Diretrizes

Orientações 07/2022 relativas à certificação enquanto instrumento para as transferências

Versão 2.0

Adotadas em 14 de fevereiro de 2023

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

HISTÓRICO DE VERSÕES

Versão 1.0	14 de junho de 2022	Adoção das orientações para consulta pública
Versão 2.0	14 de fevereiro de 2023	Adoção das orientações após consulta pública

RESUMO

O Regulamento Geral sobre a Proteção de Dados (RGPD) exige, no seu artigo 46.º, que os exportadores de dados estabeleçam garantias adequadas para as transferências de dados pessoais para países terceiros ou organizações internacionais. Para o efeito, o RGPD diversifica as garantias adequadas que os exportadores de dados podem utilizar ao abrigo do artigo 46.º para enquadrar as transferências para países terceiros, introduzindo, nomeadamente, a certificação enquanto novo procedimento de transferência [artigo 42.º, n.º 2, e artigo 46.º, n.º 2, alínea f), do RGPD].

As presentes orientações fornecem instruções sobre a aplicação do artigo 46.º, n.º 2, alínea f), do RGPD no que diz respeito às transferências de dados pessoais para países terceiros ou para organizações internacionais com base na certificação. O documento está estruturado em quatro secções com um anexo.

A primeira parte do presente documento («GENERALIDADES») esclarece que as orientações complementam as já existentes Orientações 1/2018 relativas à certificação, que têm um caráter geral, e incidem sobre requisitos específicos do capítulo V do RGPD quando a certificação é utilizada como instrumento de transferência. Nos termos do artigo 44.º do RGPD, qualquer transferência de dados pessoais para países terceiros ou organizações internacionais deve cumprir as condições das outras disposições do RGPD, para além de cumprir o disposto no capítulo V do RGPD. Por conseguinte, numa primeira fase, há que assegurar o cumprimento das disposições gerais do RGPD e, numa segunda fase, há que respeitar as disposições do capítulo V do RGPD. São descritos os intervenientes envolvidos e as suas principais funções neste contexto, com especial destaque para o papel do importador de dados a quem será concedida a certificação e do exportador de dados que a utilizará como instrumento para enquadrar as suas transferências (tendo em conta que a responsabilidade pela conformidade do tratamento de dados continua a ser do exportador de dados). Neste âmbito, a certificação pode também incluir medidas que complementem os instrumentos de transferência, a fim de assegurar o cumprimento do nível de proteção dos dados pessoais da UE. A primeira parte das orientações contém igualmente informações sobre o processo de obtenção da certificação a utilizar como instrumento para as transferências.

A segunda parte das presentes orientações («APLICAÇÃO DAS ORIENTAÇÕES SOBRE OS REQUISITOS DE ACREDITAÇÃO») recorda que os requisitos para a acreditação de um organismo de certificação constam da norma ISO 17065 e devem ser interpretados à luz das Orientações 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do RGPD e do seu anexo no contexto do capítulo V. Contudo, no âmbito de uma transferência, as presentes orientações explicam em maior pormenor alguns dos requisitos de acreditação aplicáveis ao organismo de certificação.

A terceira parte das presentes orientações («CRITÉRIOS ESPECÍFICOS DE CERTIFICAÇÃO») fornece instruções sobre os critérios de certificação já enumerados nas Orientações 1/2018 e estabelece critérios específicos adicionais que devem ser incluídos num mecanismo de certificação a utilizar como instrumento para as transferências para países terceiros. Estes critérios abrangem a avaliação da legislação dos países terceiros, as obrigações gerais dos exportadores e importadores, as regras em matéria de transferências ulteriores, as vias de recurso e execução, o processo e as ações para situações em que a legislação e as práticas nacionais impedem o cumprimento dos compromissos assumidos no âmbito da certificação, e os pedidos de acesso aos dados por parte das autoridades de países terceiros.

A quarta parte das presentes orientações («COMPROMISSOS VINCULATIVOS E COM FORÇA EXECUTIVA A ASSUMIR») apresenta os elementos que devem ser abordados nos compromissos vinculativos e com força executiva que os responsáveis pelo tratamento ou subcontratantes não sujeitos ao RGPD devem assumir para fornecer garantias adequadas em relação aos dados transferidos para países terceiros. Estes compromissos, que podem ser estabelecidos em diferentes instrumentos, incluindo contratos, devem incluir, em especial, a garantia de que o importador não tem motivos para crer que a legislação e as práticas do país terceiro aplicáveis ao tratamento em causa, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o acesso por parte das autoridades públicas, o impeçam de cumprir os seus compromissos no âmbito da certificação.

O ANEXO das presentes orientações inclui alguns exemplos de medidas complementares em consonância com as enumeradas no anexo II das Recomendações 01/2020 (Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE), no contexto da utilização da certificação enquanto instrumento para as transferências. São apresentados exemplos com vista a chamar a atenção para situações críticas.

ÍNDICE

O Comité Europeu para a Proteção de Dados,

Tendo em conta o artigo 70.º, n.º 1, alínea e), 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 EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[1],

Tendo em conta os artigos 12.º e 22.º do seu regulamento interno,

ADOTOU AS SEGUINTES ORIENTAÇÕES

1 GENERALIDADES

1.1 Objetivo e âmbito de aplicação

1. O presente documento visa fornecer orientações sobre a aplicação do artigo 46.º, n.º 2, alínea f), do RGPD no que diz respeito às transferências de dados pessoais para países terceiros ou para organizações internacionais com base na certificação. O CEPD já publicou orientações gerais relativas à certificação[2] e à acreditação[3] ao abrigo do RGPD. Por conseguinte, estas novas orientações refletem apenas os aspetos específicos relativos à certificação enquanto instrumento para as transferências. Especificam a aplicação do artigo 46.º, n.º 2, alínea f), e do artigo 42.º, n.º 2, do RGPD, fornecendo orientações práticas a este respeito e introduzindo novos elementos nas orientações já publicadas.

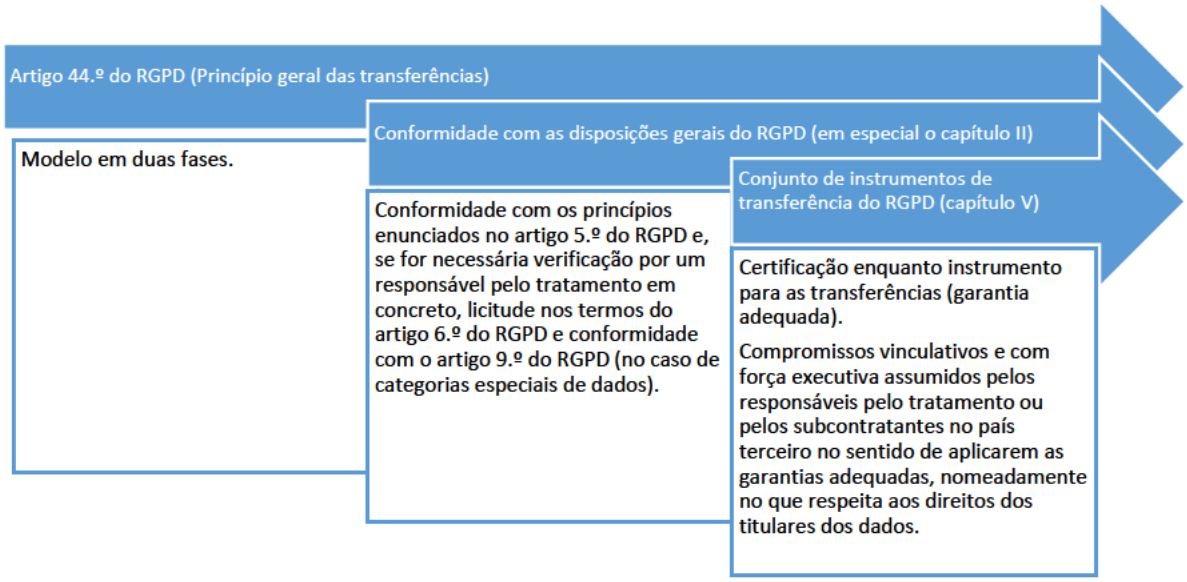
2. O CEPD avaliará o funcionamento das presentes orientações à luz da experiência adquirida com a sua aplicação prática e fornecerá instruções adicionais para clarificar a aplicação dos elementos a seguir enumerados, incluindo o papel do acordo de certificação no que diz respeito aos compromissos vinculativos e com força executiva referidos no artigo 46.º, n.º 2, alínea f), do RGPD.

1.2 Regras gerais aplicáveis às transferências internacionais

3. Nos termos do artigo 44.º do RGPD, qualquer transferência de dados pessoais para países terceiros[4] ou organizações internacionais deve cumprir as condições das outras disposições do RGPD, para além de cumprir o disposto no capítulo V do RGPD. Por conseguinte, cada transferência deve respeitar, nomeadamente, os princípios de proteção de dados previstos no artigo 5.º do RGPD, ser lícita em conformidade com o artigo 6.º do RGPD e cumprir o artigo 9.º do RGPD no caso de categorias especiais de dados. Desta forma, deve ser aplicado um teste em duas fases. Numa primeira fase, há que assegurar o cumprimento das disposições gerais do RGPD e, numa segunda fase, há que respeitar as disposições do capítulo V do RGPD.

---

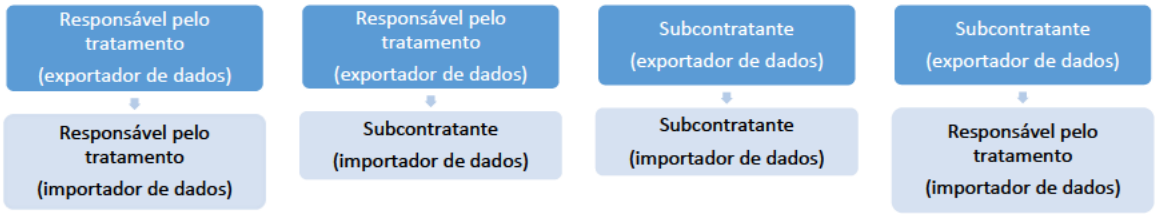
[1] As referências a «Estados-Membros» ao longo do presente documento devem ser entendidas como referências a «Estados do EEE».
[2] Orientações 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679.
[3] Orientações 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679).
[4] *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (não traduzidas para português), página 4.



4. O RGPD especifica no artigo 46.º que «[n]ão tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes 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». Nos termos do artigo 46.º, n.º 2, alínea f), do RGPD, essas garantias adequadas podem ser prestadas por um mecanismo de certificação aprovado, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.

5. Consequentemente, o exportador de dados pode decidir confiar na certificação obtida por um importador de dados como elemento para demonstrar o cumprimento das suas obrigações, nomeadamente nos termos do artigo 24.º, n.º 3, ou do artigo 28.º, n.º 5, do RGPD. O importador de dados pode optar por apresentar um pedido de certificação para demonstrar a existência de garantias adequadas.

6. Tanto o exportador de dados como o importador de dados podem desempenhar diferentes funções (por exemplo, enquanto responsáveis pelo tratamento ou subcontratantes)[5], dependendo do tratamento previsto no capítulo V, o que resulta em responsabilidades distintas:



7. Para além da utilização da certificação ou de quaisquer outros instrumentos ou procedimentos de transferência a que se referem os artigos 45.º e 46.º, o artigo 49.º do RGPD estabelece que, num número limitado de situações específicas, podem ser efetuadas transferências internacionais de dados

[5] Consultar *infra*: APLICAÇÃO DAS ORIENTAÇÕES SOBRE OS CRITÉRIOS DE CERTIFICAÇÃO.

quando não for cumprido qualquer outro procedimento previsto no capítulo V[6]. Contudo, conforme explicado em orientações anteriores emitidas pelo CEPD, as derrogações previstas no artigo 49.º do RGPD devem ser interpretadas de forma restritiva e dizem respeito principalmente a atividades de tratamento ocasionais e não repetitivas[7].

1.3 Quem são os intervenientes envolvidos e qual é o seu papel na certificação enquanto instrumento para as transferências?

8. O **Comité Europeu para a Proteção de Dados (CEPD)** está habilitado a aprovar critérios de certificação a nível do EEE (Selo Europeu de Proteção de Dados) e a emitir pareceres sobre os projetos de decisão das autoridades de controlo sobre os critérios de certificação e os requisitos de acreditação dos organismos de certificação, a fim de assegurar a coerência. É também competente pela recolha de todos os mecanismos de certificação de todos os selos e marcas de proteção de dados aprovados num registo e pela sua disponibilização ao público[8].

9. As **autoridades de controlo (AC)** aprovam os critérios de certificação quando o mecanismo de certificação não é um Selo Europeu de Proteção de Dados[9]. Podem também acreditar o organismo de certificação, conceber os critérios de certificação e emitir a certificação, se tal for estabelecido pelo direito nacional do seu Estado-Membro[10].

10. O **organismo nacional de acreditação** pode acreditar organismos de certificação terceiros utilizando a norma ISO 17065 e os requisitos de acreditação adicionais das AC, que devem estar em conformidade com a secção 2 das presentes orientações. Em alguns Estados-Membros, a AC competente pode também assegurar a acreditação, que pode ainda ser realizada por um organismo nacional de acreditação ou por ambas as entidades.

11. O **proprietário do sistema** é uma organização que estabeleceu critérios de certificação e os requisitos metodológicos de acordo com os quais a conformidade deve ser avaliada. A organização que realiza as avaliações pode ser a mesma organização que desenvolveu e que possui o sistema, mas pode haver acordos segundo os quais uma organização possui o sistema e outra(s) realiza(m) as avaliações na qualidade de organismo(s) de certificação.

12. Dependendo do direito nacional, em alternativa às AC, o **organismo de certificação** acreditado da forma acima referida pode emitir as certificações[11]. Poderá também conceber os critérios de certificação e, dessa forma, ser proprietário do sistema (ver ponto 11 *supra*). Para permitir o exercício efetivo dos poderes de correção consagrados no artigo 58.º, n.º 2, alínea f), do RGPD, é obrigatório que tenha um estabelecimento no EEE. No entanto, o organismo de certificação pode subcontratar atividades a peritos locais ou a estabelecimentos fora do EEE, que realizarão atividades de auditoria

---

[6] Para mais informações sobre o artigo 49.º e a sua articulação com o artigo 46.º em geral, ver as Orientações 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679.
[7] Orientações 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679, página 5.
[8] Artigo 42.º, n.º 8, do RGPD.
[9] Orientações 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679, ponto 2.2.
[10] Artigo 42.º, n.º 5, e artigo 43.º, n.º 1, do RGPD.
[11] Artigo 42.º, n.º 5, do RGPD.

em seu nome[12]. Porém, o organismo de certificação não pode subcontratar a decisão relativa à concessão ou não concessão de uma certificação.

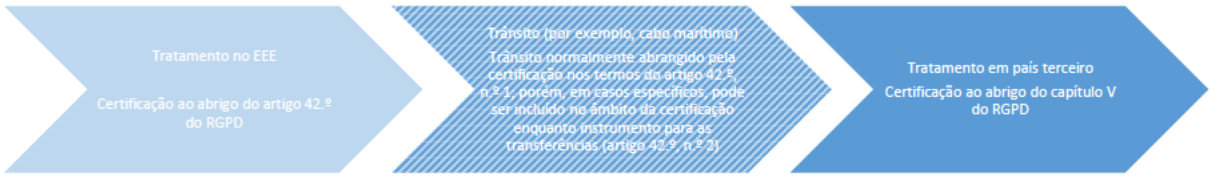
13. O **importador de dados** é a entidade (responsável pelo tratamento ou subcontratante) do país terceiro que recebe dados de um exportador de dados.

14. O **exportador de dados** é a entidade (responsável pelo tratamento ou subcontratante) que transfere dados do EEE para um importador de dados. O exportador de dados deve assegurar a conformidade com o capítulo V.

1.4 Quais são o âmbito de aplicação e o objeto da certificação enquanto instrumento para as transferências?

15. Um mecanismo de certificação enquanto instrumento para as transferências ao abrigo do artigo 42.º, n.º 2, deve ter por objetivo assegurar garantias adequadas para o tratamento de dados pessoais nos termos do artigo 46.º, n.º 2, alínea f). A certificação demonstra a existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes fora do EEE ou que constituam uma organização internacional que receba dados dos responsáveis pelo tratamento ou subcontratantes do EEE para fazer face aos riscos específicos da transferência de dados pessoais.

16. Em geral, a operação de transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, em si mesma, um tratamento de dados pessoais na aceção do artigo 4.º, ponto 2, do RGPD, efetuado num Estado-Membro[13] e, por conseguinte, passível de certificação nos termos do artigo 42.º, n.º 1, do RGPD. Contudo, algumas situações, dependendo do contexto, podem incluir o trânsito no âmbito da certificação enquanto instrumento para as transferências. Por conseguinte, o objeto da certificação — que coincide com o alvo de avaliação (AA) durante a certificação[14] — deve, em geral, ser o tratamento dos dados recebidos do EEE pelo importador de dados no país terceiro e o trânsito, caso esteja sob o controlo do importador.



17. O objeto da certificação pode ser uma única operação de tratamento ou um conjunto de operações. Estas podem incluir os processos de governação no sentido de medidas organizativas, ou seja, como parte integrante de uma operação de tratamento[15].

---

[12] Os organismos de certificação devem avaliar os seus peritos locais em conformidade com a norma ISO 17065 e com os requisitos adicionais de acreditação estabelecidos pela autoridade de controlo [artigo 43.º, n.º 1, alínea b), do RGPD].

[13] Acórdão do Tribunal de Justiça de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, n.º 83.

[14] Orientações 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679, página 17.

[15] Orientações 1/2018 sobre a certificação e a definição de critérios de certificação em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679, página 16 (por exemplo, mecanismo de tratamento de reclamações).

18. A entidade requerente seria, por conseguinte, o importador de dados no país terceiro em relação ao seu objeto de certificação.

1.5 Qual deve ser o papel do exportador na utilização da certificação como instrumento para as transferências?

19. Em geral, a transferência pelo exportador de dados enquanto tal é diretamente abrangida pelo RGPD, o que significa que o exportador é obrigado a cumprir as obrigações que lhe incumbem por força do RGPD e, em especial, a certificar-se de que os dados são transferidos de forma segura, em conformidade com o artigo 32.º e o capítulo V, a fim de assegurar que o nível de proteção das pessoas singulares garantido pelo referido regulamento não seja comprometido (artigo 44.º do RGPD)[16]. Tal pode, evidentemente, ser certificado nos termos do artigo 42.º, n.º 1.

20. Além disso, 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, designadamente, 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. Por outro lado, o exportador 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.

21. Tendo em conta a sua responsabilidade pela aplicação de todas as disposições do capítulo V, o exportador tem também de avaliar se a certificação em que tenciona confiar enquanto instrumento de transferência é eficaz à luz da legislação e das práticas em vigor no país terceiro, aplicáveis à transferência em causa. Para efeitos desta avaliação e enquanto elemento importante para demonstrar o cumprimento da sua responsabilidade, o exportador de dados pode basear-se na verificação efetuada pelo organismo de certificação em relação à avaliação documentada da legislação e das práticas do país terceiro levada a cabo pelo importador.

22. Caso a avaliação do importador revele que este e/ou o exportador de dados podem ter de adotar medidas complementares previstas na certificação para assegurar um nível de proteção essencialmente equivalente ao previsto no EEE, o exportador de dados deve verificar as medidas

[16] A este respeito, é importante salientar que o artigo 44.º do RGPD prevê claramente que uma transferência possa ser efetuada não só por um responsável pelo tratamento, mas também por um subcontratante. Por conseguinte, haverá uma situação de transferência quando um subcontratante envia dados a outro subcontratante ou mesmo a um responsável pelo tratamento num país terceiro, de acordo com as instruções do seu responsável pelo tratamento [artigo 28.º, n.º 3, alínea a), do RGPD]. Nesses casos, o subcontratante atua como exportador de dados em nome do responsável pelo tratamento e tem de assegurar que as disposições do capítulo V são cumpridas para a transferência em causa, de acordo com as instruções do responsável pelo tratamento, incluindo a utilização de um instrumento de transferência adequado. Tendo em conta que a transferência é uma atividade de tratamento realizada por conta do responsável pelo tratamento, o responsável pelo tratamento é igualmente responsável e pode ser sujeito ao disposto no capítulo V, devendo igualmente assegurar que o subcontratante forneça garantias suficientes nos termos do artigo 28.º.

complementares previstas pelo importador de dados titular da certificação e se está em condições de dar resposta às medidas técnicas e (se for caso disso) complementares solicitadas pelo importador de dados.

23. Se essas disposições não forem cumpridas, o exportador de dados terá de exigir ao importador que aplique medidas complementares adaptadas ou que as estabeleça por si mesmo.

1.6 Qual é o processo de certificação enquanto instrumento para as transferências?

24. A certificação é voluntária, mas, quando solicitada, deve ser concedida através de um processo transparente baseado em regras obrigatórias. O RGPD deposita uma confiança considerável nos mecanismos de certificação privados enquanto «autorregulação regulamentada». Deste modo, os procedimentos em causa devem assegurar que os certificados cumpram materialmente os requisitos de garantias adequadas definidos no artigo 46.º do RGPD.

25. Por conseguinte, a certificação deve basear-se na avaliação dos critérios de certificação de acordo com uma metodologia de auditoria vinculativa. A aprovação desses critérios ficará a cargo das AC nacionais ou do CEPD, conforme descrito no artigo 42.º, n.º 5, do RGPD. Os critérios de certificação devem incluir requisitos para uma avaliação do tratamento efetuado pelo importador de dados, incluindo transferências ulteriores, e do quadro jurídico aplicável do país terceiro, a fim de evitar que as regras e práticas do país terceiro impeçam o importador de cumprir as suas obrigações ao abrigo da certificação.

26. Durante o processo de certificação, o alvo de avaliação deve ser verificado, à luz dos critérios de certificação, por um organismo de certificação acreditado pelo organismo nacional de acreditação ou pela AC competente[17].

27. De acordo com o artigo 43.º, n.º 1, do RGPD, um organismo de certificação que tenha um nível adequado de competência em matéria de proteção de dados emite e renova a certificação, após informar a AC para que esta possa exercer as suas competências nos termos do artigo 58.º, n.º 2, alínea h), sempre que necessário.

28. Nos termos do artigo 43.º, n.º 5, do RGPD, os organismos de certificação comunicam às AC competentes os motivos que levaram à concessão ou revogação da certificação solicitada. Tal não significa que o organismo de certificação necessite da autorização da AC para emitir a certificação. O organismo de certificação controlará a conformidade dos seus clientes com os critérios de certificação.

29. A AC tem o poder de correção de retirar a certificação ou de ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42.º e 43.º do RGPD, ou de ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação deixarem de estar cumpridos.

30. O Selo Europeu de Proteção de Dados para as transferências internacionais de dados pode servir de instrumento para abranger as transferências para países terceiros, acompanhado de compromissos vinculativos e com força executiva[18].

---

[17] Orientações 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679), p. 9.

[18] Ver o artigo 42.º, n.º 5, do RGPD e o ponto 35 das Orientações 1/2018 do CEPD relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento.

31. Não obstante, as certificações a utilizar como instrumento para as transferências também podem ser emitidas de acordo com os sistemas nacionais de certificação aprovados nos Estados do EEE. Assim sendo, só são válidas para transferências para países terceiros a partir de exportadores no Estado do EEE em que o sistema de certificação tenha sido aprovado, uma vez que não existe reconhecimento mútuo das diferentes certificações realizadas nos Estados do EEE. Porém, as AC dos diferentes Estados do EEE são livres de aprovar o mesmo mecanismo de certificação para as transferências[19].

2 APLICAÇÃO DAS ORIENTAÇÕES SOBRE OS REQUISITOS DE ACREDITAÇÃO

32. Os requisitos de acreditação de um organismo de certificação no que diz respeito às certificações enquanto instrumento para as transferências estão previstos na norma ISO 17065 e devem ser interpretados à luz das Orientações 4/201820 no contexto do capítulo V, conforme explicado abaixo.

33. O CEPD considera que os requisitos de acreditação adicionais elaborados com base nas Orientações 4/2018 e na norma ISO 17065, adotados em conformidade com o artigo 64.º, n.º 1, alínea c), do RGPD, já abrangem os requisitos específicos necessários para a acreditação de um organismo de certificação no que diz respeito às certificações enquanto instrumento para as transferências. No entanto, num cenário de transferência, alguns requisitos carecem de alguns aperfeiçoamentos em termos de notas explicativas e de interpretação.

34. No que diz respeito aos requisitos em matéria de recursos (ver requisito 6 das Orientações 4/2018, anexo 1), o organismo de certificação deve assegurar que dispõe dos recursos necessários para poder verificar se, tal como exigido pelos critérios de certificação, o importador efetuou devidamente e de forma correta a avaliação necessária da situação jurídica e das práticas do(s) país(es) terceiro(s) onde está estabelecido ou opera[21]. Esta avaliação deve ser realizada no que toca às atividades de tratamento a certificar como parte do AA em relação às garantias adequadas previstas no artigo 46.º do RGPD, e incluir as medidas complementares identificadas e aplicadas pelo importador, se necessário. Tal inclui também, por exemplo, um conhecimento significativo da legislação e das práticas locais aplicáveis e competências linguísticas adequadas em relação ao(s) país(es) terceiro(s).

35. No que diz respeito aos requisitos processuais (ver requisito 7 das Orientações 4/2018, anexo 1), o organismo de certificação deve assegurar que o processo de certificação pode ser verificado por eventuais auditorias no local, é realizado no que respeita ao tratamento que terá lugar no(s) país(es) terceiro(s) e que a avaliação abrange igualmente a aplicação na prática da legislação e das políticas em vigor no(s) país(es) terceiro(s).

36. Quanto aos requisitos relativos a alterações que afetam a certificação (ver requisito 7.10 das Orientações 4/2018, anexo 1), o organismo de certificação deve monitorizar as alterações da legislação

[19] Se uma AC avançar com a adoção dos critérios de certificação X por iniciativa nacional e, posteriormente, tendo em conta os critérios do sistema e a regulamentação nacional específica aplicável, outros países quiserem adotar os mesmos critérios de certificação, poderão fazê-lo sem desencadear um parecer do CEPD nos termos do artigo 64.º do RGPD e basear-se no parecer emitido à primeira AC, em conformidade com o artigo 64.º, n.º 3, do RGPD [ver, a este respeito, a referência ao documento «Guidance — Addendum» (Orientações — Adenda) (anexo das Orientações 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento), ponto 66].

[20] Orientações 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do RGPD e respetivo anexo.

[21] Ver ponto 12 *supra*.

e/ou da jurisprudência do(s) país(es) terceiro(s) que possam afetar o tratamento abrangido pelo âmbito de aplicação do AA.

3 CRITÉRIOS ESPECÍFICOS DE CERTIFICAÇÃO

37. No contexto da apreciação dos critérios específicos de certificação, as presentes orientações baseiam-se nas Orientações 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento (versão 3. 0), no correspondente anexo 2 relativo à análise e avaliação dos critérios de certificação em conformidade com o artigo 42.º, n.º 5, e com a Adenda *Certification criteria assessment* (Avaliação dos critérios de certificação).

38. O CEPD considera que os critérios de certificação elaborados com base no anexo 2 e na Adenda *Certification criteria assessment* (Avaliação dos critérios de certificação) das Orientações 1/2018 já abrangem a maioria dos critérios de certificação que devem ser tidos em conta na elaboração de um sistema de certificação a utilizar como instrumento para as transferências. No entanto, poderá ser necessário especificar mais pormenorizadamente alguns dos critérios existentes para os adaptar a um cenário de transferência específico (ver ponto 3.1). Além disso, poderá ser necessário formular critérios adicionais no sentido de aplicar as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados (ver ponto 3.2).

3.1 APLICAÇÃO DAS ORIENTAÇÕES SOBRE OS CRITÉRIOS DE CERTIFICAÇÃO

39. O âmbito do mecanismo de certificação e alvo de avaliação (AA) (ver anexo 2, secção 2.a) deve ser claramente descrito na respetiva documentação, nomeadamente no que respeita à transferência de dados pessoais para um país terceiro ou se se destina a abranger também o seu trânsito.

40. Ainda em relação ao âmbito do mecanismo de certificação e alvo de avaliação (AA) (ver anexo 2, secção 2.b), a documentação relevante deve descrever concretamente a que tipo de entidade (p. ex. responsável pelo tratamento e/ou subcontratante) o mecanismo de certificação é aplicável.

41. Novamente em relação ao âmbito do mecanismo de certificação e alvo de avaliação (AA) (ver anexo 2, secção 2.f), os critérios devem exigir que o AA seja definido concretamente, de modo a evitar mal-entendidos, incluindo, pelo menos:

42. A(s) operação(ões) de tratamento, inclusivamente no caso de estarem previstas transferências ulteriores:

    a) O objetivo;

    b) O tipo de entidade (p. ex. responsável pelo tratamento e/ou subcontratante);

    c) O tipo de dados transferidos, tendo em conta se estão envolvidas categorias especiais de dados pessoais, tal como definidas no artigo 9.º do RGPD;

    d) As categorias de titulares de dados;

    e) Os países onde é efetuado o tratamento de dados.

43. No que diz respeito à transparência e aos direitos dos titulares dos dados (ver anexo 2, secção 8), os critérios de certificação devem:

a) Exigir que sejam fornecidas informações sobre as atividades de tratamento aos titulares dos dados, inclusivamente, se for caso disso, sobre a transferência de dados pessoais para um país terceiro ou uma organização internacional (ver artigos 12.º, 13.º e 14.º do RGPD);

b) Exigir que aos titulares dos dados sejam garantidos os direitos de acesso, retificação, apagamento, limitação do tratamento, notificação da retificação, do apagamento ou da limitação do tratamento, oposição ao tratamento, bem como o direito de não ficar sujeito a decisões baseadas exclusivamente no tratamento automatizado, incluindo a definição de perfis, essencialmente equivalentes aos previstos nos artigos 15.º a 19.º, 21.º e 22.º do RGPD;

c) Exigir que o importador de dados titular de uma certificação estabeleça um procedimento adequado de tratamento das reclamações, a fim de assegurar o exercício efetivo dos direitos dos titulares dos dados;

d) Exigir que se avalie se, e em que medida, estes direitos são oponíveis para os titulares dos dados no país terceiro em causa, bem como quaisquer medidas adicionais adequadas que possam ter de ser postas em prática para os fazer cumprir, por exemplo exigindo que o importador aceite submeter-se à jurisdição da autoridade de controlo competente em relação ao(s) exportador(es) e cooperar com a mesma em quaisquer procedimentos destinados a assegurar o cumprimento desses direitos e, em especial, que aceite responder a inquéritos, submeter-se a auditorias e cumprir as medidas adotadas pela referida autoridade de controlo, incluindo medidas corretivas e compensatórias.

44. No que respeita às medidas técnicas e organizativas que garantam a proteção (anexo 2, secção 10.q), os critérios de certificação devem exigir que o importador informe o exportador e, se o importador atuar como responsável pelo tratamento, notifique a AC no EEE competente em relação ao(s) exportador(es) de dados das violações de dados e as comunique aos titulares dos dados sempre que a violação seja suscetível de resultar num elevado risco para os seus direitos e liberdades, em conformidade com os requisitos do artigo 34.º do RGPD.

3.2 CRITÉRIOS DE CERTIFICAÇÃO ESPECÍFICOS ADICIONAIS

45. Tendo em conta as garantias identificadas para outros instrumentos de transferência ao abrigo do artigo 46.º do RGPD (tais como regras vinculativas aplicáveis às empresas ou códigos de conduta) e a fim de assegurar um nível de proteção coerente, e atendendo ao acórdão do TJUE no processo Schrems II, o CEPD considera que o mecanismo de certificação a utilizar como instrumento para as transferências para países terceiros deve incluir também os critérios a seguir enunciados.

1. Avaliação da legislação do país terceiro

a) Os critérios exigem que o importador tenha avaliado as regras e práticas do país terceiro onde opera e se estas impedem o importador de cumprir os seus compromissos no âmbito da certificação?

b) Os critérios exigem que o importador documente a avaliação das regras e práticas do país terceiro onde opera e mantenha a documentação à disposição do organismo de certificação e, mediante pedido, à disposição do exportador de dados e da AC no EEE competente em relação ao exportador de dados?

c) Os critérios exigem que o importador tenha identificado e aplicado as medidas organizativas e técnicas para proporcionar as garantias adequadas nos termos do artigo 46.º do RGPD, tendo em conta as «Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE»?

d) Os critérios exigem que o importador documente as medidas organizativas e técnicas efetivamente aplicadas para proporcionar as garantias adequadas nos termos do artigo 46.º do RGPD e mantenha a documentação à disposição do organismo de certificação e, mediante pedido, à disposição do exportador de dados e das autoridades competentes em matéria de proteção de dados?
e) Os critérios exigem que o importador tenha identificado e aplicado as medidas organizativas e técnicas para garantir a segurança dos dados pessoais transferidos, tendo em conta as «Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE», se o trânsito estiver incluído no âmbito da certificação enquanto instrumento para as transferências?
f) Os critérios exigem uma garantia ao organismo de certificação e ao exportador de que o importador não tem motivos para crer que a legislação e as práticas que lhe são aplicáveis o possam impedir de cumprir as suas obrigações ao abrigo da certificação?

2. Obrigações gerais dos exportadores e importadores

a) Os critérios exigem que se estabeleça, em acordos contratuais (por exemplo, num contrato de prestação de serviços existente) entre exportadores e importadores, uma descrição da transferência específica a que a certificação se aplica e que os direitos de terceiros beneficiários são reconhecidos aos titulares dos dados em causa?

b) Na medida em que os critérios exijam um conteúdo específico para estes acordos ou instrumentos contratuais e seja fornecido um modelo, os critérios exigem que sejam também objeto de avaliação?

3. Regras relativas às transferências ulteriores

a) Os critérios exigem que as transferências ulteriores estejam sujeitas a garantias específicas, em conformidade com os requisitos do capítulo V do RGPD, de modo a garantir que o nível de proteção assegurado no EEE não seja comprometido, e os critérios exigem que seja mantida documentação adequada à disposição do organismo de certificação e, mediante pedido, à disposição do exportador de dados e da AC no EEE competente em relação ao(s) exportador(es) de dados?

4. Vias de recurso e execução

a) Os critérios preveem que os titulares dos dados possam fazer valer os seus direitos enquanto terceiros beneficiários contra o importador de dados perante o tribunal do EEE da residência habitual do titular dos dados, ou junto de uma organização internacional, incluindo a indemnização pelos danos sofridos pelo titular dos dados em caso de não conformidade do importador com o sistema de certificação aplicável?
b) Os critérios permitem avaliar adequadamente se um importador é responsável no EEE pelos danos sofridos pelo titular dos dados em caso de não conformidade com o sistema de certificação aplicável?
c) Os critérios exigem que os titulares dos dados possam apresentar uma reclamação contra o importador junto de uma autoridade de controlo no EEE, em especial no Estado do EEE da sua residência habitual, local de trabalho ou competente em relação ao(s) exportador(es) de dados?

d) Os critérios exigem que o importador coopere com a autoridade de controlo no EEE competente em relação ao(s) exportador(es) de dados e aceite ser auditado e inspecionado por esta, ter em conta o seu parecer e respeitar as suas decisões?

5. Processo e ações para situações em que a legislação nacional impede o cumprimento dos compromissos assumidos no âmbito da certificação

a) Os critérios exigem o compromisso de que, sempre que tenha razões para crer que as alterações na legislação e nas práticas que lhe são aplicáveis podem impedir o cumprimento das obrigações que lhe incumbem por força da certificação, o importador de dados de um país terceiro ou de uma organização internacional informe imediatamente desse facto o organismo de certificação e o exportador de dados, para que este último possa avaliar se deve ou não cessar imediatamente as transferências?
b) Os critérios exigem uma descrição das medidas a tomar (incluindo a notificação do exportador no EEE e a adoção de medidas adicionais adequadas) se o importador de dados tomar conhecimento de legislação ou práticas de um país terceiro que impeçam o cumprimento das obrigações decorrentes da certificação, bem como das medidas a tomar em caso de pedidos de informações por parte de autoridades de países terceiros (incluindo a obrigação de rever e, se necessário, contestar a legalidade do pedido e de minimizar quaisquer informações divulgadas)?

6. Tratamento dos pedidos de acesso aos dados por parte de autoridades de países terceiros

a) Os critérios exigem que o importador de dados informe prontamente o exportador de dados em caso de pedidos de acesso por parte de autoridades de países terceiros e tome medidas adicionais adequadas?
b) Os critérios exigem que as transferências resultantes de pedidos de acesso desproporcionados por parte de autoridades públicas de países terceiros, em especial pedidos que exijam transferências maciças e indiscriminadas de dados pessoais, não sejam realizadas?

7. Garantias adicionais relativas ao exportador

46. Os critérios exigem que, quando previsto, o importador de dados assegure, também através de requisitos vinculativos a este respeito para o exportador de dados, que as medidas complementares que identificou sejam acompanhadas de medidas complementares correspondentes por parte do exportador de dados, tendo em conta as Recomendações 01/2020 do CEPD e os casos de utilização, a fim de assegurar uma aplicação eficaz das medidas complementares do importador?

4 COMPROMISSOS VINCULATIVOS E COM FORÇA EXECUTIVA A ASSUMIR

47. O RGPD exige, no seu artigo 42.º, n.º 2, que os responsáveis pelo tratamento e os subcontratantes não sujeitos ao RGPD que adiram a um mecanismo de certificação destinado às transferências assumam, adicionalmente, compromissos vinculativos e com força executiva, por meio de instrumentos

contratuais ou de outros instrumentos juridicamente vinculativos[22], no sentido de aplicar as garantias adequadas previstas no mecanismo de certificação, inclusivamente em relação aos direitos dos titulares dos dados.

48. Tal como especificado no RGPD, esses compromissos podem ser assumidos através de um contrato, o que parece ser a solução mais simples. Poderão também ser utilizados outros instrumentos, desde que os responsáveis pelo tratamento/subcontratantes que aderem ao mecanismo de certificação consigam demonstrar o caráter vinculativo e executório desses outros meios.

49. Em qualquer caso, o caráter vinculativo e executório deve ser assegurado ao abrigo do direito da UE e os compromissos devem também ser vinculativos e oponíveis pelos titulares dos dados enquanto terceiros beneficiários.

50. Uma opção simples seria incluir os compromissos vinculativos e com força executiva no contrato entre o exportador de dados e o importador de dados. Na prática, as partes poderiam utilizar um contrato existente (por exemplo, um acordo de serviços entre o exportador e o importador de dados, um contrato de acordo de tratamento de dados, em conformidade com o artigo 28.º do RGPD, entre os responsáveis pelo tratamento e os subcontratantes, ou um acordo de partilha de dados entre diferentes responsáveis pelo tratamento) em que os compromissos vinculativos e com força executiva pudessem ser incluídos. Esses compromissos devem ser claramente distinguidos de quaisquer outras cláusulas. Outra opção seria recorrer a um contrato separado, por exemplo incluindo no mecanismo de certificação destinado às transferências um modelo de contrato que teria de ser assinado pelos responsáveis pelo tratamento/subcontratantes no país terceiro e por todos os seus exportadores.

51. Deve haver flexibilidade para escolher a opção mais adequada em função da situação específica.

52. Caso o mecanismo de certificação se destine a ser utilizado para transferências e transferências ulteriores de um subcontratante para subcontratantes ulteriores, deve também ser feita referência ao mecanismo de certificação e ao instrumento que prevê compromissos vinculativos e com força executiva no acordo de subcontratação assinado entre o subcontratante e o seu responsável pelo tratamento.

Exemplo de compromissos vinculativos e com força executiva incluídos no contrato entre o exportador de dados e o importador de dados:

[22] Este instrumento juridicamente vinculativo não pode ser outro instrumento do capítulo V (como, por exemplo, as cláusulas-tipo de proteção de dados), uma vez que os compromissos vinculativos e com força executiva referidos no artigo 46.º, n.º 2, alínea f), têm de ser concebidos de modo a garantir que o importador respeitará os critérios de certificação.

53. Em geral, o contrato ou outro instrumento juridicamente vinculativo deve estabelecer que o responsável pelo tratamento/subcontratante titular de uma certificação que atue na qualidade de importador se compromete a cumprir as regras especificadas na certificação destinada às transferências ao tratar os dados recebidos do EEE e garante que não tem motivos para crer que a legislação e as práticas do país terceiro aplicáveis ao tratamento em causa, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o acesso por parte das autoridades públicas, o impeçam de cumprir os seus compromissos ao abrigo da certificação e que informará o exportador de quaisquer alterações relevantes da legislação ou prática a este respeito.

54. O contrato ou outro instrumento deve também prever procedimentos que permitam exigir o cumprimento desses compromissos em caso de não conformidade com as regras ao abrigo da certificação pelo responsável pelo tratamento/subcontratante que atua na qualidade de importador, em especial no que diz respeito aos direitos dos titulares cujos dados são transferidos ao abrigo da certificação.

55. Mais especificamente, o contrato ou outro instrumento deve abordar:

- a existência do direito de os titulares cujos dados são transferidos ao abrigo da certificação fazerem cumprir, enquanto terceiros beneficiários, os compromissos assumidos pelo importador de dados certificado no âmbito da certificação,

- a questão da responsabilidade em caso de não conformidade com as regras ao abrigo da certificação por um importador de dados titular de certificação fora do EEE. Os titulares dos dados devem ter a possibilidade de, em caso de não conformidade com as regras ao abrigo da certificação por um importador de dados titular de certificação fora do EEE, instaurar uma ação, incluindo uma ação de indemnização, contra essa entidade junto de uma AC do EEE e de um tribunal do EEE da residência habitual do titular dos dados, invocando o seu direito de terceiro beneficiário. O importador titular de certificação deve aceitar a decisão do titular dos dados de o fazer. Em caso de incumprimento pelo importador passível de conduzir à responsabilidade do exportador de dados, os titulares dos dados devem também ter a possibilidade de instaurar uma ação contra o exportador de dados junto da AC ou do tribunal competente do local de estabelecimento do exportador de dados ou da residência habitual do titular dos dados23. O importador de dados e o exportador de dados devem também aceitar que o titular dos dados possa ser representado por um organismo, organização ou associação sem fins lucrativos, nas condições estabelecidas no artigo 80.º, n.º 1, do RGPD,

- a existência de um direito do exportador de exigir o cumprimento, pelo importador titular de certificação, das regras estabelecidas na certificação na qualidade de terceiro beneficiário,

- a existência da obrigação de o importador de dados titular de certificação notificar o exportador e a autoridade de controlo do exportador de dados de quaisquer medidas tomadas pelo organismo de certificação em resposta a um incumprimento detetado das regras de certificação pelo próprio importador de dados.

[23] Esta responsabilidade não deve prejudicar os procedimentos a aplicar ao abrigo da certificação com o organismo de certificação, que também pode tomar medidas contra os responsáveis pelo tratamento/subcontratantes certificados em conformidade com a certificação, impondo medidas corretivas.

ANEXO

A. EXEMPLOS DE MEDIDAS COMPLEMENTARES A APLICAR PELO IMPORTADOR CASO O TRÂNSITO ESTEJA INCLUÍDO NO ÂMBITO DA CERTIFICAÇÃO

Caso de utilização 1: Armazenamento de dados para fins de cópia de segurança e outros fins que não exigem o acesso aos dados não encriptados

Devem ser estabelecidos critérios relativos às normas de encriptação e à segurança da chave de desencriptação, nomeadamente critérios relativos à situação jurídica no país terceiro. Se o importador puder ser forçado a transmitir as chaves de desencriptação, a medida complementar não pode ser considerada eficaz[24].

Caso de utilização 2: Transferência de dados pseudonimizados

No caso de dados pseudonimizados, devem ser estabelecidos critérios relativos à segurança das informações adicionais necessárias para atribuir os dados transferidos a uma pessoa identificada ou identificável, em especial:

— critérios relativos à situação jurídica no país terceiro. Se o importador puder ser forçado a aceder a dados adicionais ou a utilizá-los para os atribuir a uma pessoa identificada ou identificável, a medida não pode ser considerada eficaz[25],

— critérios relativos à definição de informações adicionais à disposição das autoridades de países terceiros que possam ser suficientes para atribuir os dados a uma pessoa identificada ou identificável.

Caso de utilização 3: Encriptação de dados para protegê-los do acesso das autoridades públicas do país terceiro do importador durante o trânsito entre o exportador e o importador

No caso de dados encriptados, devem ser incluídos os eventuais critérios para a segurança do trânsito. Se o importador puder ser forçado a transmitir as chaves criptográficas para desencriptação ou autenticação ou a modificar um componente utilizado para o trânsito de uma forma que comprometa as suas propriedades de segurança, a medida complementar não pode ser considerada eficaz[26].

Caso de utilização 4: Destinatário protegido

No caso dos destinatários protegidos, devem ser definidos critérios para os limites do privilégio. O tratamento de dados deve permanecer dentro dos limites do privilégio legal. O mesmo se aplica ao tratamento por subcontratantes ulteriores e transferências ulteriores, cujos destinatários também devem ser privilegiados[27].

[24] Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE, versão 2.0, anexo 2, «Caso de utilização 1: Armazenamento de dados para fins de cópia de segurança e outros fins que não exigem o acesso aos dados não encriptados», ponto 85; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pt.pdf.

[25] Ver as recomendações anteriormente citadas, pontos 86-89.

[26] Ver as recomendações anteriormente citadas, ponto 90.

[27] Ver as recomendações anteriormente citadas, ponto 91.

B. EXEMPLOS DE MEDIDAS COMPLEMENTARES NO CASO DE O TRÂNSITO NÃO SER ABRANGIDO PELA CERTIFICAÇÃO E O EXPORTADOR TER DE AS ASSEGURAR

Caso de utilização 2: Transferência de dados pseudonimizados

Devem ser previstos critérios relativos às informações adicionais à disposição das autoridades de países terceiros que possam ser suficientes para atribuir os dados a uma pessoa identificada ou identificável.

Caso de utilização 3: Encriptação de dados para protegê-los do acesso das autoridades públicas do país terceiro do importador durante o trânsito entre o exportador e o importador

Devem ser previstos critérios relativos à fiabilidade da autoridade ou infraestrutura de certificação de chave pública utilizada, à segurança das chaves criptográficas utilizadas para autenticação ou desencriptação e à fiabilidade da gestão das chaves, bem como à utilização de *software* devidamente mantido sem vulnerabilidades conhecidas.

Se o importador puder ser forçado a divulgar as chaves criptográficas destinadas à desencriptação ou autenticação ou a modificar um componente utilizado para o trânsito de uma forma que comprometa as suas propriedades de segurança, a medida não pode ser considerada eficaz[28].

Caso de utilização 4: Destinatário protegido

No caso dos destinatários protegidos, devem ser definidos critérios para os limites do privilégio. O tratamento de dados deve permanecer dentro dos limites do privilégio legal. O mesmo se aplica ao tratamento por subcontratantes ulteriores e transferências ulteriores, cujos destinatários também devem ser privilegiados[29].

[28] Ver as recomendações anteriormente citadas, ponto 90.
[29] Ver as recomendações anteriormente citadas, ponto 91.