Parecer 15/2026 sobre os critérios de certificação Europrivacy no que diz respeito à sua aprovação pelo Comité como Selo Europeu de Proteção de Dados, a utilizar enquanto instrumento para as transferências nos termos dos artigos 42.º e 46.º do RGPD

Adotado em 15 abril 2026

Translations are proofread by EDPB Members.
This language version has not been proofread yet.

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 63.º, o artigo 64.º, n.º 2, o artigo 42.º e o artigo 46.º do 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 (a seguir designado por «RGPD»),

Tendo em conta o Acordo sobre o Espaço Económico Europeu (a seguir designado por «EEE»), nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta os artigos 10.º e 22.º do seu Regulamento Interno,

1 Os Estados-Membros, as autoridades de controlo, o Comité Europeu para a Proteção de Dados (a seguir designado por «CEPD» ou «Comité») e a Comissão Europeia promovem, em especial a nível da União, a criação de procedimentos de certificação em matéria de proteção de dados (a seguir designados por «procedimentos de certificação») e de selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o RGPD, tendo em conta as necessidades específicas das micro, pequenas e médias empresas[2]. Além disso, a criação de procedimentos de certificação pode reforçar a transparência e permitir que os titulares dos dados avaliem o nível de proteção de dados dos produtos e serviços pertinentes[3].

2 Além do cumprimento pelos responsáveis pelo tratamento ou pelos subcontratantes sujeitos ao RGPD, os procedimentos de certificação em matéria de proteção de dados, bem como selos ou marcas aprovados de acordo com o artigo 42.º, n.º 5, do RGPD também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes que não estão sujeitos ao referido regulamento por força do artigo 3.º no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais (a seguir designados por «importadores de dados») nos termos referidos no artigo 46.º, n.º 2, alínea f), do RGPD[4].

3 A certificação a utilizar como instrumento para as transferências é um novo mecanismo de transferência introduzido pelo artigo 46.º do RGPD a fim de assegurar que, não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, do RGPD, os responsáveis pelo tratamento ou subcontratantes abrangidos pelo RGPD (a seguir designados por «exportadores de dados do EEE») só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes. Em especial, nos termos do artigo 46.º, n.º 2, alínea f), do RGPD, um procedimento de certificação, aprovado nos termos do artigo 42.º do RGPD, pode prever estas garantias adequadas se for acompanhado de compromissos vinculativos e com força executiva assumidos pelos importadores de dados no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados. Os critérios de certificação fazem parte integrante de um procedimento de certificação. Por conseguinte,

[1] As referências a «Estados-Membros» ao longo do presente parecer devem ser entendidas como referências a «Estados do EEE».
[2] Artigo 42.º, n.º 1, do RGPD.
[3] Considerando 100 do RGPD.
[4] Ver artigo 42.º, n.º 2, do RGPD.

o RGPD exige a aprovação dos critérios de um procedimento nacional de certificação pela autoridade de controlo competente [artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b), do RGPD] ou, no caso de um Selo Europeu de Proteção de Dados, pelo CEPD [artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o), do RGPD].

4 Caso uma autoridade de controlo (a seguir designada por «AC») tencione propor a aprovação pelo CEPD de um Selo Europeu de Proteção de Dados nos termos do artigo 42.º, n.º 5, do RGPD, a AC deve declarar a intenção do proprietário do sistema de disponibilizar o procedimento de certificação em todos os Estados-Membros. Neste caso, a principal função do CEPD consiste em assegurar a aplicação coerente do RGPD, através do procedimento de controlo da coerência a que se referem os artigos 63.º, 64.º e 65.º do RGPD. Neste contexto, nos termos do artigo 64.º, n.º 2, do RGPD, o CEPD aprova os critérios de certificação.

5 Um Selo Europeu de Proteção de Dados aprovado nos termos do artigo 42.º, n.º 5, do RGPD, criado para demonstrar a existência de garantias adequadas facultadas pelos importadores de dados, juntamente com compromissos vinculativos e com força executiva, serve de instrumento para abranger as transferências de dados de todos os Estados do EEE para países terceiros ou organizações internacionais[5].

6 Ao avaliar um procedimento de certificação a utilizar enquanto instrumento para as transferências, a avaliação do CEPD é realizada com base nas «Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento» (a seguir designadas por «diretrizes») e na respetiva adenda intitulada *Guidance on certification criteria assessment* [Orientações sobre a avaliação dos critérios de certificação] (a seguir designada por «adenda»), bem como nas «Orientações 07/2022 relativas à certificação enquanto instrumento para as transferências» (a seguir designadas por «Orientações relativas à certificação enquanto instrumento para as transferências»).

7 O CEPD reconhece que cada procedimento de certificação deve ser abordado individualmente e não prejudica a avaliação de qualquer outro procedimento de certificação.

8 Os procedimentos de certificação a utilizar enquanto instrumento para as transferências devem permitir aos importadores de dados demonstrar a existência de garantias adequadas, a fim de assegurar que o nível de proteção das pessoas singulares garantido pelo RGPD não será comprometido quando os dados pessoais transferidos forem tratados fora do EEE[6]. Por conseguinte, os respetivos critérios devem refletir adequadamente os requisitos e princípios relativos à proteção de dados pessoais previstos no RGPD, de modo a assegurar que a proteção concedida pelo RGPD acompanhará os dados pessoais[7].

9 Ao mesmo tempo, o proprietário do sistema deve assegurar o alinhamento e a conformidade do procedimento de certificação com quaisquer normas ISO e práticas de certificação incluídas ou alavancadas.

10 Consequentemente, as certificações devem acrescentar valor aos importadores de dados, ao contribuir para a aplicação de medidas organizativas e técnicas normalizadas e especificadas, a fim de demonstrar que estão em vigor garantias adequadas ao proceder ao tratamento de dados pessoais recebidos por exportadores de dados do EEE. Nesta perspetiva, o CEPD recorda que o objeto da certificação — que coincide com o alvo da

[5] Orientações 07/2022 do CEPD relativas à certificação enquanto instrumento para as transferências, versão 2.0, adotadas em 14 de fevereiro de 2023, n.º 30.
[6] Artigo 44.º do RGPD.
[7] Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», COM(2017) 7 final, p. 4.

avaliação («target of evaluation» — ToE) durante a certificação — deve, em geral, ser o tratamento dos dados transferidos para o importador de dados no país terceiro e o trânsito, caso esteja sob o controlo do mesmo importador[8].

11 As certificações também terão valor acrescentado para o exportador de dados, que poderá decidir confiar na certificação obtida por um importador de dados enquanto instrumento para transferir dados pessoais nos termos do artigo 46.º, n.º 2, alínea f), do RGPD e como elemento para demonstrar o cumprimento das obrigações, por exemplo, nos termos do artigo 24.º, n.º 3, ou do artigo 28.º, n.º 5, do RGPD[9].

12 A este respeito, o CEPD recorda que o exportador de dados que pretenda utilizar a certificação como garantia adequada nos termos do artigo 46.º, n.º 2, alínea f), do RGPD é obrigado a verificar se a certificação em que pretende confiar é eficaz à luz das características do tratamento previsto. Para o efeito, o exportador de dados deve analisar a certificação emitida, a fim de verificar se o certificado é válido e não caducou, se abrange a transferência específica a efetuar e se o trânsito de dados pessoais é abrangido pelo âmbito da certificação, bem como se estão envolvidas transferências ulteriores e se é fornecida documentação adequada sobre as mesmas[10].

13 Por outro lado, o exportador de dados tem de verificar se o organismo de certificação que emitiu a certificação está acreditado por um organismo nacional de acreditação ou por uma autoridade de controlo competente. Adicionalmente, o exportador de dados deve fazer referência à utilização da certificação enquanto instrumento de transferência no contrato de tratamento de dados nos termos do artigo 28.º do RGPD, em caso de transferências do responsável pelo tratamento para o subcontratante, ou num contrato de partilha de dados com o importador de dados, em caso de transferências do responsável pelo tratamento para outro responsável pelo tratamento[11]. Tem igualmente de cumprir as obrigações específicas previstas no artigo 13.º, n.º 1, alínea f), do RGPD, em especial, informar o titular dos dados das garantias adequadas utilizadas, ou seja, em caso de certificação nos termos do artigo 46.º, n.º 2, alínea f), do RGPD, do certificado recebido pelo importador de acordo com um procedimento de certificação específico e dos meios para obter uma cópia do certificado e das garantias constantes dos critérios de certificação ou do local onde foram disponibilizadas.

14 O CEPD congratula-se com os esforços envidados pelos proprietários dos sistemas para elaborar procedimentos de certificação que, ao aumentar a transparência, são instrumentos práticos e potencialmente eficazes em termos de custos para assegurar uma maior coerência com o RGPD e promover o direito à privacidade e à proteção de dados dos titulares dos dados.

15 O CEPD recorda que as certificações são instrumentos voluntários de responsabilização e que a adesão a um procedimento de certificação não impede as autoridades de controlo de exercerem as suas funções e poderes nos termos do RGPD e da legislação nacional pertinente. Tal, no contexto das certificações a utilizar enquanto instrumento para as transferências, também no que se refere especificamente ao respeito das obrigações assumidas como compromissos vinculativos e com força executiva pelos importadores de dados perante os exportadores de dados, através de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, para aplicar as garantias adequadas previstas pelo

[8] Ver as Orientações 07/2022 do CEPD relativas à certificação enquanto instrumento para as transferências, versão 2.0, adotadas em 14 de fevereiro de 2023, n.º 16.
[9] Orientações 07/2022 relativas à certificação enquanto instrumento para as transferências, n.º 5.
[10] Orientações 07/2022 relativas à certificação enquanto instrumento para as transferências, n.º 20.
[11] *Ibidem*.

procedimento de certificação, nomeadamente no que diz respeito aos direitos dos titulares dos dados.

16 O presente parecer visa assegurar a aplicação coerente do RGPD, nomeadamente pelas AC, pelos responsáveis pelo tratamento e pelos subcontratantes, à luz dos elementos essenciais que os procedimentos de certificação são obrigados a estabelecer. Em especial, o presente parecer visa avaliar os critérios de certificação destinados a ser utilizados enquanto instrumento para as transferências realizadas por importadores de dados. Por conseguinte, no presente parecer, o CEPD aborda questões como o âmbito, a aplicabilidade e a pertinência dos critérios em caso de transferências realizadas a partir de todos os Estados do EEE e/ou de quaisquer exportadores de dados abrangidos pelo âmbito de aplicação do RGPD.

17 O parecer do CEPD centra-se exclusivamente nos critérios de certificação. O CEPD pode exigir informações de alto nível sobre os métodos de avaliação, a fim de poder avaliar exaustivamente a auditabilidade dos critérios no contexto do seu parecer. Todavia, tal não abrange qualquer tipo de aprovação desses métodos de avaliação.

18 O parecer do CEPD é aprovado nos termos do artigo 64.º, n.º 2, do RGPD, em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD, no prazo de oito semanas a contar do primeiro dia útil subsequente à decisão da presidente e da autoridade de controlo competente de que o processo está completo. Por decisão da presidente, este prazo pode ser prorrogado por mais seis semanas, em virtude da complexidade do assunto em apreço. Se o parecer do CEPD concluir que não é possível aprovar os critérios em causa, a AC pode voltar a apresentar os critérios para aprovação depois de as preocupações expressas no parecer inicial do CEPD serem abordadas,

Adotou o seguinte parecer:

1 Resumo dos factos

19 Em conformidade com o artigo 42.º, n.º 2, e o artigo 46.º, n.º 2, alínea f), do RGPD, com as Diretrizes 1/2018 e com as Orientações 07/2022 relativas à certificação enquanto instrumento para as transferências, o European Center for Certification and Privacy (a seguir designado por «proprietário do sistema») elaborou a versão 82 dos critérios Europrivacy (a seguir designados por «critérios de certificação»).

20 O CEPD recorda que já aprovou os critérios de certificação Europrivacy (versão 60) em 10 de outubro de 2022, através da emissão do Parecer 28/2022 do CEPD, enquanto Selo Europeu de Proteção de Dados nos termos do artigo 42.º, n.º 5, do RGPD, destinado a demonstrar a conformidade com o RGPD, em consonância com o artigo 42.º, n.º 1, do RGPD. Esse sistema não era uma certificação nos termos do artigo 46.º, n.º 2, alínea f), do RGPD destinada às transferências de dados.

21 Em 29 de janeiro de 2026, a autoridade de controlo do Luxemburgo (a seguir designada por «AC do Luxemburgo») apresentou ao CEPD uma versão atualizada dos critérios de certificação já aprovados do Selo Europeu de Proteção de Dados Europrivacy, com um âmbito alargado que inclui, em especial, os requerentes abrangidos pelo artigo 3.º, n.º 2, do RGPD, bem como outras alterações relativas aos critérios de certificação principais (versão 82). O CEPD adotou o Parecer 14/2026 sobre esta versão atualizada (versão 82) dos critérios de certificação Europrivacy destinados a demonstrar a conformidade com o RGPD nos termos do artigo 42.º, n.º 5.

22 Na mesma data, a AC do Luxemburgo apresentou igualmente ao CEPD, para aprovação nos termos do artigo 64.º, n.º 2, do RGPD, um conjunto adicional de critérios de certificação (*The*

Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46, extensão do sistema de certificação Europrivacy para a certificação de importadores de dados nos termos do artigo 46.º), destinados a ser utilizados enquanto instrumento para as transferências nos termos do artigo 46.º, n.º 2, alínea f), do RGPD.

23 A decisão de que este processo está completo foi tomada em 31 de março de 2026.

2 Avaliação

24 O CEPD realizou a sua avaliação dos critérios de certificação destinados a ser utilizados enquanto instrumento para as transferências por importadores de dados para a respetiva aprovação nos termos do artigo 42.º, n.º 5, do RGPD, em conjugação com o artigo 46.º, n.º 2, alínea f), do RGPD, em consonância com a estrutura prevista no anexo 2 das Diretrizes 1/2018, a sua adenda e as Orientações relativas à certificação enquanto instrumento para as transferências[12].

25 O Comité salienta que, em consonância com as condições estabelecidas no artigo 42.º, n.º 2, e no artigo 46.º, n.º 2, alínea f), do RGPD, o atual sistema destina-se a ser utilizado enquanto instrumento para as transferências e as certificações emitidas de acordo com o sistema podem, por conseguinte, ser invocadas pelos exportadores de dados na aceção do capítulo V do RGPD (ou seja, pelo responsável pelo tratamento ou pelos subcontratantes sujeitos ao RGPD para o tratamento em causa[13]) para transferir dados pessoais para importadores de dados certificados não sujeitos ao RGPD nos termos do artigo 3.º[14]. Tal significa que as transferências de dados pessoais para o importador de dados no país terceiro só podem ser efetuadas após esse mesmo importador ter sido certificado e ter assinado compromissos vinculativos e com força executiva perante o exportador de dados do EEE no sentido de aplicar as garantias adequadas previstas nos critérios de certificação ao proceder ao tratamento de dados pessoais transferidos no âmbito do ToE, nomeadamente no que diz respeito aos direitos dos titulares dos dados.

26 No contexto do presente parecer e a fim de aprovar os critérios de certificação Europrivacy destinados a ser utilizados enquanto instrumento para as transferências, o CEPD avaliou os controlos e verificações preliminares do pedido e do alvo da avaliação para importadores de dados (ADI), os critérios fundamentais do RGPD do Europrivacy para importadores de dados (GI), e os controlos e verificações das medidas tecnológicas e organizativas (T).

27 No que diz respeito ao processo de certificação, tendo em conta a especificidade da certificação a utilizar enquanto instrumento para as transferências, o CEPD salienta a necessidade de uma grande transparência e congratula-se com os esclarecimentos prestados a este respeito no sistema de certificação Europrivacy, segundo o qual as transferências não podem ter início antes da emissão da certificação. A este respeito, o CEPD reconhece que, antes da transferência de dados pessoais ocorrer, a avaliação pode ser efetuada com dados pessoais não sujeitos ao RGPD ou com dados não pessoais. Caso seja necessário, é possível utilizar dados falsos para avaliar critérios específicos e, após o início da transferência de dados, o auditor reavalia esses critérios na auditoria de acompanhamento seguinte[15].

[12] Ver, em especial: secções 3 e 4 das Orientações 07/2022.
[13] Ver Diretrizes 05/2021 do CEPD sobre a interação entre a aplicação do artigo 3.º e as disposições relativas às transferências internacionais nos termos do capítulo V do RGPD, versão 2.0, adotadas em 14 de fevereiro de 2023, n.º 9.
[14] Artigo 42.º, n.º 2, do RGPD.
[15] Ver Europrivacy™/®, *Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR*, EP-CS.1.DI, secção 6.1.

28 O CEPD recorda que podem ser necessários alguns ajustamentos da acreditação realizada pelos organismos de certificação no que diz respeito a uma certificação enquanto instrumento para as transferências, em consonância com as Orientações relativas à certificação enquanto instrumento para as transferências[16]. Todavia, o presente parecer não aborda esta questão, pois não é da competência do CEPD.

29 O CEPD recorda igualmente a necessidade de os critérios de certificação serem disponibilizados em consonância com o artigo 42.º, n.º 8, do RGPD e, em especial, em caso de certificação a utilizar como instrumento para as transferências, em consonância com o artigo 13.º, n.º 1, alínea f), do RGPD, aos titulares dos dados cujos dados pessoais serão transferidos com base na certificação emitida ao importador de dados.

30 O Comité observa, conforme clarificado nas definições do sistema, que as referências a «autoridades de proteção de dados competentes» constantes do sistema têm o significado de autoridades de proteção de dados no EEE[17].

31 Da mesma forma, o Comité observa que as referências a «legislação aplicável» e a «legislação de países terceiros» se referem à legislação aplicável ao requerente e/ou aos dados pessoais tratados no alvo da avaliação, na medida em que essa legislação não imponha limitações aos direitos de proteção de dados que vão além do necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1, do RGPD, seja proporcionada ao objetivo visado, respeite a essência do direito à proteção de dados e preveja medidas específicas para salvaguardar os direitos e interesses fundamentais dos titulares dos dados.

2.1 Âmbito do procedimento de certificação e alvo da avaliação

32 A extensão do sistema de certificação Europrivacy para a certificação de importadores de dados nos termos do artigo 46.º destina-se a ser utilizada nos termos do artigo 42.º, n.º 2, e do artigo 46.º, n.º 2, alínea f), do RGPD por importadores de dados localizados fora do EEE que não estão sujeitos ao RGPD nos termos do artigo 3.º, com vista a demonstrar a existência de garantias adequadas no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais Assim, o seu âmbito de aplicação difere do da certificação Europrivacy nos termos do artigo 42.º, n.º 1, a que se refere o n.º 3 do presente parecer, uma vez que prevê critérios específicos a aplicar e respeitar quando é emitida uma certificação Europrivacy a requerentes (responsáveis pelo tratamento ou subcontratantes) localizados fora do EEE que atuarão como importadores de dados.

33 O sistema de certificação Europrivacy enquanto instrumento para as transferências é um sistema destinado a ser aplicado tanto a uma transferência singular como a um conjunto de transferências, quando estas últimas estão estreitamente correlacionadas. O sistema de certificação contém critérios de certificação para as operações de tratamento no âmbito do

[16] Orientações 07/2022, secção 2.

[17] Ver a definição de «AC competente» prevista nos critérios Europrivacy: «autoridade competente em matéria de proteção de dados» refere-se às autoridades responsáveis pela proteção de dados no EEE. De um modo geral, refere-se às autoridades nacionais de proteção de dados que possuem competência para impor a conformidade dos dados pessoais tratados pelo alvo da avaliação. No caso de uma certificação no âmbito do RGPD emitida a um importador de dados nos termos do artigo 46.º do RGPD, a autoridade de proteção de dados competente é a do exportador de dados no EEE, exceto para apresentar uma reclamação, caso em que qualquer autoridade do EEE é competente.

alvo da avaliação (ToE) realizadas em dados pessoais transferidos para o importador de dados, incluindo o trânsito, caso esteja sob o controlo do mesmo importador[18].

34 O CEPD toma nota de que o âmbito de aplicação deste sistema de certificação não abrange os responsáveis conjuntos pelo tratamento e que, nos casos em que a responsabilidade conjunta pelo tratamento esteja incluída no ToE, o organismo de certificação deve recusar-se a emitir a certificação[19].

2.2 Operações de tratamento

35 Os critérios de certificação abordam as componentes pertinentes das operações de tratamento dos dados pessoais transferidos no âmbito do ToE. Em especial, os critérios de certificação preveem garantias para o tratamento de categorias especiais de dados pessoais (secção GI.2 dos critérios sobre o tratamento de dados especiais). A este respeito, o Comité congratula-se com o facto de os critérios de certificação atualizados (critério GI.2.1.3 sobre as garantias adicionais para o tratamento de categorias especiais de dados pessoais) exigirem igualmente que o requerente disponha de limitações e garantias adicionais, adaptadas à natureza específica dos dados e aos riscos correspondentes, caso o tratamento envolva categorias especiais de dados pessoais.

2.3 Princípios do tratamento de dados

36 Na secção GI.1, os critérios de certificação abordam adequadamente os princípios da proteção de dados, de forma coerente com os previstos no artigo 5.º do RGPD, com o objetivo de assegurar que o tratamento de dados no ToE é lícito e proporcionado.

37 Em especial, no âmbito do critério de certificação GI.1.1.2, o princípio da limitação da finalidade e as obrigações pertinentes do requerente para o cumprir estão devidamente desenvolvidos. O CEPD observa que os dados pessoais transferidos só podem ser tratados para as finalidades para as quais foram transferidos. O critério de certificação GI.1.1.3, em consonância com as atuais cláusulas contratuais-tipo adotadas pela Comissão Europeia[20], identifica as únicas isenções ao abrigo das quais os dados podem ser objeto de tratamento posterior para outras finalidades que não aquelas para as quais foram inicialmente recolhidos (ou seja, consentimento prévio informado, obrigação legal, interesses vitais dos titulares dos dados e processos judiciais).

38 O CEPD observa igualmente que o requerente é obrigado a apresentar uma avaliação escrita, a fim de assegurar que a legislação e as práticas no país terceiro não o impedem de cumprir os critérios Europrivacy, respeitam a essência dos direitos e liberdades fundamentais dos titulares dos dados e não excedem o que é necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1, do RGPD. A entidade certificada tem de rever a avaliação sempre que alterações regulamentares ou organizativas sejam suscetíveis de prejudicar o cumprimento dos critérios, ou afetar o ToE ou os direitos dos titulares dos dados, e seja necessário informar o organismo de certificação (critério GI 1.1.1).

[18] Ver critérios de certificação GI.11.1.5 e GI.11.1.6.
[19] Europrivacy™/®, *Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR*, EP-CS.1.DI, secção 3.2.2, onde também se afirma claramente que a responsabilidade conjunta pelo tratamento está excluída do âmbito de aplicação do sistema no caso de requerentes abrangidos pelo artigo 46.º.
[20] Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

2.4 Obrigações gerais dos responsáveis pelo tratamento e dos subcontratantes

39 Os critérios de certificação refletem as obrigações do responsável pelo tratamento nos termos do artigo 24.º do RGPD (secção GI.4 dos critérios) e exigem a avaliação dos acordos contratuais entre o subcontratante e o responsável pelo tratamento, em conformidade com o artigo 28.º do RGPD (secção GI.5 dos critérios de certificação sobre os subcontratantes ou subcontratantes ulteriores), com o objetivo de garantir que os subcontratantes que participam no tratamento de dados do ToE assegurem o mesmo nível de proteção de dados que o exigido pelos critérios Europrivacy. A este respeito, o CEPD congratula-se com os diferentes critérios de certificação relacionados com a contratação de subcontratantes ulteriores no caso de requerentes que atuam como responsáveis pelo tratamento ou como subcontratantes, uma vez que esta distinção permite refletir melhor a separação de funções e responsabilidades entre os intervenientes na cadeia de tratamento (secção GI.5.1).

40 Os critérios de certificação exigem que todos os requerentes nomeiem um encarregado da proteção de dados (EPD), mesmo caso o requerente não seja obrigado a designar um EPD nos termos do artigo 37.º do RGPD. Os critérios de certificação verificam se o EPD cumpre os mesmos requisitos que os previstos nos artigos 37.º a 39.º (secção GI.9 dos critérios de certificação sobre a designação do encarregado da proteção de dados), a fim de assegurar que o papel, a função e a qualificação do encarregado da proteção de dados que supervisiona a conformidade do tratamento de dados no ToE cumprem os requisitos necessários. A este respeito, o Comité observa que a designação de um encarregado da proteção de dados não constitui uma obrigação imperativa para os responsáveis pelo tratamento e os subcontratantes nos termos do RGPD, a menos que estejam preenchidas as condições previstas no artigo 37.º, n.º 1, do RGPD.

41 Os critérios de certificação exigem a verificação do conteúdo dos registos de atividades de tratamento, em consonância com o artigo 30.º do RGPD (secção GI.5.3 dos critérios sobre os registos de atividades de tratamento). A este respeito, o Comité congratula-se com o facto de os critérios de certificação exigirem claramente que os requerentes cooperem com os pedidos apresentados pelas autoridades de proteção de dados do EEE competentes para os exportadores e lhes facultem, mediante pedido, o registo das atividades de tratamento (critério GI.5.3.5).

2.5 Direitos dos titulares dos dados

42 Os critérios de certificação abordam os direitos do titular dos dados em conformidade com o capítulo III do RGPD e exigem a adoção das respetivas medidas com o objetivo de assegurar que o tratamento no ToE respeita e permite o exercício efetivo dos direitos dos titulares dos dados. A secção GI.3 dos critérios de certificação sobre a transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados prevê, entre outras garantias, que os titulares dos dados têm o direito de ser informados sobre o tratamento de dados e sobre como podem exercer os seus direitos. O CEPD congratula-se, em especial, com o facto de os critérios de certificação preverem que o requerente deve dispor de procedimentos ou de um mecanismo para tratar os pedidos dos titulares dos dados e, caso não dê seguimento aos pedidos apresentados pelos titulares dos dados, informá-los das razões que o levaram a não tomar medidas, do direito de apresentar uma reclamação a uma autoridade de proteção de dados do EEE e de intentar uma ação judicial.

2.6 Medidas técnicas e organizativas, e avaliação dos riscos para os direitos e liberdades dos titulares dos dados

43 Os critérios de certificação exigem a aplicação de medidas técnicas e organizativas que demonstrem um nível de segurança adequado ao risco do tratamento e que implementem a proteção de dados desde a conceção e por defeito, em conformidade com os artigos 25.º e 32.º do RGPD (secção GI.6 dos critérios de certificação sobre a proteção de dados desde a conceção e por defeito, e a segurança do tratamento), com o objetivo de garantir que os dados tratados no ToE beneficiem de uma segurança adequada e da proteção de dados desde a conceção e por defeito. Além disso, os critérios de certificação incluem uma secção (ou seja, critérios T sobre medidas tecnológicas e organizativas, verificações e controlos), em que as medidas técnicas e organizativas são abordadas de forma exaustiva.

44 Os critérios de certificação exigem a aplicação de medidas para assegurar que as obrigações de notificação de violações de dados pessoais são cumpridas em tempo útil e no âmbito de aplicação, em conformidade com os artigos 33.º e 34.º do RGPD (secção GI.7 dos critérios de certificação sobre a gestão de violações de dados).

45 A este respeito, o Comité observa que os critérios de certificação incluem uma lista pormenorizada (critério GI.7.1.1 sobre o dever de documentar as violações de dados) das informações que o requerente deve documentar quando ocorre uma violação de dados (por exemplo, as categorias de dados pessoais que são ou podem ser afetadas, o número aproximado de titulares de dados que são ou podem ser afetados, as categorias e o número aproximado de registos de dados pessoais a que diz respeito ou pode dizer respeito, e as consequências prováveis da violação de dados pessoais). Além disso, o CEPD congratula-se com o facto de os critérios de certificação preverem claramente que, caso a violação de dados pessoais seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, o requerente deve dispor de regras, um procedimento ou um mecanismo para informar a autoridade de proteção de dados do EEE competente para o(s) exportador(es) e os titulares dos dados, em conformidade com os requisitos constantes dos artigos 33.º e 34.º do RGPD (critério GI.7.1.2 sobre a obrigação do responsável pelo tratamento de notificar e comunicar violações de dados e GI.7.2 sobre a comunicação de uma violação de dados pessoais ao titular dos dados).

46 O CEPD congratula-se igualmente com o facto de os critérios de certificação exigirem a avaliação do risco para os direitos e liberdades das pessoas singulares decorrente do tratamento de dados abrangido pelo ToE, prevendo o envolvimento da autoridade de proteção de dados do EEE competente para o(s) exportador(es), em conformidade com o artigo 35.º do RGPD [secção GI.8 dos critérios de certificação sobre a obrigação de avaliar se é necessária uma avaliação de impacto sobre a proteção de dados (AIPD)].

2.7 Critérios para demonstrar a existência de garantias adequadas para a transferência de dados pessoais

47 Os critérios de certificação exigem a identificação de todas as transferências de dados pessoais para países terceiros e organizações internacionais envolvidas no ToE e a fundamentação da escolha feita relativamente ao mecanismo de transferência de dados que prevê garantias adequadas, coerentes com as previstas no capítulo V do RGPD (secção GI.10 dos critérios sobre as transferências de dados pessoais para países terceiros ou organizações internacionais). O CEPD reconhece que estes critérios de certificação serão aplicáveis no caso de «transferências ulteriores» de dados pessoais envolvidos no ToE para o mesmo país terceiro em que o requerente está localizado ou para um país terceiro diferente.

O Comité congratula-se com o facto de estes critérios de certificação exigirem especificamente que o requerente disponha de um levantamento ou registo claro de todos os fluxos de dados pessoais no âmbito do ToE e das transferências identificadas para países terceiros e organizações internacionais, bem como adote a finalidade adequada para a transferência de dados pessoais em consonância com as previstas no capítulo V do RGPD, tendo em conta a obrigação de não comprometer o nível de proteção dos dados pessoais proporcionado no EEE.

48 O CEPD observa igualmente que os critérios de certificação exigem que o requerente tenha realizado uma avaliação de impacto da transferência e, se necessário, adotado medidas complementares para assegurar que o nível de proteção dos dados transferidos não seja comprometido (critério GI.10.1.5).

3 Critérios adicionais para um Selo Europeu de Proteção de Dados a utilizar enquanto instrumento para as transferências

49 De acordo com as Orientações relativas à certificação enquanto instrumento para as transferências, o sistema de certificação deve assegurar que o importador de dados avaliou «as regras e práticas do país terceiro onde opera e se estas impedem o importador de cumprir os seus compromissos no âmbito da certificação». A este respeito, o Comité observa que o critério ADI.2.1.5 define as condições a cumprir pelos requerentes aquando da definição do ToE durante a revisão do seu pedido de certificação. Em especial, antes de considerar uma auditoria de certificação, exige que o organismo de certificação verifique se o requerente está em condições de demonstrar que a legislação e as práticas do país terceiro não impedem o cumprimento dos requisitos de certificação. Se tal não for o caso, o processo de certificação será interrompido durante a fase de pedido.

50 O Comité observa igualmente que, ao abrigo do critério GI.11.1.3, o requerente deve analisar a legislação e as práticas do país terceiro e identificar o potencial impacto nos direitos e liberdades do titular dos dados cujos dados podem ser importados e dispor de regras, procedimentos ou políticas para disponibilizar a sua análise escrita da legislação e das práticas locais ao organismo de certificação e às autoridades competentes em matéria de proteção de dados, mediante pedido.

51 Além disso, de acordo com as Orientações relativas à certificação enquanto instrumento para as transferências, os critérios de certificação preveem que, se necessário, o requerente deve ter adotado medidas complementares para assegurar que o nível de proteção dos dados pessoais transferidos não seja comprometido e que, se tal não for possível, o importador de dados tem de informar o exportador de dados e a transferência de dados pessoais deve ser suspensa ou interrompida (critério GI.11.1.3).

52 Por outro lado, o Comité observa que o sistema Europrivacy, em consonância com o artigo 42.º, n.º 2, do RGPD, prevê que deve ser assinado um contrato entre o importador de dados e o exportador de dados, incluindo os compromissos vinculativos e com força executiva pertinentes, antes da realização de qualquer transferência e prevê um modelo desse contrato. A este respeito, o CEPD observa que, em conformidade com as Orientações relativas à certificação enquanto instrumento para as transferências, os critérios de certificação incluem uma lista pormenorizada do conteúdo dos compromissos vinculativos e com força executiva que devem ser assumidos pelo requerente em relação a cada exportador no EEE, entre os quais a obrigação de reconhecer o direito dos titulares dos dados, enquanto terceiros

beneficiários, de fazer cumprir, contra o importador de dados titular de uma certificação, as regras ao abrigo da certificação, de cooperar com as autoridades de proteção de dados do EEE competentes para os exportadores de dados (nomeadamente ao aceitar as suas auditorias e inspeções, tendo em conta os seus conselhos e respeitando as suas decisões), de respeitar qualquer decisão vinculativa emitida na jurisdição e nos tribunais dos Estados do EEE relacionada com a certificação, de tratar apenas os dados recebidos durante a validade do certificado, bem como de devolver e/ou apagar os dados recebidos se o certificado for retirado. Os critérios de certificação preveem igualmente que o requerente deve garantir que não tem motivos para crer que a legislação e as práticas do país terceiro aplicáveis ao tratamento no ToE, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o acesso a autoridades públicas, o impedem de cumprir os seus compromissos ao abrigo da certificação e de informar o exportador de dados de quaisquer alterações pertinentes da legislação ou das práticas a este respeito (critério GI.11.1.1 sobre os compromissos vinculativos e com força executiva para importadores de dados).

4 Conclusões/Recomendações

53 Em conclusão, o CEPD considera que os critérios de certificação Europrivacy destinados a ser utilizados enquanto instrumento para as transferências são coerentes com o RGPD e aprova-os no âmbito da atribuição do Comité definida no artigo 70.º, n.º 1, alínea o), do RGPD, resultando numa certificação comum (Selo Europeu de Proteção de Dados) a utilizar enquanto instrumento para as transferências.

54 O CEPD considera que os critérios de certificação fazem parte integrante do sistema de certificação e regista o procedimento de certificação Europrivacy no registo público dos procedimentos de certificação e dos selos e marcas de proteção de dados, nos termos do artigo 42.º, n.º 8, do RGPD.

5 Observações finais

55 O presente parecer é dirigido à AC do Luxemburgo e será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

Pelo Comité Europeu para a Proteção de Dados

A presidente

Anu Talus