem mediar o intercâmbio de informações regulamentares sobre o transporte de mercadorias entre os operadores económicos interessados e as autoridades competentes. As portas eFTI devem assegurar ligações seguras e autenticadas aos componentes de TIC que mediam o acesso de agentes individuais a nível das autoridades competentes de um determinado Estado-Membro, por um lado, e das plataformas eFTI que detêm os dados aos quais esses agentes necessitariam de aceder, por outro. Não devem ser armazenados ou tratados dados eFTI, com exceção dos metadados ligados ao tratamento de dados eFTI, tais como identificadores ou registos de operações, e apenas para fins legítimos, como o encaminhamento, a validação ou adaptação de formatos e para fins de acompanhamento ou estatísticos.

(9) Além disso, a fim de reduzir os custos inerentes ao estabelecimento de ligações entre as plataformas eFTI e uma porta eFTI, em especial para os operadores económicos, mas também para as autoridades competentes, tal como previsto no artigo 8.º, n.º 2, do Regulamento (UE) 2020/1056, as plataformas eFTI devem ser obrigadas a estabelecer e manter uma ligação segura e autenticada a uma única porta eFTI. Esta porta eFTI deve, portanto, mediar a ligação a todas as autoridades competentes de todos os Estados-Membros, através de uma rede de ligações seguras e autenticadas entre as diferentes portas eFTI.

(10) Tendo em conta o requisito previsto no artigo 11.º do Regulamento (UE) 2020/1056 de que os Estados-Membros mantenham uma lista atualizada das plataformas eFTI titulares de uma certificação válida emitida por um organismo de avaliação da conformidade acreditado no seu Estado-Membro, esta ligação única de uma plataforma eFTI à rede de portas eFTI deve ser estabelecida com a porta eFTI do Estado-Membro em que a certificação dessa plataforma foi emitida. Tal facilitaria e tornaria o processo de verificação da validade da certificação de uma plataforma eFTI menos oneroso, no âmbito do processo de garantia da segurança e autenticidade da comunicação com uma plataforma eFTI. No entanto, para ter em conta situações em que nenhum organismo de avaliação da conformidade tenha sido acreditado para certificar plataformas eFTI num Estado-Membro, as plataformas eFTI devem poder estabelecer a sua ligação única à porta eFTI desse Estado-Membro, mesmo se tiverem obtido a certificação noutro Estado-Membro.

(11) A fim de assegurar um elevado nível de confiança no ambiente de intercâmbio eFTI, os Estados-Membros devem continuar a ser responsáveis por assegurar que todos os acessos ao ambiente de intercâmbio eFTI por parte das suas autoridades competentes seja devidamente identificado, autenticado e autorizado. Os Estados-Membros devem assegurar que o acesso e o tratamento, por parte das autoridades competentes, dos dados disponibilizados pelos operadores económicos nas plataformas eFTI só são permitidos após a devida identificação e autenticação da identidade dos agentes responsáveis, bem como a devida autorização com base nos direitos de acesso e tratamento atribuídos aos agentes, com base nas suas respetivas responsabilidades em relação às disposições nacionais e da UE abrangidas pelo âmbito de aplicação do Regulamento (UE) 2020/1056. Para o efeito, os Estados-Membros devem assegurar que todas as autoridades competentes criem e mantenham registos atualizados dos direitos de acesso e de tratamento de cada agente responsável e que todos os pedidos de acesso e tratamento de dados eFTI incluam referências aos direitos de acesso e de tratamento do agente responsável pelo pedido. Estes direitos de acesso e de tratamento devem ser expressos como referências codificadas para minimizar a transferência dos dados pessoais dos agentes, tal como definido no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]). Os Estados-Membros devem também assegurar que as suas autoridades competentes tomam todas as medidas necessárias, como a realização de testes, ações de formação e auditorias, para assegurar que os seus agentes acedem aos dados e os tratam em conformidade com as regras nacionais e da UE aplicáveis em matéria de privacidade dos dados e confidencialidade comercial.

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

(12) O Regulamento (UE) 2020/1056 exige que os operadores económicos interessados comuniquem às autoridades competentes a «ligação eletrónica única de identificação» para os dados eFTI legíveis por máquina correspondentes às informações regulamentares. Do ponto de vista processual, esta comunicação deve ser feita de duas formas e os componentes de TIC a criar pelos Estados-Membros devem ser compatíveis com ambos os procedimentos. As autoridades competentes devem poder escolher qualquer um destes dois procedimentos ao pedirem acesso aos dados eFTI para efetuar verificações das informações regulamentares.

(13) Em primeiro lugar, em conformidade com os atuais procedimentos de verificação da conformidade em suporte de papel, os operadores económicos interessados devem poder comunicar diretamente à autoridade competente a ligação eletrónica de identificação única durante os controlos realizados com presença física, quer durante a operação de transporte, quer durante os controlos realizados nas instalações do operador económico, se as disposições nacionais ou da UE previrem a possibilidade de controlos após a conclusão das operações de transporte. Para facilitar o tratamento por parte das autoridades competentes, a ligação eletrónica única de identificação deve ser comunicada num formato legível por máquina, como um código de barras ou um código QR, apresentado no ecrã de um dispositivo eletrónico portátil, como um telemóvel ou um táblete, ou impresso em papel. As autoridades dos Estados-Membros devem poder decidir aceitar que, durante os controlos físicos das operações de transporte em curso, o operador económico possa, a título excecional, comunicar a ligação eletrónica única de identificação por correio eletrónico ou outra aplicação de mensagens eletrónicas, em situações em que a ligação não possa ser diretamente exibida pelo operador num ecrã ou em papel. Para os controlos realizados nas instalações dos operadores económicos, quando o número de operações de transporte a inspecionar for substancialmente mais elevado, as autoridades competentes devem poder optar por receber as ligações eletrónicas únicas de identificação por correio eletrónico ou através de outra aplicação de mensagens eletrónicas, a fim de facilitar e otimizar o tratamento dessas ligações. A escolha destes meios de comunicação adicionais deve continuar a ser da competência das respetivas autoridades competentes.

(14) Em segundo lugar, e para tornar o processo mais compatível com um futuro em que os processos sejam cada vez mais automatizados, os operadores económicos devem comunicar a ligação eletrónica única de identificação publicando-a num repositório ou registo eletrónico, juntamente com determinados identificadores, como a identificação única do meio de transporte, derivados do conjunto de dados eFTI associado a essa ligação eletrónica única de identificação. As autoridades competentes poderão então obter essa ligação do registo realizando uma consulta com base nesses identificadores. Tal permitiria às autoridades competentes verificar as informações sobre as mercadorias transportadas num camião, comboio ou batelão sem parar ou embarcar fisicamente no meio de transporte e, se for caso disso, aplicar medidas de acompanhamento em conformidade com a legislação nacional. Permitiria igualmente às autoridades competentes obter de forma mais fácil ou fiável informações sobre várias operações de transporte efetuadas por um determinado meio de transporte, num determinado período de tempo, como no caso dos controlos de cabotagem rodoviária, em conformidade com as disposições do Regulamento (CE) n.º 1072/2009 do Parlamento Europeu e do Conselho ([3]).

(15) A fim de garantir a interoperabilidade e a segurança do intercâmbio de informações entre as portas eFTI criadas pelos diferentes Estados-Membros, e entre as portas eFTI e as plataformas eFTI, deve ser utilizado no ambiente eFTI um conjunto de normas e especificações harmonizadas para o intercâmbio de mensagens, incluindo a configuração de acordos de intercâmbio de mensagens, processos operacionais, formatos de dados, identificadores e certificados de segurança. Os Estados-Membros deverão também chegar a acordo sobre procedimentos seguros para o intercâmbio dos certificados de segurança, nomeadamente através de um sistema personalizado ou de um protocolo seguro de transferência de ficheiros.

(16) A fim de reduzir os custos e o tempo necessário para criar as portas eFTI e os outros componentes de TIC, os Estados-Membros devem, na medida do possível, basear-se em normas abertas mantidas por organizações europeias ou internacionais e em soluções reutilizáveis. Para os formatos de intercâmbio de mensagens, as normas abertas internacionalmente mais utilizadas são XML e JSON. Embora o JSON seja um formato mais recente e, em certos aspetos, mais simples de implementar, o formato XML é o formato mais comum utilizado pelos sistemas de TIC das autoridades competentes na maioria dos Estados-Membros. Por conseguinte, a fim de permitir que os Estados-Membros reutilizem soluções existentes e reduzam assim os seus custos iniciais de implementação, todas as comunicações entre as portas eFTI e entre as portas eFTI e as plataformas eFTI devem ser efetuadas utilizando um único formato de intercâmbio de mensagens, o XML. Do mesmo modo, as normas para o intercâmbio seguro de mensagens mantidas pela Comissão como parte do módulo digital eDelivery ([4]) e, em particular, do perfil AS4 eDelivery, proporcionam uma solução técnica eficiente em termos de custos que os Estados-Membros já têm experiência em implementar.

([3]) Regulamento (CE) n.º 1072/2009 do Parlamento Europeu e do Conselho, de 21 de outubro de 2009, que estabelece regras comuns para o acesso ao mercado do transporte internacional rodoviário de mercadorias (JO L 300 de 14.11.2009, p. 72).

([4]) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

(17) Ao mesmo tempo, os Estados-Membros devem poder reutilizar normas e soluções de intercâmbio de mensagens já utilizadas noutros serviços públicos digitais para comunicação entre a porta eFTI e as plataformas eFTI criadas nesse Estado-Membro, além do eDelivery. Os requisitos detalhados e as normas subjacentes a essas soluções devem ser disponibilizados ao público para permitir a sua implementação por parte de programadores de plataformas eFTI interessados e para permitir que os organismos de avaliação da conformidade acreditados avaliem a sua conformidade com as especificações.

(18) Do mesmo modo, a fim de permitir que os agentes das autoridades competentes utilizem os componentes de TIC que constituem o ponto de acesso, ou os «pontos de acesso das autoridades», ao ambiente eFTI, os Estados-Membros deverão poder utilizar as soluções eletrónicas existentes que asseguram a identificação e a autenticação da identidade dos agentes quando acedem a outros serviços públicos digitais nacionais que dão acesso a dados pessoais ou comerciais de terceiros. Estas soluções devem basear-se, quando disponíveis, nos meios de identificação eletrónica estabelecidos nos termos do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([5]).

(19) No mesmo espírito, os Estados-Membros devem poder reutilizar quaisquer componentes existentes dos sistemas de TIC das suas autoridades competentes que desempenhem funções semelhantes às especificadas no presente regulamento, tais como registos de autorizações, desde que estes sejam adaptados em conformidade com os requisitos específicos estabelecidos no presente regulamento.

(20) Para simplificar a utilização do ambiente de intercâmbio eFTI por parte dos agentes das autoridades competentes e facilitar a sua análise dos dados eFTI disponibilizados pelos operadores económicos numa plataforma eFTI, os Estados-Membros devem poder adaptar a aplicação e a sua interface gráfica de utilizador às necessidades dos seus agentes. Os Estados-Membros devem também poder introduzir funcionalidades adicionais que apoiem as aplicações dos utilizadores, tais como a utilização de algoritmos inteligentes que possam pré-processar os dados eFTI, combinando-os igualmente com informações de outras fontes eletrónicas, se assim o desejarem.

(21) Para um funcionamento contínuo e harmonioso do ambiente eFTI, quaisquer problemas operacionais que surjam relacionados com os componentes de TIC criados pelos Estados-Membros devem ser rapidamente resolvidos. Para ajudar a assegurar que tal acontece, os Estados-Membros e a Comissão devem criar uma rede de assistência técnica, composta por serviços de assistência específicos a nível nacional e da União, respetivamente. Esta rede deve estabelecer procedimentos de comunicação claros e assegurar períodos mínimos de disponibilidade sincronizada, a fim de permitir uma reação rápida a eventuais incidentes e períodos de indisponibilidade que possam afetar o funcionamento do ambiente de intercâmbio eFTI. Estes pontos de contacto de assistência técnica deverão dispor de competências e recursos humanos e financeiros suficientes para poderem desempenhar as suas funções. Com base em relatórios de atividades, os serviços de assistência podem publicar informações agregadas em painéis de informações específicos do serviço de assistência. Os períodos mínimos de disponibilidade comum dos serviços de assistência devem ser revistos periodicamente, a fim de permitir ajustar a sua atividade e uma alocação eficaz dos recursos.

(22) Os componentes de TIC a criar pelos Estados-Membros funcionarão como componentes integrantes do ambiente mais vasto de intercâmbio eFTI. Isto significa que a criação e a manutenção destes componentes devem assentar em esforços coordenados, com base numa interpretação harmonizada das especificações estabelecidas no presente regulamento. Para o efeito, os Estados-Membros devem igualmente criar uma rede de apoio operacional, em cooperação com a Comissão, sob a forma de um grupo específico de peritos. A fim de aproveitar os conhecimentos especializados e a experiência desenvolvidos no âmbito do Fórum de Transportes e Logística Digital (DTLF), ou seja, o grupo de peritos criado pela Comissão ([6]) para prestar assistência no desenvolvimento e na execução das atividades e programas da União destinados à digitalização do setor dos transportes e da logística, esse grupo de peritos específico deve ser criado como um subgrupo do DTLF.

(23) Para facilitar os esforços de execução dos Estados-Membros e assegurar a aplicação uniforme destas especificações, prevê-se complementar o presente regulamento com documentos de apoio técnico mais detalhados e não vinculativos, elaborados pela Comissão em cooperação com os Estados-Membros no âmbito deste grupo específico de peritos.

([5]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

([6]) Decisão C(2018) 5921 da Comissão, de 13 de setembro de 2018, que cria o grupo de peritos sobre o transporte de mercadorias e a logística digitais: o Fórum de Transporte e Logística Digital (DTLF).

(24) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité de Facilitação Digital dos Transportes e do Comércio,

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Ambiente de intercâmbio eFTI», o conjunto de componentes de TIC utilizados para o intercâmbio de dados em conformidade com o Regulamento (UE) 2020/1056 e com os atos de execução e delegados adotados nos termos desse regulamento;

2) «Componente de TIC», uma unidade material (hardware) ou imaterial (software), ou um conjunto dessas unidades, utilizados para executar funcionalidades específicas que permitam a comunicação eletrónica de dados;

3) «Agente da autoridade competente», uma pessoa singular com direito de acesso e tratamento dos requisitos de informações regulamentares a que se refere o artigo 2.º, n.º 1, do Regulamento (UE) 2020/1056, em nome de uma autoridade competente de um Estado-Membro;

4) «Dados eFTI», os dados que correspondem a informações regulamentares, quando disponibilizados pelos operadores económicos numa plataforma eFTI em conformidade com o Regulamento (UE) 2020/1056;

5) «Pedido de acesso a dados eFTI», um pedido, em nome de uma autoridade competente, para receber os dados eFTI disponibilizados pelos operadores económicos numa plataforma eFTI;

6) «Comunicação de seguimento», uma comunicação entre as autoridades competentes e os operadores económicos interessados relativa às informações disponibilizadas pelos operadores económicos numa plataforma eFTI, na sequência de uma verificação da conformidade dessas informações por parte de um agente da autoridade competente, conforme comunicadas em resposta a um pedido de acesso a dados eFTI. Esta comunicação de seguimento pode consistir num pedido de dados eFTI em falta ou de informações relacionadas com as medidas de acompanhamento tomadas pela autoridade competente em conformidade com as disposições nacionais aplicáveis;

7) «Direitos de acesso», as autorizações concedidas a um agente da autoridade competente para realizar operações relacionadas com um ou mais subconjuntos de dados eFTI;

8) «Direitos de tratamento», as operações ou conjuntos de operações que um agente da autoridade competente está autorizado a realizar num subconjunto específico de dados eFTI recebido em resposta a um pedido de acesso a dados eFTI;

9) «Meio de identificação eletrónica», uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação por um serviço em linha;

10) «Referências de identificação», um número de identificação pessoal ou uma referência codificada que permite a identificação única de um agente da autoridade competente;

11) «Ponto de acesso da autoridade (AAP)», um componente de TIC ou um conjunto de componentes de TIC que executam as funcionalidades estabelecidas no artigo 4.º;

12) «Porta eFTI» (*eFTI Gate*), um componente de TIC ou um conjunto de componentes de TIC que executam as funcionalidades estabelecidas no artigo 6.º;

13) «Porta requerente», uma porta eFTI que processa um pedido de acesso a dados eFTI apresentado através de um AAP ligado ou integrado nessa porta eFTI;

14) «Porta destinatária», uma porta eFTI que processa um pedido de acesso a dados eFTI recebido de uma porta requerente;

15) «eDelivery», um conjunto de especificações e normas técnicas para o intercâmbio de mensagens eletrónicas desenvolvido pela Comissão no âmbito do programa do Mecanismo Interligar a Europa ([7]) e prosseguido no âmbito do programa Europa Digital ([8]);

16) «Ponto de acesso eDelivery», um componente de comunicação que faz parte do serviço de envio eletrónico eDelivery baseado em especificações e normas técnicas;

17) «Descoberta estática», um mecanismo que permite a um ponto de acesso eDelivery obter os dados de ligação de outro ponto de acesso eDelivery sem recorrer a sistemas de terceiros;

18) «Descoberta dinâmica», um mecanismo que permite a um ponto de acesso eDelivery obter os dados de ligação de outro ponto de acesso eDelivery realizando uma pesquisa desses dados num sistema de terceiros;

19) «Chaves de segurança», pares de chaves criptográficas públicas e privadas, geradas por algoritmos criptográficos, sob a forma de números muito elevados, que têm uma relação única entre si;

20) «Certificado de segurança», um documento digital emitido por uma autoridade de certificação, utilizado para estabelecer um canal de comunicação eletrónica seguro entre duas partes. Este documento inclui a chave de segurança pública e informações sobre o objeto do certificado;

21) «Autoridade de certificação», uma entidade responsável pela gestão do ciclo de vida dos certificados digitais, o que pode incluir processos de registo e processos de emissão, entrega, ativação, suspensão, revogação, renovação ou reativação dos certificados de segurança;

22) «Aplicação de utilizador», um componente de TIC que executa as funcionalidades estabelecidas no artigo 7.º;

23) «Documentos de orientação técnica», um conjunto de documentos técnicos detalhados e não vinculativos, elaborados pela Comissão em cooperação com os Estados-Membros no âmbito do grupo de trabalho referido no artigo 13.º.

Artigo 2.º

Medidas Comuns

1. Os Estados-Membros asseguram que as suas autoridades competentes têm acesso a sistemas de TIC capazes de processar as ligações eletrónicas únicas de identificação (UIL) comunicadas pelos operadores económicos nos termos do artigo 4.º, n.º 3, do Regulamento (UE) 2020/1056, e que permitem que os agentes das suas autoridades competentes acedam e efetuem o tratamento dos dados eFTI utilizando qualquer um dos seguintes procedimentos:

a) Processando diretamente a UIL, quando comunicada pelo operador económico num formato legível por máquina, apresentando-a no ecrã de um dispositivo eletrónico ou impressa num suporte físico, como papel, ou, enviando-a por correio eletrónico ou através de outra aplicação de mensagens eletrónicas, se a autoridade competente optar por autorizar essa comunicação;

b) Obtendo em primeiro lugar a UIL, tal como comunicada pelos operadores económicos através da publicação num registo específico, por meio de um identificador único associado a uma operação de transporte.

2. Os Estados-Membros asseguram que os sistemas de TIC a que se refere o n.º 1 dispõem, pelo menos, das seguintes funcionalidades:

a) Identificação devidamente autenticada e devida autorização dos agentes das autoridades competentes de cada vez que um agente apresenta um pedido de acesso a dados eFTI;

b) Mediação dos pedidos de acesso a dados eFTI apresentados pelos agentes das autoridades competentes, incluindo obtenção das informações pedidas à plataforma ou plataformas eFTI adequadas, através de ligações seguras a essas plataformas.

([7]) https://digital-strategy.ec.europa.eu/pt/activities/cef-digital.
([8]) https://digital-strategy.ec.europa.eu/pt/activities/digital-programme.

3. Para implementar as funcionalidades enumeradas no n.º 2, esses sistemas de TIC incluem, pelo menos, os seguintes componentes:

a) Pontos de acesso das autoridades (AAP);

b) Um registo de autorizações;

c) Portas eFTI;

d) Um mecanismo de pesquisa;

e) Uma aplicação de utilizador.

4. Os Estados-Membros asseguram que os componentes enumerados no n.º 3 cumprem os requisitos estabelecidos no capítulo II. Os Estados-Membros são responsáveis pela instalação, alojamento, desenvolvimento, disponibilidade, monitorização, atualização e manutenção desses componentes, bem como pela segurança das informações neles tratadas. Se dois ou mais Estados-Membros criarem ou desenvolverem conjuntamente um ou vários dos referidos componentes, serão conjuntamente responsáveis pela sua instalação, alojamento, desenvolvimento, disponibilidade, monitorização, atualização, manutenção e segurança.

5. Os Estados-Membros continuam a ser responsáveis por assegurar que o acesso e o tratamento dos dados eFTI pelas autoridades competentes sejam efetuados apenas para efeitos de verificação da conformidade com as disposições legais nacionais e da UE aplicáveis, e em conformidade com as disposições nacionais e da UE aplicáveis que estabelecem as condições para a realização dessas verificações de conformidade, bem como com as regras em matéria de respeito da privacidade dos dados pessoais e da confidencialidade dos dados comerciais.

Artigo 3.º

Pedidos de acesso a dados eFTI, respostas e comunicação de seguimento

1. Os agentes da autoridade competente apresentam todos os pedidos de acesso aos dados eFTI através do componente AAP descrito no artigo 4.º, utilizando a aplicação de utilizador descrita no artigo 7.º.

2. Um pedido de acesso a dados eFTI contém as seguintes informações:

a) A UIL dos dados eFTI aos quais é pedido acesso, ou um ou mais identificadores que permitam obter essa UIL do registo de identificadores descrito no artigo 11.º. Estas informações devem ser fornecidas pelo agente da autoridade competente responsável pelo pedido;

b) As referências aos direitos de acesso do agente da autoridade competente responsável pela apresentação do pedido, tal como inscritas no registo de autorizações descrito no artigo 5.º. Estas informações são adicionadas automaticamente pela aplicação de utilizador;

c) O número de identificação único do pedido, tal como emitido pelo AAP. Estas informações são adicionadas automaticamente pela aplicação de utilizador.

3. As respostas a um pedido de acesso a dados eFTI podem assumir uma das seguintes formas:

a) Dados eFTI, tal como transmitidos por uma plataforma eFTI com base nas informações contidas num pedido, e os metadados ou identificadores associados ao intercâmbio de mensagens necessários para permitir às portas eFTI destinatárias ou aos pontos de acesso da autoridade associar os dados eFTI ao respetivo pedido;

b) Mensagens de erro, contendo uma descrição textual breve ou codificada do tipo de erro quando uma porta eFTI ou uma plataforma eFTI não consegue fornecer os dados eFTI pedidos por motivos técnicos ou operacionais;

c) Mensagem que indica que não há dados disponíveis, emitida por uma porta eFTI destinatária quando processa um pedido que contém identificadores e o mecanismo de pesquisa da porta não deteta qualquer UIL ativa associada a esses identificadores no seu registo de identificadores;

d) Mensagem «sem resposta», transmitida por uma porta eFTI ou plataforma eFTI quando essa porta ou plataforma confirmou a receção do pedido, mas não enviou uma mensagem que contenha os dados eFTI pedidos no prazo de 60 segundos após a confirmação da receção.

4. Se o agente da autoridade competente verificar que as informações disponibilizadas por um operador económico numa plataforma eFTI, e obtidas em resposta a um pedido de acesso a dados eFTI, estão incompletas ou não cumprem de outra forma os requisitos de informações regulamentares com base nos quais o pedido foi apresentado, o agente pode comunicar essas conclusões ao operador económico apresentando uma comunicação de seguimento específica para essas informações. Essa comunicação de seguimento cumpre os requisitos legais nacionais aplicáveis em matéria de ações de acompanhamento das verificações de conformidade regulamentares.

5. Se for apresentada a comunicação de seguimento específica a que se refere o n.º 4, a autoridade competente transmite-a igualmente através do componente AAP, utilizando a aplicação de utilizador. Esta comunicação contém:

a) As informações a comunicar ao operador económico pela autoridade competente, em formato de texto livre ou sob a forma de documento anexado;

b) A UIL dos dados eFTI e o número de identificação único do pedido de acesso aos dados para os quais é apresentada a comunicação de seguimento.

CAPÍTULO II

COMPONENTES FUNCIONAIS

Artigo 4.º

Pontos de Acesso da Autoridade

1. Os componentes do AAP permitem o acesso dos agentes das autoridades competentes ao ambiente de intercâmbio eFTI e constituem o único ponto de acesso do agente a esse ambiente.

2. O AAP dispõe das seguintes funcionalidades:

a) Autenticar a identidade dos agentes da autoridade competente ou assegurar a autenticação da identidade dos agentes da autoridade competente;

b) Autorizar o pedido de acesso a dados eFTI dos agentes da autoridade competente, com base nos seus direitos de acesso inscritos no registo de autorizações, ou rejeitar o pedido se o agente da autoridade competente não tiver direitos de acesso ativos registados;

c) Registar os pedidos de acesso a dados eFTI autorizados através da emissão de um número de identificação único para cada um destes pedidos e registar, pelo menos, as seguintes informações para cada pedido:

   i) referências de identificação do agente responsável pela apresentação do pedido;

   ii) a UIL dos dados eFTI aos quais é pedido acesso, ou o identificador ou identificadores fornecidos pelo agente no momento de apresentação do pedido;

   iii) as referências aos direitos de acesso do agente da autoridade competente responsável pela apresentação do pedido, tal como inscritas no registo de autorizações;

   iv) a data e a hora em que o pedido foi apresentado;

d) Transmitir os pedidos de acesso a dados eFTI autorizados à porta eFTI para tratamento, fornecendo as seguintes informações:

   i) o número de identificação único do pedido;

   ii) a UIL dos dados eFTI para os quais é pedido acesso, ou o identificador ou identificadores fornecidos pelo funcionário no momento de apresentação do pedido;

   iii) as referências aos direitos de tratamento do agente da autoridade competente responsável pela apresentação do pedido, tal como inscritas no registo de autorizações;

e) Receber as respostas aos pedidos transmitidos pela porta eFTI e disponibilizá-las ao agente da autoridade competente responsável por esse pedido através da aplicação de utilizador;

f) Manter pistas de auditoria das respostas recebidas para cada pedido, registando, pelo menos, as seguintes informações:

i) o número de identificação único do pedido para o qual a resposta foi recebida;

ii) a data e hora em que a resposta foi recebida pelo AAP;

iii) a data e a hora em que o AAP transmitiu a resposta ao agente responsável pelo respetivo pedido;

g) Conservar um arquivo dos pedidos de acesso a dados eFTI e do registo das respostas recebidas durante um período de dois anos ou, se as disposições nacionais aplicáveis em matéria de disponibilidade de provas para efeitos de execução das disposições para as quais é necessário acesso a dados eFTI estabelecerem um período de tempo maior, durante esse período;

h) Se for apresentada uma comunicação de seguimento em conformidade com o artigo 3.º, n.º 4, registá-la através da emissão de um número de identificação único para a comunicação de seguimento e registar, pelo menos, as seguintes informações para essa comunicação de seguimento:

i) referências de identificação do agente responsável pela apresentação da comunicação de seguimento;

ii) a UIL dos dados eFTI e o número de identificação único do pedido de acesso aos dados para os quais foi apresentada a comunicação de seguimento;

iii) a data e a hora em que a comunicação de seguimento foi apresentada;

iv) o conteúdo da comunicação de seguimento;

i) Transmitir as comunicações de seguimento à porta eFTI para tratamento, fornecendo as seguintes informações:

i) a UIL dos dados eFTI e o número de identificação único do pedido de acesso aos dados para os quais foi apresentada a comunicação de seguimento;

ii) o conteúdo da comunicação de seguimento;

3. Para disponibilizar as funcionalidades previstas no n.º 2, o AAP:

a) Utiliza meios de identificação eletrónica adequados que permitem a identificação e autenticação fiáveis dos agentes das autoridades competentes, ou que permitem verificar se a identificação e a autenticação desses agentes são asseguradas por outro componente de TIC adequado;

b) Utiliza um registo de autorizações;

c) Estabelece e mantém uma ligação segura a uma porta eFTI;

d) Estabelece uma ligação segura à aplicação do utilizador.

4. Os Estados-Membros podem criar AAP externos à porta eFTI, como parte integrante dos sistemas de TIC existentes das suas autoridades competentes, ou integrados na sua porta eFTI.

Artigo 5.º

Registo de autorizações

Os Estados-Membros asseguram que os direitos dos agentes das suas autoridades competentes para aceder e tratar os dados eFTI são registados e mantidos atualizados num registo de autorizações. O registo de autorizações deve incluir, para cada agente da autoridade competente, pelo menos os seguintes elementos:

a) Referências de identificação únicas do agente;

b) Os direitos de acesso do respetivo agente, expressos sob a forma de uma lista de referências dos atos jurídicos nacionais e da União que exigem a prestação de informações regulamentares, em relação aos quais o respetivo agente tem competências e, mais especificamente, uma lista dos identificadores dos subconjuntos de dados eFTI que correspondem a essas disposições, conforme estabelecido no anexo, pontos 3 e 4, Regulamento Delegado (UE) 2024/2024 da Comissão ([9]);

c) Os direitos de tratamento do respetivo agente, expressos sob a forma de referências codificadas às operações de tratamento que o agente tem o direito de efetuar em cada um dos respetivos subconjuntos de dados eFTI, em conformidade com a legislação da União ou nacional aplicável que determina as competências desse agente;

d) Um registo das alterações aos direitos de acesso e de tratamento desse agente.

Artigo 6.º

Portas eFTI

1. As portas eFTI asseguram, diretamente ou através da ligação a outras portas eFTI, que:

a) Os pedidos de acesso a dados eFTI autorizados são transmitidos à plataforma eFTI e contêm as informações específicas pedidas;

b) Para cada um destes pedidos, a resposta recebida da respetiva plataforma eFTI é transmitida à aplicação de utilizador do agente da autoridade competente responsável pelo pedido, quer diretamente, quer através de um AAP, consoante o caso; e

c) Quando apresentada, a comunicação de seguimento ao pedido é transmitida à plataforma eFTI que contém os dados eFTI para os quais o pedido foi apresentado e a resposta fornecida.

2. As portas eFTI dispõem das seguintes funcionalidades:

a) Validar o pedido de acesso a dados eFTI e, quando apresentada, à comunicação de seguimento, de uma das seguintes formas:

   i) ao funcionar na qualidade de «porta requerente», se o AAP for estabelecido como um componente separado, externo à porta eFTI, verificando a chave de segurança do AAP através do qual foi apresentado o pedido ou a comunicação de seguimento;

   ii) ao funcionar na qualidade de «porta destinatária», verificando a chave de segurança da porta eFTI através da qual o pedido ou a comunicação de seguimento foram recebidos;

   iii) se a validação da chave de segurança da porta eFTI respetiva falhar, enviando uma mensagem de erro à «porta requerente», ao AAP ou ao agente da autoridade competente responsável pelo pedido ou pela comunicação de seguimento, consoante o caso;

b) Tratar o pedido de acesso a dados eFTI e a eventuais comunicações de seguimento apresentadas, através do mecanismo de pesquisa estabelecido em conformidade com o artigo 8.º, e, nessa base, transmitir o pedido ou a comunicação de seguimento, consoante o caso:

   i) à plataforma eFTI ou à(s) porta(s) eFTI adequada(s), ao funcionar na qualidade de «porta requerente»;

   ii) à plataforma eFTI adequada, ao funcionar na qualidade de «porta destinatária»;

c) Manter uma pista de auditoria de todos os pedidos de acesso a dados eFTI ou comunicações de seguimento tratadas, registando, pelo menos, as seguintes informações:

   i) o número de identificação único do pedido de acesso a dados eFTI ou da comunicação de seguimento;

   ii) o identificador do AAP ou da «porta eFTI requerente» através da qual o pedido ou a comunicação de seguimento foram recebidos;

   iii) a data e a hora em que o pedido foi recebido;

([9]) Regulamento Delegado (UE) 2024/2024 da Comissão, de 26 de julho de 2024, que completa o Regulamento (UE) 2020/1056 estabelecendo o conjunto comum de dados eFTI e os subconjuntos de dados eFTI (JO L, 2024/2024, 20.12.2024, ELI: http://data.europa.eu/eli/reg_del/2024/2024/oj).

d) Validar a resposta recebida a um pedido tratado, do seguinte modo:

i) ao receber a resposta diretamente da plataforma eFTI, verificando a chave de segurança e o estado de certificação da plataforma eFTI, com base no registo referido no n.º 3, alínea e);

ii) ao receber a resposta de uma «porta eFTI destinatária», verificando a chave de segurança dessa porta eFTI com base no registo referido no n.º 3, alínea f);

iii) se a validação da chave de segurança da plataforma ou porta eFTI respetiva falhar, enviando uma mensagem de erro correspondente à «porta requerente», ao AAP ou à aplicação de utilizador do agente da autoridade competente responsável pelo pedido, consoante o caso;

e) Transmitir a resposta recebida para um pedido processado pela mesma via, na direção oposta ao pedido enviado, conforme aplicável:

i) à «porta eFTI requerente»; ou

ii) à aplicação de utilizador do agente da autoridade competente responsável pelo pedido, diretamente ou através do AAP;

f) Se for recebida uma confirmação de receção do pedido, mas não for recebida outra resposta no prazo de 60 segundos após a confirmação, transmitir uma mensagem «sem resposta» à «porta requerente», ao AAP ou à aplicação de utilizador do agente da autoridade competente responsável pelo pedido, consoante o caso;

g) Manter uma pista de auditoria de todas as respostas a pedidos de acesso transmitidos, registando, pelo menos, as seguintes informações:

i) a UIL do conjunto de dados eFTI recebidos em resposta ao pedido;

ii) o número de identificação único da plataforma eFTI ou da «porta eFTI destinatária» através da qual a resposta foi recebida;

iii) a data e a hora em que a resposta foi recebida;

iv) se não tiver sido recebida qualquer resposta, uma indicação nesse sentido;

h) Arquivar e conservar os registos especificados nas alíneas c) e g) disponíveis para efeitos de auditoria, durante um período de dois anos ou, se as disposições nacionais em matéria de disponibilidade de provas para efeitos de execução das disposições para as quais é necessário acesso a dados eFTI estabelecerem um período de tempo maior, durante esse período.

3. Para proporcionar as funcionalidades a que se refere o n.º 2, a porta eFTI:

a) Utiliza um mecanismo de pesquisa, em conformidade com o artigo 8.º;

b) Estabelece e mantém uma ligação segura aos AAP que mediam o acesso ao ambiente de intercâmbio eFTI dos agentes das autoridades competentes do Estado-Membro que criou a respetiva porta eFTI;

c) Se os AAP forem estabelecidos como componentes integrados da porta eFTI, estabelece e mantém uma ligação segura à aplicação ou aplicações de utilizador, consoante o caso, dos agentes da autoridade competente do Estado-Membro que criou a respetiva porta eFTI;

d) Se os AAP forem estabelecidos como componentes separados da porta eFTI, cria e mantém atualizado um registo dos números de identificação únicos e certificados de segurança desses AAP;

e) Estabelece e mantém uma ligação segura a todas as outras portas eFTI, bem como um registo atualizado que contém os números de identificação únicos e os certificados de segurança dessas portas eFTI;

f) Estabelece e mantém uma ligação segura a todas as plataformas eFTI que receberam certificação no Estado-Membro ou Estados-Membros que criaram a porta eFTI respetiva, bem como um registo atualizado dos números de identificação únicos, das chaves de segurança e do estado de certificação dessas plataformas eFTI;

g) É capaz de utilizar serviços ou artefactos com definições comuns, tais como configurações, códigos de erro, taxonomias ou listas de códigos no ambiente de intercâmbio eFTI, estando estes serviços ou artefactos acordados no âmbito da rede de apoio operacional a que se refere o artigo 13.º.

4. Se num Estado-Membro não existirem organismos de avaliação da conformidade acreditados para certificar plataformas eFTI em conformidade com o artigo 11.º do Regulamento (UE) 2020/1056, esse Estado-Membro assegura que a sua porta eFTI estabelece e mantém a ligação segura e o registo atualizado, tal como referido no n.º 3, alínea f), a plataformas eFTI que receberam certificação de organismos de avaliação da conformidade acreditados noutros Estados-Membros. Esse Estado-Membro fá-lo a pedido do operador económico ou do prestador de serviços eFTI que opera essa plataforma e após solicitar e receber confirmação do Estado-Membro onde a plataforma eFTI recebeu a certificação de que não recebeu outro pedido de confirmação de outro Estado-Membro para essa plataforma eFTI. Tal dispensa a porta eFTI do Estado-Membro em que a plataforma eFTI recebeu certificação da obrigação de estabelecer e manter uma ligação segura a essa plataforma.

Artigo 7.º

Aplicação de utilizador

1. A aplicação de utilizador permite a um agente da autoridade competente interagir com o AAP.

2. A aplicação de utilizador dispõe, pelo menos, das seguintes funcionalidades:

a) Gerar os pedidos de acesso a dados eFTI, com base nas informações fornecidas por um agente da autoridade competente, depois de este ser devidamente identificado, autenticado e autorizado pelo AAP;

b) Receber e apresentar para visualização pelo agente da autoridade competente responsável pelo pedido, os dados eFTI correspondentes fornecidos pela(s) respetiva(s) plataforma(s) eFTI em resposta a esse pedido, mensagens «sem resposta» ou mensagens de erro transmitidas pelo AAP ou pela «porta eFTI destinatária»;

c) Permitir outras operações de tratamento dos dados eFTI recebidos pelo agente da autoridade competente responsável pelo pedido, em conformidade com os seus direitos de tratamento;

d) Se as disposições nacionais aplicáveis o permitirem, gerar comunicações de seguimento, com base nas informações fornecidas por um agente da autoridade competente.

3. Para proporcionar as funcionalidades referidas no n.º 2, a aplicação de utilizador dispõe, pelo menos das seguintes capacidades:

a) Fornece aos agentes da autoridade competente uma interface gráfica de utilizador;

b) Estabelece e mantém uma ligação segura a um AAP ou a uma porta eFTI, consoante o caso;

c) Para o tratamento de dados, utiliza como referência os subconjuntos de dados que correspondem às disposições dos atos jurídicos nacionais e da União, estabelecidos pelo Regulamento Delegado (UE) 2024/2024, em relação aos quais os agentes das autoridades competentes têm competências.

Artigo 8.º

Mecanismo de pesquisa

1. O mecanismo de pesquisa deve ser um componente integrado numa porta eFTI que, como funcionalidade principal, processa as informações incluídas no pedido ou na comunicação de seguimento, do seguinte modo:

a) A partir da UIL dos dados eFTI, obtém o identificador da plataforma eFTI que armazena os dados eFTI para os quais foi apresentado o pedido de acesso ou a comunicação de seguimento e o identificador da porta eFTI respetiva à qual essa plataforma está ligada;

b) Se o pedido de informações incluir um ou vários dos identificadores previstos no artigo 11.º, n.º 3, pesquisa o registo de identificadores para obter o valor correspondente e

   i) se for encontrada uma correspondência, obter o UIL ou conjunto de UIL ativos relacionados com os respetivos identificadores e processar as informações nas UIL respetivas em conformidade com a alínea a);

   ii) se não for encontrada uma correspondência, notificar a porta eFTI deste facto.

2. Para proporcionar a funcionalidade referida no n.º 1, o mecanismo de pesquisa:

a) Administra um registo de identificadores, em conformidade com o artigo 11.º;

b) Utiliza um registo de editor de serviços de metadados (SMP) e um localizador de metadados de serviços (SML) em conformidade com as especificações eDelivery, ou um serviço de registo com capacidades semelhantes, para permitir encontrar plataformas eFTI com base nas informações contidas no pedido ou na comunicação de seguimento.

CAPÍTULO III

ESPECIFICAÇÕES TÉCNICAS

Artigo 9.º

Intercâmbio de mensagens

1. Os Estados-Membros asseguram que as portas eFTI que criam, bem como os AAP e as aplicações de utilizador das suas autoridades competentes, comunicam e podem receber comunicações num formato normalizado de intercâmbio de mensagens. A comunicação entre portas eFTI e entre as portas eFTI e as plataformas eFTI é efetuada utilizando o formato XML.

2. Todas as comunicações entre as portas eFTI ocorre sob a forma de intercâmbio de mensagens através dos pontos de acesso eDelivery, em conformidade com as especificações para intercâmbio de mensagens do eDelivery e utilizando o mecanismo de descoberta estática do eDelivery.

3. O intercâmbio de mensagens através de pontos de acesso eDelivery, em conformidade com as especificações para intercâmbio de mensagens do eDelivery, utilizando o mecanismo de descoberta dinâmica do eDelivery é também ativado para a comunicação entre as portas eFTI e as plataformas eFTI.

4. Se um Estado-Membro já tiver criado especificações equivalentes e seguras, definidas a nível nacional, para o intercâmbio de mensagens entre serviços públicos digitais, pode decidir ativar essa comunicação entre as plataformas eFTI e a porta eFTI criada pelo Estado-Membro, que pode decorrer com base nessas especificações de intercâmbio de mensagens equivalentes. Nestes casos, os Estados-Membros asseguram que essas especificações são disponibilizadas ao público, devidamente detalhadas e atualizadas.

Artigo 10.º

Certificados de segurança

1. Os Estados-Membros emitem certificados de segurança, através de uma autoridade de certificação, para os pontos de acesso eDelivery integrados nas portas eFTI que criaram e para os pontos de acesso eDelivery ou, se for caso disso, ao ponto de acesso de intercâmbio de mensagens equivalente de cada plataforma eFTI que tenha recebido certificação de um organismo de avaliação da conformidade acreditado no respetivo Estado-Membro.

2. Os Estados-Membros asseguram que as chaves de segurança privadas do ponto de acesso eDelivery integrado na(s) porta(s) eFTI são armazenadas de forma segura e que os respetivos certificados digitais são emitidos de forma segura entre portas eFTI e entre a porta eFTI e as plataformas eFTI ligadas a essa porta.

3. Os Estados-Membros asseguram a existência de mecanismos seguros para receção, registo, obtenção e validação das chaves públicas ou dos certificados de segurança das plataformas eFTI ligadas à sua porta eFTI. Se um Estado-Membro criar um registo SMP em conformidade com as especificações do eDelivery para SMP e com mecanismos de segurança adequados, pode utilizar esse registo SMP para este efeito.

Artigo 11.º

Registo de identificadores

1. O registo de identificadores referido no artigo 8.º, n.º 2, alínea a) permite aos operadores económicos carregar, através de uma plataforma eFTI, a UIL de um conjunto de dados eFTI, juntamente com os identificadores que permitem a obtenção única dessa UIL, conforme indicado no n.º 3. O registo de identificadores permite carregar, ativar, desativar ou apagar a UIL de um conjunto de dados eFTI e dos respetivos identificadores.

2. A composição da UIL permite obter o identificador da porta eFTI, o identificador da plataforma eFTI e o identificador único do conjunto de dados eFTI correspondente às informações regulamentares disponibilizadas pelos operadores económicos na plataforma eFTI respetiva, sendo que:

a) O identificador da porta eFTI é constituído por um identificador que a permite encontrar de forma única no ambiente eFTI;

b) O identificador da plataforma eFTI é constituído por um identificador que a permite encontrar de forma única no ambiente eFTI;

c) A identificação única do conjunto de dados eFTI é constituída por um número único no formato de identificador único universal (UUID) atribuído automaticamente pela plataforma eFTI.

3. Os identificadores compatíveis com o registo consistem em:

a) Elementos de dados do conjunto de dados eFTI que correspondem às informações regulamentares disponibilizadas pelos operadores económicos, conforme descrito no anexo, ponto 2, Regulamento Delegado (UE) 2024/2024, com os seguintes números de identificação:

   i) eFTI39;

   ii) eFTI188;

   iii) eFTI374;

   iv) eFTI378;

   v) eFTI448;

   vi) eFTI581;

   vii) eFTI578;

   viii) eFTI618;

   ix) eFTI620;

   x) eFTI987;

   xi) eFTI1000.

b) Um elemento de dados que indica se estão a ser transportadas mercadorias perigosas, a identificar com as seguintes características: identificador do elemento de dados «eFTI1451»; designação «Mercadorias perigosas a bordo. Indicador»; definição «Indicação de estarem ou não a ser transportadas mercadorias perigosas, de acordo com a classificação ADR/ADN/RID. "Sim" significa que se encontram as mercadorias perigosas a bordo da unidade de transporte, "Não" significa que as mercadorias transportadas não constam da lista ADR/ADN/RID de mercadorias perigosas ou que as mercadorias perigosas estão isentas dos requisitos de informação constantes dos pontos 3.5.6, 5.1.5.4.2, 5.4.1, 5.5.2.4.1 ou 5.5.3.7 da lista ADR/ADN/RID.»

4. O registo de identificadores ativa a UIL, para que fique disponível para consultas, depois do carregamento, e desativa-a quando é carregado o identificador referido no n.º 3, alínea a), subalínea ii), do presente artigo. Para permitir verificações de controlo em conformidade com as disposições do Regulamento (CE) n.º 1072/2009, o registo de identificadores só desativa as UIL para cada UIL para o qual o identificador indicado no n.º 3, alínea a), subalínea vi), do presente artigo tenha o valor «3», correspondente a «transporte rodoviário» após o período referido no artigo 8.º, n.º 2, do Regulamento (CE) n.º 1072/2009. Após a desativação, o registo apaga a UIL e os identificadores a ela ligados.

CAPÍTULO IV

MANUTENÇÃO E GOVERNAÇÃO

Artigo 12.º

Rede de assistência técnica

1. Os Estados-Membros criam serviços de assistência com dois níveis diferentes:

a) Está disponível um serviço de assistência de «nível 1» para prestar apoio técnico aos agentes das autoridades competentes em caso de problemas operacionais;

b) Está disponível um serviço de assistência de «nível 2» para prestar apoio:

i) aos serviços de assistência de «nível 1», que prestam apoio aos agentes;

ii) aos serviços de assistência de «nível 1» criados pelos proprietários das plataformas eFTI, para prestar apoio técnico aos operadores económicos.

2. A Comissão cria um serviço de assistência de «nível 3» que:

a) Presta apoio técnico aos serviços de assistência de «nível 2», para resolver questões operacionais relacionadas com o funcionamento do ambiente geral de intercâmbio eFTI, incluindo regras, procedimentos e especificações de implementação funcionais e técnicas, bem como os conjuntos e subconjuntos comuns de dados eFTI estabelecidos nos atos de execução e delegados nos termos do Regulamento (UE) 2020/1056;

b) Funciona na qualidade de facilitador de questões operacionais que digam respeito a dois ou mais Estados-Membros e quando é necessária coordenação a nível da União, incluindo a interoperabilidade técnica das portas eFTI e a comunicação entre portas eFTI;

c) Interage com os serviços da Comissão que fornecem *software* específico ou especificações de produtos utilizados pelo ambiente de intercâmbio eFTI, como o eDelivery.

3. Os serviços de assistência de «nível 1» e de «nível 2» estabelecem igualmente contacto entre si para resolverem questões de interesse comum aos seus níveis.

4. A disponibilidade dos serviços de assistência deve ser sincronizada em toda a União para assegurar um período mínimo de disponibilidade comum durante os dias úteis, entre as 10h00 e as 16h00, no fuso horário da Europa Central (CET/CEST), com exceção dos feriados nacionais. Durante os fins de semana e feriados nacionais, está disponível um serviço de emergência, no qual está sempre disponível em permanência pelo menos um membro do pessoal, para dar resposta a questões urgentes que afetem gravemente o funcionamento do ambiente de intercâmbio eFTI, a nível nacional ou da União.

5. Todos os serviços de assistência utilizam ferramentas de assistência específicas que permitem a identificação e o acompanhamento únicos de cada pedido de apoio técnico, nomeadamente quando a resolução de um pedido exige a comunicação entre os serviços de assistência.

6. Os serviços de assistência mantêm registos de todos os pedidos de assistência e do seu historial e compilam regularmente relatórios das suas atividades.

7. Os Estados-Membros comunicam entre si e à Comissão os dados de contacto dos seus serviços de assistência de «nível 2».

8. A data de início da disponibilidade dos serviços de assistência é a data referida no artigo 5.º, n.º 1, do Regulamento (UE) 2020/1056. A adequação do período mínimo de disponibilidade comum dos serviços de assistência deve ser avaliada no prazo de 12 meses a contar dessa data.

Artigo 13.º

Rede de apoio operacional

1. É criado um grupo de trabalho específico como subgrupo do grupo de peritos criado nos termos da Decisão C (2018) 5921, com o mandato de assegurar que as operações eFTI são realizadas com o nível de qualidade exigido.

2. Os membros do grupo de trabalho nomeados pelos Estados-Membros atuam igualmente na qualidade de «pontos de contacto eFTI nacionais».

3. Os membros do grupo de trabalho cooperam e reúnem-se regularmente para, nomeadamente:

a) Fornecer informações atualizadas sobre o estado operacional do ambiente de intercâmbio eFTI;

b) Prestar assistência aos serviços da Comissão nos seus esforços para resolver problemas técnicos e operacionais comunicados pelos Estados-Membros ou pelo serviço de assistência de «nível 3» que exijam coordenação e orientação operacional a nível da União;

c) Prestar assistência à Comissão na elaboração de documentos de orientação técnica para dar apoio à aplicação do presente regulamento.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Artigo 14.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 sua data de entrada em vigor.

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

Feito em Bruxelas, em 5 de julho de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN