Recomendações

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

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

Adotado em 18 de junho de 2021

Histórico de versões

Versão 2.0	18 de junho de 2021	Adoção das Recomendações após consulta pública
Versão 1.0	10 de novembro de 2020	Adoção das Recomendações para consulta pública

Resumo

O Regulamento Geral sobre a Proteção de Dados da UE (RGPD) foi adotado com um duplo objetivo: facilitar a livre circulação de dados pessoais na União Europeia, preservando ao mesmo tempo os direitos e liberdades fundamentais das pessoas, nomeadamente o seu direito à proteção de dados pessoais.

No seu recente acórdão Schrems II, no processo C-311/18, o Tribunal de Justiça da União Europeia (a seguir «Tribunal de Justiça») recorda-nos que a proteção concedida aos dados pessoais no Espaço Económico Europeu (a seguir «EEE») deve acompanhar os dados onde quer que os mesmos sejam utilizados. A transferência de dados pessoais para países terceiros não pode ser um meio de comprometer ou atenuar a proteção que lhe é concedida no EEE. O Tribunal de Justiça também afirma o que precede esclarecendo que o nível de proteção em países terceiros não precisa de ser idêntico ao garantido no EEE, mas essencialmente equivalente. Confirma igualmente a validade das cláusulas contratuais-tipo como instrumentos de transferência que podem servir para assegurar contratualmente um nível de proteção essencialmente equivalente para os dados transferidos para países terceiros.

As cláusulas contratuais-tipo e outros instrumentos de transferência referidos no artigo 46.º do RGPD não funcionam num vazio. O Tribunal de Justiça declara que os responsáveis pelo tratamento dos dados ou os subcontratantes, agindo como exportadores, são responsáveis por verificar, caso a caso e, sempre que adequado, em colaboração com o importador no país terceiro, se o direito ou a prática do país terceiro afetam a eficácia das garantias adequadas contidas nos instrumentos de transferência do artigo 46.º do RGPD. Em tais casos, o Tribunal de Justiça deixa ainda em aberto a possibilidade de os exportadores aplicarem medidas complementares que colmatem as lacunas na proteção e a aproximem do nível exigido pela legislação da UE. O Tribunal de Justiça não especifica quais poderão ser as medidas. No entanto, sublinha que os exportadores devem identificá-las caso a caso. O que precede está em consonância com o princípio da responsabilidade constante do artigo 5.º, n.º 2, do RGPD, que exige que os responsáveis pelo tratamento sejam responsáveis pelo cumprimento dos princípios RGPD relativos ao tratamento dos dados pessoais e que sejam capazes de o comprovar.

A fim de ajudar os exportadores (sejam estes responsáveis pelo tratamento dos dados ou subcontratantes, entidades privadas ou organismos públicos que tratam dados pessoais abrangidos pelo âmbito de aplicação do RGPD) na complexa tarefa de avaliar países terceiros e identificar medidas complementares adequadas sempre que necessário, o Comité Europeu para a Proteção de Dados (a seguir «CEPD») adotou as presentes recomendações. As presentes recomendações preveem várias etapas a seguir, possíveis fontes de informação e alguns exemplos de medidas complementares que podem ser aplicadas.

Numa **primeira etapa**, o CEPD recomenda ao exportador que **conheça as suas transferências**. Fazer um levantamento de todas as transferências de dados pessoais para países terceiros pode ser um processo difícil. No entanto, é necessário ter conhecimento do destino dos dados pessoais para garantir que estes beneficiam de um nível de proteção essencialmente equivalente onde quer sejam tratados. O exportador deve igualmente verificar se os dados transferidos são adequados, pertinentes e limitados ao necessário relativamente aos fins para os quais são tratados.

Numa **segunda** etapa, é necessário **verificar o instrumento de transferência utilizado para a transferência** entre os enumerados no capítulo V do RGPD. Se a Comissão Europeia já tiver declarado que o país, a região ou o setor para os quais são transferidos os dados são adequados, através de uma decisão de adequação ao abrigo do artigo 45.º do RGPD ou ao abrigo da anterior Diretiva 95/46, enquanto a decisão estiver em vigor, o exportador deverá apenas verificar se a decisão de adequação permanece válida. Na falta de uma decisão de adequação, o exportador deve recorrer a um dos instrumentos de transferência enumerados no artigo 46.º do RGPD. O exportador apenas poderá recorrer a uma das derrogações previstas no artigo 49.º do RGPD em alguns casos, desde que cumpra

as condições estipuladas. As derrogações não podem, na prática, tornar-se a «regra», mas devem limitar-se a situações específicas.

A **terceira etapa** consiste em **avaliar** se existe algo no direito ou nas práticas do país terceiro que possa afetar a eficácia das garantias adequadas dos instrumentos de transferência a que recorre o exportador, no contexto da transferência específica. A avaliação do exportador deve centrar-se, antes de mais, na legislação do país terceiro que é pertinente para a sua transferência e para o instrumento de transferência do artigo 46.º do RGPD utilizado. O exame das práticas das autoridades públicas do país terceiro permitir-lhe-á verificar se as garantias contidas no instrumento de transferência podem assegurar, na prática, a proteção efetiva dos dados pessoais transferidos. O exame destas práticas será especialmente relevante para a avaliação do exportador nos casos em que:

(i.) a legislação do país terceiro que cumpre formalmente as normas da UE não é manifestamente aplicada ou cumprida na prática;

(ii.) existem práticas incompatíveis com os compromissos do instrumento de transferência quando não existe legislação pertinente no país terceiro;

(iii.) os dados transferidos do exportador e/ou o importador são ou podem ser abrangidos pelo âmbito de aplicação de legislação problemática (ou seja, que afeta a garantia contratual do instrumento de transferência de um nível de proteção essencialmente equivalente e não cumpre as normas da UE em matéria de direitos fundamentais, necessidade e proporcionalidade).

Nas duas primeiras situações, o exportador deve suspender a transferência ou aplicar medidas complementares adequadas se desejar prosseguir com a transferência.

Na terceira situação, tendo em conta as incertezas quanto à potencial aplicação de legislação problemática à transferência, o exportador pode decidir: suspender a transferência; implementar medidas complementares para prosseguir com a transferência; ou, em alternativa, decidir prosseguir com a transferência sem aplicar medidas complementares se considerar e puder demonstrar e documentar que não tem motivos para crer que a legislação relevante e problemática será interpretada e/ou aplicada, na prática, de modo a abranger os dados transferidos e o importador.

Para avaliar os elementos a ter em consideração na avaliação da legislação de um país terceiro em matéria de acesso aos dados pelas autoridades públicas para fins de vigilância, o exportador deve consultar as Recomendações do CEPD sobre as garantias essenciais europeias.

O exportador deve efetuar a referida avaliação com a devida diligência e documentá-la integralmente. As autoridades de controlo e/ou judiciais competentes podem solicitar a referida avaliação e responsabilizá-lo por qualquer decisão tomada com base na mesma.

Numa **quarta etapa**, há que **identificar e adotar as medidas complementares** necessárias para aproximar o nível de proteção dos dados transferidos do nível da norma europeia de equivalência essencial. A etapa em causa apenas é necessária se a avaliação do exportador revelar que a legislação e/ou as práticas do país terceiro afetam a eficácia do instrumento de transferência do artigo 46.º do RGPD que o exportador utiliza ou pretende utilizar no contexto da transferência. As presentes recomendações contêm, no anexo 2, uma lista não exaustiva de exemplos de medidas complementares e algumas das condições necessárias à sua eficácia. À semelhança das garantias adequadas contidas nos instrumentos de transferência do artigo 46.º, algumas medidas complementares podem ser eficazes nuns países, mas não necessariamente noutros. O exportador será responsável por avaliar a respetiva eficácia no contexto da transferência e à luz da legislação e da prática do país terceiro e do instrumento de transferência utilizado, uma vez que será responsabilizado por qualquer decisão que venha a tomar a esse respeito. Tal poderá igualmente exigir a conjugação de diversas medidas complementares. Em última análise, é possível que nenhuma medida complementar possa assegurar um nível de proteção essencialmente equivalente à transferência específica. No caso de não haver nenhuma medida complementar adequada, o exportador deve evitar, suspender ou pôr termo à transferência a fim de não comprometer o nível de proteção dos dados pessoais. O exportador

deve igualmente efetuar a referida avaliação de medidas complementares com a devida diligência e documentá-la.

Numa **quinta etapa**, o exportador deve **adotar** todas as **medidas processuais formais** que a adoção da sua medida complementar possa exigir, em função do instrumento de transferência do artigo 46.º do RGPD que utilizar. As presentes recomendações especificam algumas destas formalidades. Pode ser necessário consultar as autoridades de controlo competentes relativamente a algumas das referidas medidas.

A **sexta e última etapa** consiste em **reavaliar**, com a periodicidade adequada, o nível de proteção concedido aos dados transferidos para países terceiros e controlar eventuais desenvolvimentos passados ou futuros que o possam afetar. O princípio da responsabilidade exige a vigilância permanente do nível de proteção dos dados pessoais.

As autoridades de controlo continuarão a exercer o seu mandato que consiste em monitorizar a aplicação do RGPD e em impor a sua observância. As autoridades de controlo terão em devida consideração as medidas adotadas pelos exportadores para assegurar que os dados transferidos beneficiam de um nível de proteção essencialmente equivalente. Conforme recorda o Tribunal de Justiça, a autoridade de controlo competente suspenderá ou proibirá as transferências de dados sempre que considerar que não pode ser garantido um nível de proteção essencialmente equivalente.

As autoridades de controlo continuarão a elaborar orientações destinadas aos exportadores e a coordenar as suas ações no seio do CEPD, a fim de garantir a coerência na aplicação da legislação da UE em matéria de proteção de dados.

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 «RGPD»),

Tendo em conta o Acordo sobre o Espaço Económico Europeu (Acordo EEE) e, nomeadamente, os seus anexo XI e protocolo n.º 37, com a redação que lhes 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,

Considerando o seguinte:

(1) O Tribunal de Justiça da União Europeia (a seguir «Tribunal de Justiça») conclui no seu Acórdão de 16 de julho de 2020 *Data Protection Commissioner/ Facebook Ireland LTD* e *Maximillian Schrems*, C-311/18, que o artigo 46.º, n.º 1, e o artigo 46.º, n.º 2, alínea c), do Regulamento 2016/679 devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, exigidos por estas disposições, devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União Europeia por este regulamento, lido à luz da Carta dos Direitos Fundamentais da União Europeia[2].

(2) Tal como sublinhado pelo Tribunal de Justiça, deve ser assegurado um nível de proteção das pessoas singulares essencialmente equivalente ao garantido na União Europeia pelo RGPD, tendo em consideração a Carta, independentemente do disposto no capítulo V com base no qual se realiza uma transferência de dados pessoais para um país terceiro. As disposições do capítulo V visam assegurar a continuidade do referido elevado nível de proteção sempre que dados pessoais são transferidos para um país terceiro.[3]

(3) O considerando 108 e o artigo 46.º, n.º 1, do RGPD preveem que, na falta de uma decisão da UE sobre o nível de proteção adequado, um responsável pelo tratamento ou um subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. O responsável pelo tratamento ou subcontratante pode prever garantias adequadas, sem necessidade de qualquer autorização específica de uma autoridade de controlo, mediante a utilização de um dos instrumentos de transferência enumerados no artigo 46.º, n.º 2, do RGPD, tais como cláusulas-tipo de proteção de dados.

---

[1] As referências a «Estados-Membros» no presente documento devem ser entendidas como referências a «Estados-Membros do EEE».
[2] Acórdão do Tribunal de Justiça de 16 de julho de 2020, *Data Protection Commissioner/ Facebook Ireland Ltd* e *Maximillian Schrems* (C-311/18, a seguir «acórdão Schrems II)»), ponto 2) do dispositivo.
[3] Acórdão Schrems II, n.os 92 e 93.

(4) O Tribunal de Justiça esclarece que as cláusulas-tipo de proteção de dados adotadas pela Comissão se destinam exclusivamente a prever garantias contratuais aplicáveis de modo uniforme em todos os países terceiros aos responsáveis pelo tratamento e subcontratantes estabelecidos na União Europeia. Devido à sua natureza contratual, as cláusulas-tipo de proteção de dados não podem vincular as autoridades públicas de países terceiros, uma vez que estas não são parte signatária do contrato. Consequentemente, os exportadores de dados podem ter de complementar as garantias constantes das referidas cláusulas-tipo de proteção de dados com medidas complementares por forma a assegurar o cumprimento do nível de proteção exigido pela legislação da UE num determinado país terceiro. O Tribunal de Justiça faz referência ao considerando 109 do RGPD, que menciona tal possibilidade e incentiva os responsáveis pelo tratamento e subcontratantes a utilizá-la.[4]

(5) O Tribunal de Justiça afirmou que cabe, antes de mais, ao responsável pelo tratamento verificar, caso a caso e, se for caso disso, em colaboração com o importador dos dados, se o direito do país terceiro de destino assegura um nível de proteção essencialmente equivalente, à luz do direito da União, dos dados pessoais transferidos com base em cláusulas-tipo de proteção de dados, fornecendo, se necessário, medidas complementares às oferecidas por essas cláusulas.[5]

(6) Se o responsável pelo tratamento ou subcontratante estabelecido na União Europeia não puder adotar medidas complementares adequadas para assegurar um nível de proteção essencialmente equivalente nos termos da legislação da UE, o responsável pelo tratamento ou subcontratante ou, na falta destes, a autoridade de controlo competente deve suspender ou pôr termo à transferência de dados pessoais para o país terceiro em causa.[6]

(7) O RGPD ou o Tribunal de Justiça não definem nem especificam as «garantias adicionais», «medidas adicionais» ou «medidas complementares» das garantias dos instrumentos de transferência enumerados no artigo 46.º, n.º 2, do RGPD que os responsáveis pelo tratamento e os subcontratantes podem adotar para assegurar o cumprimento do nível de proteção exigido num determinado país terceiro ao abrigo da legislação da UE.

(8) Por iniciativa própria, o CEPD decidiu analisar esta questão e disponibilizar aos responsáveis pelo tratamento e subcontratantes, agindo como exportadores, recomendações sobre o processo que podem seguir para identificar e adotar medidas complementares. As presentes recomendações destinam-se a fornecer aos exportadores uma metodologia para determinar se devem ser adotadas medidas adicionais em relação às suas transferências e quais são essas medidas. A principal responsabilidade dos exportadores consiste em assegurar que os dados transferidos beneficiem no país terceiro de um nível de proteção essencialmente equivalente ao garantido no EEE. O CEPD procura, com as presentes recomendações, incentivar a aplicação coerente do RGPD e do acórdão do Tribunal de Justiça, em conformidade com o mandato do CEPD.[7]

ADOTOU AS PRESENTES RECOMENDAÇÕES:

---

[4]Acórdão Schrems II, n.^{os} 132 e 133.
[5] Acórdão Schrems II, n.º 134.
[6] Acórdão Schrems II, n.º 135.
[7]Artigo 70.º, n.º 1, alínea e), do RGPD.

RESPONSABILIDADE PELAS TRANSFERÊNCIAS DE DADOS

1. O direito primário da UE considera o direito à proteção de dados um direito fundamental[8]. Assim, é atribuído um elevado nível de proteção ao direito à proteção de dados e apenas podem ser implementadas restrições se forem previstas na legislação, respeitarem o conteúdo essencial do direito, forem proporcionadas e necessárias e corresponderem efetivamente aos objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.[9] O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.[10]

2. Os dados devem ser acompanhados de um nível de proteção essencialmente equivalente ao garantido na UE sempre que estes são enviados para países terceiros fora do EEE, a fim de assegurar que o nível de proteção garantido pelo RGPD não é comprometido durante e após a transferência.

3. O direito à proteção de dados tem um caráter ativo, exigindo que os exportadores e importadores (quer sejam responsáveis pelo tratamento e/ou subcontratantes) vão para além de um reconhecimento ou cumprimento passivo deste direito.[11] Os responsáveis pelo tratamento e subcontratantes devem procurar cumprir o direito à proteção de dados de forma ativa e contínua, mediante a implementação de medidas jurídicas, técnicas e organizativas que garantam a sua eficácia. Os responsáveis pelo tratamento e os subcontratantes devem igualmente poder demonstrar tais esforços aos titulares dos dados e às autoridades de controlo em matéria de proteção de dados. Trata-se do chamado princípio da responsabilidade.[12]

4. O princípio da responsabilidade, necessário para assegurar a aplicação efetiva do nível de proteção conferido pelo RGPD, é igualmente aplicável às transferências de dados para países terceiros[13], uma vez que estas constituem elas próprias uma forma de tratamento de dados.[14] Tal como sublinhado pelo Tribunal de Justiça no seu acórdão, deve ser assegurado um nível de proteção essencialmente equivalente ao garantido na União Europeia pelo RGPD, tendo em consideração a Carta, independentemente do disposto no capítulo com base no qual se realiza uma transferência de dados pessoais para um país terceiro.[15]

5. No Acórdão Schrems II, o Tribunal de Justiça sublinha as responsabilidades dos exportadores e importadores de assegurar que o tratamento de dados pessoais foi e continuará a ser efetuado em conformidade com o nível de proteção estabelecido pela legislação da UE em matéria de

---

[8] Artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais, artigo 16.º, n.º 1, do TFUE e artigo 1, n.º 2, do RGPD.
[9] Artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da UE.
[10] Considerando 4 do RGPD e Acórdão Google LLC, sucessora da Google Inc./ Commission nationale de l'informatique et des libertés (CNIL), C-507/17, n.º 60.
[11] Conclusões apresentadas pela advogada-geral E. Sharpston em 17 de junho de 2010 nos processos C-92/09 e C-93/02, Volker und Markus Schecke GbR/ Land Hessen, n.º 71.
[12] Artigo 5.º, n.º 2, e artigo 28.º, n.º 3, alínea h), do RGPD.
[13] Artigo 44.º e considerando 101 do RGPD, bem como o artigo 47.º, n.º 2, alínea d), do RGPD.
[14] Acórdão do Tribunal de Justiça de 6 de outubro de 2015, *Maximillian Schrems/ Data Protection Commissioner* (C-362/14, a seguir «Acórdão Schrems I»), n.º 45.
[15] Acórdão Schrems II, n.os 92 e 93.

proteção de dados e de suspender a transferência e/ou rescindir o contrato sempre que o importador dos dados não esteja ou deixe de estar em condições de respeitar as cláusulas-tipo de proteção de dados incorporadas no contrato pertinente entre o exportador e o importador.[16] O responsável pelo tratamento ou o subcontratante, agindo como exportador, devem assegurar que os importadores colaboram com o exportador, sempre que adequado, no desempenho destas responsabilidades, mantendo-o informado, por exemplo, de qualquer desenvolvimento que afete o nível de proteção dos dados pessoais recebidos no país do importador.[17] As referidas responsabilidades são uma aplicação do princípio da responsabilidade do RGPD às transferências de dados.[18]

ROTEIRO: APLICAÇÃO DO PRINCÍPIO DA RESPONSABILIDADE ÀS TRANSFERÊNCIAS DE DADOS NA PRÁTICA

6. O exportador de dados poderá encontrar a seguir um roteiro das medidas a adotar para saber se deve aplicar medidas complementares para poder transferir legalmente dados para fora do EEE. No presente documento, entende-se por «exportador de dados» ou «exportador» o responsável pelo tratamento ou o subcontratante que age como exportador de dados,[19] e trata dados pessoais abrangidos pelo âmbito de aplicação do RGPD (incluindo o tratamento por entidades privadas e organismos públicos durante a transferência dos dados para entidades privadas).[20] No que respeita às transferências de dados pessoais efetuadas entre organismos públicos, estão previstas orientações específicas nas *Diretrizes 2/2020 sobre a aplicação do artigo 46.º n.º 2, alínea a), e do artigo 46.º, n.º 3, alínea b), do Regulamento (UE) 2016/679 às transferências de dados pessoais entre autoridades e organismos públicos estabelecidos no EEE e fora do EEE.*[21]

7. O exportador deve documentar de forma adequada a avaliação e as medidas complementares que selecionar e implementar e deve, mediante solicitação, disponibilizar a documentação à autoridade de controlo competente.[22]

---

[16]Acórdão Schrems II, n.os 134, 135, 139, 140, 141 e 142.
[17]Acórdão Schrems II, n.º 134.
[18]Artigo 5.º, n.º 2, e artigo 28.º, n.º 3, alínea h), do RGPD.
[19] Por conseguinte, por exemplo, não será considerado «exportador de dados» o titular de dados que fornece os seus dados pessoais através de um questionário em linha a um responsável pelo tratamento estabelecido num país terceiro.
[20]Ver Diretrizes 3/2018 do CEPD sobre o âmbito de aplicação territorial do RGPD (artigo 3.º) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21]Diretrizes 2/2020 do CEPD sobre a aplicação do artigo 46.º n.º 2, alínea a), e do artigo 46.º, n.º 3, alínea b), do Regulamento (UE) 2016/679 às transferências de dados pessoais entre autoridades e organismos públicos estabelecidos no EEE e fora do EEE; ver https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[22]Artigo 5.º, n.º 2, e artigo 24.º, n.º 1, do RGPD.

Etapa 1: Conhecer as transferências

8. Para saber o que lhe poderá ser exigido para poder prosseguir as suas transferências ou para realizar novas transferências de dados pessoais,[23] o exportador de dados deve começar por se assegurar de que tem pleno conhecimento das suas transferências. O registo e o levantamento de todas as transferências podem constituir um exercício complexo para as entidades envolvidas em transferências múltiplas, diversas e regulares com países terceiros e que utilizam diversos subcontratantes e subcontratantes ulteriores. Conhecer as suas transferências é uma primeira etapa essencial para cumprir as obrigações que incumbem ao exportador de dados por força do princípio da responsabilidade.

9. Para estar totalmente ciente das suas transferências, o exportador poderá apoiar-se nos registos das atividades de tratamento que poderá estar obrigado a manter enquanto responsável pelo tratamento ou subcontratante por força do artigo 30.º do RGPD.[24] Podem ser igualmente úteis as medidas anteriores adotadas em cumprimento das obrigações de prestação de informações aos titulares dos dados, nos termos dos artigos 13.º, n.º 1, alínea f), e 14.º, n.º 1, alínea f), do RGPD, relativamente às transferências dos seus dados pessoais para países terceiros.[25]

10. Aquando do levantamento das transferências, o exportador deve igualmente ter em conta as transferências ulteriores, por exemplo, se os seus subcontratantes estabelecidos fora do EEE transferem os dados pessoais que lhes foram confiados para um subcontratante ulterior estabelecido noutro país terceiro ou no mesmo país terceiro.[26]

11. Em consonância com o princípio da «minimização dos dados»,[27] o exportador deve igualmente verificar se os dados transferidos são adequados, pertinentes e limitados ao necessário relativamente aos fins para os quais estes são transferidos e tratados no país terceiro.

---

[23]Considera-se igualmente uma transferência o acesso remoto por uma entidade de um país terceiro aos dados localizados no EEE.

[24] Ver artigo 30.º do RGPD, nomeadamente o n.º 1, alínea e), e o n.º 2, alínea c). Além disso, os registos do tratamento de dados do exportador devem conter uma descrição das atividades de tratamento (incluindo, sem caráter limitativo, as categorias de titulares dos dados, as categorias de dados pessoais, as finalidades do tratamento e informações específicas sobre as transferências de dados). Alguns responsáveis pelo tratamento e subcontratantes estão isentos da obrigação de manter registos de tratamento (artigo 30.º, n.º 5, do RGPD). Para mais informação sobre a referida isenção, ver o *Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR* (documento de posição sobre as derrogações à obrigação de manter registos das atividades de tratamento, nos termos do artigo 30.º, n.º 5, do RGPD) do Grupo de Trabalho do Artigo 29.º (aprovado pelo CEPD em 25 de maio de 2018).

[25]Por força das regras sobre a transparência do RGPD, o exportador deve informar os titulares dos dados sobre as transferências de dados pessoais para países terceiros [artigo 13.º, n.º 1, alínea f), e artigo 14.º, n.º 1, alínea f), do RGPD]. Em especial, deve informar os titulares dos dados da existência ou falta de uma decisão de adequação da Comissão Europeia ou, no caso das transferências referidas nos artigos 46.º ou 47.º do RGPD, ou no artigo 49.º, n.º 1, segundo parágrafo, do RGPD, referir as garantias adequadas ou apropriadas e os meios para obter cópia das mesmas, ou o local onde podem ser encontradas. As informações prestadas ao titular dos dados devem ser corretas e atuais, especialmente à luz da jurisprudência do Tribunal de Justiça em matéria de transferências.

[26]Sempre que o responsável pelo tratamento tiver dado, previamente e por escrito, autorização específica ou geral, em conformidade com o artigo 28.º, n.º 2, do RGPD.

[27]Artigo 5.º, n.º 1, alínea c), do RGPD.

12. Estas atividades devem ser realizadas antes de qualquer transferência e atualizadas antes de retomar as transferências após a suspensão das operações de transferência de dados: o exportador deve saber onde podem estar localizados ou onde podem ser tratados pelos importadores os dados pessoais exportados (mapa de destinos).

13. Recorde-se que o acesso remoto a partir de um país terceiro (por exemplo, em situações de assistência) e/ou o armazenamento numa nuvem situada fora do EEE, é igualmente considerado uma transferência.[28] Mais especificamente, se o exportador estiver a utilizar uma infraestrutura de nuvem internacional, deve avaliar se os dados serão transferidos para países terceiros e quais, salvo se o prestador de serviços na nuvem estiver estabelecido no EEE e indicar claramente no contrato que os dados não serão tratados em países terceiros.

Etapa 2: Identificar os instrumentos de transferência utilizados

14. A segunda etapa consiste em identificar os instrumentos de transferência a que o exportador recorre entre os previstos e enumerados no capítulo V do RGPD.

Decisões de adequação

15. Através das suas **decisões de adequação** relativas a alguns ou a todos os países terceiros para os quais o exportador transfere dados pessoais, a Comissão Europeia pode reconhecer que estes países oferecem um nível adequado de proteção dos dados pessoais.[29]

16. Tal decisão de adequação permite que os dados pessoais sejam transferidos do EEE para o país terceiro em causa sem que seja necessário um instrumento de transferência do artigo 46.º do RGPD.

17. As decisões de adequação podem abranger um país na sua totalidade ou limitar-se a uma parte do mesmo. As decisões de adequação podem abranger todas as transferências de dados para um país ou limitar-se a alguns tipos de transferências (por exemplo, num único setor).[30]

18. A Comissão Europeia publica a lista de decisões de adequação no respetivo sítio web.[31]

19. Se o exportador transfere dados pessoais para países terceiros, regiões ou setores abrangidos por uma decisão de adequação da Comissão (na medida em que seja aplicável), **não deve adotar outras medidas adicionais descritas nas presentes recomendações**[32]**.** O exportador deve, no

[28]Ver a pergunta frequente n.º 11 «(deve-se ter em conta que fornecer acesso a dados de um país terceiro, por exemplo para fins administrativos, também equivale a uma transferência» , do documento Perguntas frequentes sobre o Acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – *Data Protection Commissioner contra Facebook Ireland Limited and Maximillian Schrems*, de 23 de julho de 2020.

[29] A Comissão Europeia tem autoridade para determinar, com base no artigo 45.º do RGPD, se um país fora da UE oferece um nível adequado de proteção dos dados pessoais. A Comissão Europeia pode igualmente determinar que uma organização internacional oferece um nível adequado de proteção.

[30] Artigo 45.º, n.º 1, do RGPD.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Desde que o exportador e o importador de dados tenham implementado medidas para cumprirem as restantes obrigações nos termos do RGPD; caso contrário, as referidas medidas devem ser implementadas.

entanto, controlar sempre se as decisões de adequação pertinentes para as suas transferências foram revogadas ou anuladas.[33]

20. Contudo, as decisões de adequação não impedem que os titulares dos dados apresentem reclamações. Também não impedem que as autoridades de controlo instaurem processos num tribunal nacional, caso tenham dúvidas quanto à validade de uma decisão, para que o tribunal nacional possa apresentar um pedido de decisão prejudicial ao Tribunal de Justiça para apreciação da referida validade.[34]

Exemplo:

Um cidadão da UE, M. Schrems, apresentou uma queixa em junho de 2013 à Comissão Irlandesa para a Proteção de Dados e solicitou à autoridade de controlo em causa que proibisse ou suspendesse a transferência pela Facebook Ireland dos seus dados pessoais para os Estados Unidos, pois considerava que o direito e as práticas em vigor neste país não asseguravam uma proteção suficiente dos dados pessoais conservados no seu território contra as atividades de vigilância aí exercidas pelas autoridades públicas. A Comissão Irlandesa para a Proteção de Dados rejeitou a queixa com o fundamento de que na Decisão 2000/520/CE a Comissão tinha constatado que, ao abrigo do regime «porto seguro», os Estados Unidos asseguravam um nível adequado de proteção dos dados pessoais transferidos (decisão relativa ao «porto seguro»). O Sr. Schrems contestou a decisão da Comissão Irlandesa para a Proteção de Dados e o Supremo Tribunal da Irlanda submeteu uma questão sobre a validade da Decisão 2000/520/CE ao Tribunal de Justiça da União Europeia (Tribunal de Justiça). Subsequentemente, o Tribunal de Justiça declarou inválida a Decisão 2000/520/CE da Comissão relativa ao nível de proteção assegurado pelos princípios de «porto seguro».[35]

Instrumentos de transferência do artigo 46.º do RGPD

21. O artigo 46.º do RGPD enumera diversos instrumentos de transferência contendo «*garantias adequadas*» que os exportadores podem utilizar para transferir dados pessoais para países terceiros na ausência de decisões de adequação. Os principais tipos de instrumentos de transferência do artigo 46.º do RGPD são os seguintes:

- cláusulas-tipo de proteção de dados;
- regras vinculativas aplicáveis às empresas;

[33] A Comissão Europeia deve rever periodicamente todas as decisões de adequação e verificar se os países terceiros que beneficiam de decisões de adequação continuam a assegurar um nível adequado de proteção (ver artigo 45.º, n.os 3 e 4, do RGPD). O Tribunal de Justiça pode ainda declarar inválidas as decisões de adequação [ver os seus acórdãos nos processos C-362/14 (Schrems I) e C-311/18 (Schrems II)].

[34] Acórdão Schrems II, n.os 118 a 120. As autoridades de controlo não podem ignorar a decisão de adequação e suspender ou proibir as transferências de dados pessoais para tais países, citando apenas a inadequação do nível de proteção. Apenas podem exercer o seu poder de suspender ou proibir transferências de dados pessoais para o país terceiro em causa por outros motivos (por exemplo, medidas de segurança insuficientes em violação do artigo 32.º do RGPD; inexistência de uma base jurídica para o tratamento dos dados enquanto tal em violação do artigo 6.º do RGPD). As autoridades de controlo podem examinar, com total independência, se a transferência desses dados respeita as exigências estabelecidas pelo RGPD e, sendo caso disso, intentar uma ação nos órgãos jurisdicionais nacionais para que estes últimos, caso tenham dúvidas quanto à validade da decisão de adequação, submetam um pedido de decisão prejudicial ao Tribunal de Justiça para efeitos da apreciação dessa validade.

[35] Acórdão Schrems I.

- códigos de conduta;
- procedimentos de certificação;
- cláusulas contratuais *ad hoc*.

22. Independentemente do instrumento de transferência do artigo 46.º do RGPD escolhido, o exportador deve assegurar-se de que, em termos gerais, os dados pessoais transferidos beneficiam de um nível de proteção essencialmente equivalente.

23. Os instrumentos de transferência do artigo 46.º do RGPD contêm principalmente garantias adequadas de natureza contratual que podem ser aplicadas a transferências para todos os países terceiros. A situação existente no país terceiro para o qual o exportador transfere dados pode ainda exigir que este complemente os referidos instrumentos de transferência e as garantias aí contidas com medidas adicionais («medidas complementares») para assegurar um nível de proteção essencialmente equivalente.[36]

Derrogações

24. Para além das decisões de adequação e dos instrumentos de transferência do artigo 46.º do RGPD, o RGPD contém uma terceira via que permite transferências de dados pessoais em determinadas situações. Em determinadas condições específicas, o exportador pode ainda transferir dados pessoais com base numa das derrogações previstas no artigo 49.º do RGPD.

25. O artigo 49.º do RGPD tem caráter excecional. As derrogações que contém devem ser interpretadas de uma forma que não contrarie a própria natureza das derrogações enquanto exceções à regra segundo a qual os dados pessoais só podem ser transferidos para um país terceiro se esse país proporcionar um nível adequado de proteção de dados ou, em alternativa, se forem adotadas garantias adequadas. As derrogações não podem, na prática, tornar-se a «regra», mas devem limitar-se a situações específicas. O CEPD emitiu as Diretrizes 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679. [37]

26. Antes de invocar uma derrogação do artigo 49.º do RGPD, o exportador deve verificar se a sua transferência cumpre as condições rigorosas estabelecidas na referida disposição para cada derrogação.

***

27. Se a transferência não puder basear-se legalmente numa decisão de adequação, nem uma derrogação do artigo 49.º, é necessário prosseguir para a etapa 3.

[36] Acórdão Schrems II, n.os 130 e 133. Ver também a subsecção 2.3 *infra*.
[37] Para mais informações, ver https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

Etapa 3: Avaliar se o instrumento de transferência do artigo 46.º do RGPD utilizado é eficaz tendo em conta todas as circunstâncias da transferência

28. O instrumento de transferência do artigo 46.º do RGPD selecionado deve ser eficaz, assegurando que o nível de proteção garantido pelo RGPD não é comprometido pela transferência.[38]

29. Em especial, a proteção conferida aos dados pessoais transferidos para o país terceiro deve ser essencialmente equivalente à que é garantida no EEE pelo RGPD, lido à luz da Carta dos Direitos Fundamentais da UE.[39] Tal não ocorre se o importador de dados for impedido de cumprir as suas obrigações ao abrigo do instrumento de transferência do artigo 46.º do RGPD escolhido devido ao direito e às práticas do país terceiro aplicáveis à transferência, incluindo durante o trânsito de dados do exportador para o país do importador[40].

30. Por conseguinte, o exportador deve, se necessário em colaboração com o importador, avaliar se existe algo no direito ou na prática[41] do país terceiro que possa afetar a eficácia das garantias adequadas do instrumento de transferência do artigo 46.º do RGPD que utilizou, no contexto da transferência específica. Tal implica determinar se a sua transferência é abrangida pelo âmbito de aplicação da legislação e/ou práticas suscetíveis de afetar a eficácia do instrumento de transferência do artigo 46.º do RGPD que utiliza. A avaliação exigida deve basear-se sobretudo na legislação disponível ao público.

31. Esta avaliação deve conter elementos relativos ao acesso aos dados das autoridades públicas do país terceiro do importador, tais como:

    - elementos que indiquem se as autoridades públicas do país terceiro do importador podem procurar aceder aos dados com ou sem o conhecimento do importador de dados, à luz da legislação, prática e precedentes comunicados;
    - elementos que indiquem se as autoridades públicas do país terceiro do importador poderão ter acesso aos dados através do importador de dados ou através dos fornecedores de telecomunicações ou canais de comunicação, à luz da legislação, dos poderes legais, dos recursos técnicos, financeiros e humanos de que dispõem e dos precedentes comunicados.

Identificar leis e práticas pertinentes à luz de todas as circunstâncias da transferência

32. O exportador deve analisar as características de cada uma das suas transferências e determinar se o ordenamento jurídico nacional e/ou as práticas em vigor do país para o qual os dados são transferidos (ou transferidos ulteriormente) afetam as suas transferências. O âmbito da avaliação do exportador limita-se, por conseguinte, à legislação e prática pertinentes para a proteção dos dados específicos que transfere, ao contrário das avaliações de adequação gerais e abrangentes que a Comissão Europeia realiza em conformidade com o artigo 45.º do RGPD.

[38] Artigo 44.º do RGPD e n.os 126, 137 e 148 do Acórdão Schrems II.
[39] Acórdão Schrems II, n.º 105 e ponto 2) do dispositivo.
[40] Ver Acórdão Schrems II, n.º 183, em conjugação com o n.º 184.
[41] Ver n.º 126 do Acórdão Schrems II, no qual o Tribunal de Justiça refere expressamente o «direito e das práticas em vigor no país terceiro em causa» e a necessidade de «[...] assegurar, na prática, a proteção efetiva dos dados pessoais transferidos para o país terceiro em causa» (sublinhado nosso), e n.º 158.

33. O contexto jurídico e/ou as práticas aplicáveis dependerão das circunstâncias específicas da transferência, nomeadamente:

- as finalidades para as quais os dados são transferidos e tratados (por ex., marketing, RH, armazenamento, apoio informático, ensaios clínicos);
- os tipos de entidade envolvidos no tratamento (pública/privada; responsável pelo tratamento/subcontratante);
- o setor no qual a transferência ocorre (por ex., *adtech*, telecomunicações, financeiro, etc.);
- as categorias de dados pessoais transferidos (por ex., os dados pessoais relativos a crianças podem ser abrangidos pelo âmbito de aplicação de uma legislação específica do país terceiro)[42];
- se os dados serão armazenados no país terceiro ou se existe acesso remoto aos dados armazenados na UE ou no EEE;
- o formato dos dados a transferir (ou seja, texto corrido/pseudonimizado ou encriptado[43]);
- a possibilidade de ocorrência de transferências ulteriores dos dados do país terceiro em causa para outro país terceiro.[44]

34. A avaliação do exportador deve ter em consideração todos os intervenientes na transferência (por exemplo, responsáveis pelo tratamento, subcontratantes e subcontratantes ulteriores que tratam dados no país terceiro), tal como identificados no exercício de levantamento das transferências. Quanto maior for o número de responsáveis pelo tratamento, subcontratantes ou importadores envolvidos, mais complexa será a avaliação do exportador. O exportador deve igualmente ter em consideração na referida avaliação qualquer possível transferência ulterior.

35. O exportador deve, em todo o caso, prestar especial atenção a todas as leis pertinentes, nomeadamente, as leis que estabeleçam requisitos de divulgação de dados pessoais a autoridades públicas ou que concedam a tais autoridades públicas poderes de acesso a dados pessoais (por exemplo, para fins de aplicação do direito penal, controlo regulamentar ou segurança nacional). Se estes requisitos ou poderes limitarem os direitos fundamentais dos titulares dos dados, respeitando simultaneamente a sua essência e sendo necessários e proporcionados numa sociedade democrática para salvaguardar objetivos importantes, tal como também reconhecidos no direito da União ou dos Estados-Membros da UE[45], poderão não colidir

---

[42] A transferência de dados pessoais é uma operação de tratamento (artigo 4.º, n.º 2, do RGPD). Se o exportador pretender transferir dados sensíveis abrangidos pelos artigos 9.º e 10.º do RGPD, só poderá efetuar uma transferência se esta for abrangida por uma das derrogações e pelas condições estabelecidas nos artigos 9.º e 10.º do RGPD e no direito dos Estados-Membros da UE. Em conformidade com o artigo 32.º do RGPD, deverá também aplicar, com o importador na qualidade de responsável pelo tratamento ou subcontratante, medidas técnicas e organizativas adequadas para garantir um nível de segurança adequado aos riscos para os direitos e liberdades dos titulares dos dados decorrentes de uma potencial violação de dados pessoais dos dados transferidos (artigo 4.º, n.º 12, do RGPD). As categorias de dados transferidos e a sua sensibilidade serão relevantes para a avaliação do risco e da adequação das medidas.

[43] Alguns países terceiros não permitem a importação de dados encriptados.

[44] Sempre que o responsável pelo tratamento tiver dado, previamente e por escrito, autorização específica ou geral, em conformidade com o artigo 28.º, n.º 2, do RGPD.

[45] Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e as Recomendações do CEPD 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

com os compromissos contidos no instrumento de transferência do artigo 46.º do RGPD utilizado pelo exportador.

36. O exportador deve avaliar as regras e práticas de natureza geral pertinentes, na medida em que tenham impacto na aplicação efetiva das garantias contidas no instrumento de transferência do artigo 46.º do RGPD.

37. Aquando da realização da referida avaliação, são igualmente pertinentes diferentes aspetos do sistema jurídico do país terceiro em causa, por exemplo, os elementos enumerados no artigo 45.º, n.º 2, do RGPD. A título de exemplo, a situação do Estado de direito no país terceiro pode ser pertinente para avaliar a eficácia dos mecanismos colocados à disposição dos particulares para que estes possam recorrer (judicialmente) contra o acesso ilícito do Governo a dados pessoais. A existência de uma lei abrangente em matéria de proteção de dados ou de uma autoridade independente para a proteção de dados, bem como a adesão a instrumentos internacionais que preveem garantias em matéria de proteção de dados, podem contribuir para assegurar a proporcionalidade da interferência do Governo.

38. Considera-se que as obrigações ou os poderes resultantes de tais leis e práticas colidem ou são incompatíveis com os compromissos do instrumento de transferência do artigo 46.º do RGPD se[46]:

- Não respeitam a essência dos direitos e liberdades fundamentais da Carta dos Direitos Fundamentais da UE, ou

- Excedem o que é necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos importantes também reconhecidos no direito da União ou dos Estados-Membros, como os enumerados no artigo 23.º, n.º 1, do RGPD.

39. O exportador deve verificar se os compromissos do importador de dados que permitem aos titulares dos dados exercer os seus direitos previstos no instrumento de transferência do artigo 46.º do RGPD [tais como pedidos de acesso, retificação e apagamento de dados transferidos, e as vias de recurso (judicial)] podem ser aplicados de forma eficaz na prática e não são comprometidos pela legislação e/ou práticas do país terceiro de destino.

40. As normas da UE, tais como os artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, devem ser utilizadas como referência, em especial para avaliar se o acesso por parte das autoridades públicas se limita ao que é necessário e proporcionado numa sociedade democrática e se os titulares dos dados têm direito a uma via de recurso eficaz.

41. As recomendações do CEPD sobre as garantias europeias essenciais[47] proporcionam clarificações sobre os elementos que têm de ser avaliados por forma a determinar se o quadro jurídico que rege o acesso aos dados pessoais das autoridades públicas de um país terceiro (sejam estas agências de segurança nacional ou autoridades policiais) pode ou não ser considerado uma interferência justificável[48]. Em especial, as referidas recomendações devem ser cuidadosamente

[46]Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD, Acórdão Schrems II, n.os 174 e 187, e as Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020.

[47] Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020.

[48] E, por conseguinte, não colide com os compromissos assumidos no instrumento de transferência do artigo 46.º do RGPD.

consideradas sempre que a legislação que rege o acesso aos dados pelas autoridades públicas é ambígua ou não está disponível ao público. O primeiro requisito das Garantias Essenciais Europeias é a existência de um quadro jurídico que regula o acesso, quando previsto, que esteja disponível ao público e seja suficientemente claro.

42. Aplicadas à situação das transferências de dados com base nos instrumentos de transferência do artigo 46.º, as recomendações do CEPD sobre as Garantias Europeias Essenciais podem orientar o exportador de dados na avaliação da questão de saber se tais poderes interferem de forma injustificada com as obrigações do exportador e do importador de dados de assegurarem a equivalência essencial nos termos do RGPD ou com os compromissos contidos no instrumento de transferência. A ausência de um nível de proteção essencialmente equivalente será especialmente evidente quando o direito ou a prática do país terceiro pertinente para a transferência não cumprir os requisitos das Garantias Essenciais Europeias. O CEPD reitera que as Garantias Essenciais Europeias constituem uma norma de referência para a avaliação da ingerência inerente às medidas de vigilância de países terceiros, no contexto das transferências internacionais de dados. Estas normas decorrem da legislação da UE e da jurisprudência do Tribunal de Justiça e do TEDH que vinculam os Estados-Membros da UE.

43. A avaliação do exportador deve, antes de mais, basear-se na legislação disponível ao público. O exame das práticas das autoridades públicas do país terceiro permitir-lhe-á verificar se as garantias contidas no instrumento de transferência do artigo 46.º do RGPD podem constituir um meio suficiente para garantir, na prática, a proteção efetiva dos dados pessoais transferidos[49]. A análise das práticas em vigor no país terceiro será especialmente importante para a avaliação do exportador nas situações a seguir descritas.

43.1 **A legislação pertinente do país terceiro pode cumprir formalmente as normas da UE em matéria de direitos e liberdades fundamentais e a necessidade e proporcionalidade das restrições a esses direitos e liberdades.** No entanto, a prática das autoridades públicas (por exemplo, quando acedem a dados pessoais na posse do setor privado ou quando impõem — ou não — a legislação enquanto órgãos de supervisão ou judiciais) podem indicar claramente que, normalmente, estas não aplicam ou não cumprem a legislação que rege, em princípio, as suas atividades. Neste caso, o exportador deve ter em conta estas práticas na sua avaliação e considerar que a ferramenta do artigo 46.º do RGPD não poderá assegurar eficazmente, por si só (ou seja, sem medidas complementares), um nível de proteção essencialmente equivalente. Nesse caso, se pretender prosseguir com a transferência, o exportador deverá aplicar medidas complementares adequadas.

43.2 **A legislação pertinente (por exemplo, sobre o acesso aos dados pessoais na posse do setor privado) pode não existir no país terceiro.** Neste caso, o exportador não pode deduzir automaticamente desta ausência de legislação pertinente que o instrumento de transferência do artigo 46.º do RGPD poderá ser efetivamente aplicado. O exportador deve verificar se existem indicações de práticas em vigor no país que sejam incompatíveis com o direito da UE e com os compromissos do instrumento de transferência do artigo 46.º do RGPD. Se existirem práticas incompatíveis, o instrumento de transferência do artigo 46.º do RGPD não poderá assegurar efetivamente, por si só (ou seja, sem medidas complementares adequadas), um nível

[49] Acórdão Schrems II, n.º 126.

de proteção essencialmente equivalente. Nesse caso, se pretender prosseguir com a transferência, o exportador deverá aplicar medidas complementares adequadas.

43.3 **A avaliação pode revelar que a legislação pertinente do país terceiro pode ser problemática[50] e que os dados transferidos e/ou o importador em causa são ou podem ser abrangidos pelo âmbito de aplicação desta legislação problemática[51].**

Tendo em conta as incertezas que rodeiam a eventual aplicação de legislação problemática à transferência, o exportador poderá decidir:

- Suspender a transferência;
- Aplicar medidas complementares[52] para prevenir o risco da potencial aplicação ao importador e/ou aos dados transferidos de leis e/ou práticas do país terceiro do importador de dados suscetíveis de afetar as garantias contratuais do instrumento de transferência de um nível de proteção essencialmente equivalente ao garantido no EEE; ou
- Em alternativa, o exportador pode decidir prosseguir com a transferência sem necessidade de aplicar medidas complementares, se considerar que não tem motivos para crer que a legislação pertinente e problemática será aplicada, na prática, aos dados transferidos e/ou ao importador. O exportador deve demonstrar e documentar através da sua avaliação, se for caso disso em colaboração com o importador, que a legislação não é interpretada e/ou aplicada, na prática, de modo a abranger os dados transferidos e o importador, tendo igualmente em conta a experiência de outros intervenientes que operam no mesmo setor e/ou relacionada com dados pessoais transferidos semelhantes e as fontes de informação adicionais descritas mais adiante[53].

  Por conseguinte, o exportador deve demonstrar e documentar num relatório pormenorizado[54] que a legislação problemática não será aplicada, na prática, aos dados

---

[50] Entende-se por «legislação problemática» a legislação que 1) impõe ao destinatário de dados pessoais provenientes da União Europeia obrigações e/ou afeta os dados transferidos de uma forma que pode colidir com a garantia contratual dos instrumentos de transferência de um nível de proteção essencialmente equivalente e 2) não respeita a essência dos direitos e liberdades fundamentais reconhecidos pela Carta dos Direitos Fundamentais da UE ou excede o que é necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos importantes também reconhecidos no direito da União ou dos Estados-Membros da UE, como os enumerados no artigo 23.º, n.º 1, do RGPD.

[51] Pode não ser claro se o importador e/ou os dados transferidos são abrangidos pelo âmbito de aplicação dos termos gerais frequentemente utilizados na legislação nacional em matéria de segurança para limitar o seu âmbito de aplicação, como, por exemplo, «prestador de serviços de comunicações eletrónicas» e «informações dos serviços de informação estrangeiros».

[52] Ver considerando 109 do RGPD e Acórdão Schrems II, n.º 132.

[53] Ver pontos 45 a 47.

[54] Os relatórios a elaborar deverão incluir informações completas sobre a avaliação jurídica da legislação e das práticas, bem como sobre a sua aplicação às transferências específicas, o procedimento interno de elaboração da avaliação (incluindo informações sobre os intervenientes envolvidos na avaliação, por exemplo, gabinetes de advogados, consultores ou departamentos internos) e as datas das verificações. Os relatórios devem ser aprovados pelo representante legal do exportador.

transferidos e/ou ao importador e, consequentemente, não impedirá o importador de cumprir as suas obrigações ao abrigo do artigo 46.º do RGPD[55].

Possíveis fontes de informação

44. Sempre que adequado, o importador de dados deve fornecer ao exportador as fontes e informações pertinentes relacionadas com o país terceiro no qual se encontra estabelecido e as leis aplicáveis à transferência.

45. O exportador e o importador podem completar a avaliação do exportador com informações obtidas a partir de fontes, tais como as enumeradas como exemplos no anexo 3.

46. Para além do quadro jurídico do país terceiro aplicável à transferência, as fontes e as informações devem ser pertinentes, objetivas, fiáveis, verificáveis e acessíveis ao público ou de outro modo acessíveis para determinar se o instrumento de transferência do artigo 46.º pode ser efetivamente aplicado[56], o que deve ser avaliado e documentado pelo exportador.

Relevantes: as informações devem ser relevantes para a transferência e/ou importador específicos e a sua conformidade com os requisitos estabelecidos no direito da UE e no instrumento de transferência do artigo 46.º do RGPD, e não devem ser demasiado gerais ou abstratas.

Objetivas: informações corroboradas por dados empíricos baseados em conhecimentos adquiridos no passado e não em suposições de potenciais acontecimentos e riscos.

Fiáveis: o exportador e o importador devem avaliar objetivamente a fiabilidade da fonte de informação e das próprias informações e avaliá-las separadamente.

Verificáveis: as informações e as conclusões devem ser verificáveis ou contrastáveis com outros tipos de informações ou fontes, como parte de uma avaliação global, também para permitir à autoridade de supervisão ou judicial competente verificar, caso necessário, a objetividade e a fiabilidade dessas informações.

Acessíveis ao público ou de outro modo acessíveis: as informações devem, de preferência, ser públicas ou, pelo menos, acessíveis para facilitar a verificação dos critérios acima referidos e assegurar a sua eventual partilha com as autoridades de controlo, as autoridades judiciais e, em última análise, os titulares dos dados.

[55] A demonstração de que a legislação problemática não é aplicada, na prática, aos dados transferidos e ao importador, tendo também em conta a experiência de outros intervenientes que operam no mesmo setor e/ou relacionada com dados pessoais transferidos semelhantes, não isenta o exportador de prever as medidas complementares necessárias para proteger os dados pessoais durante a sua transmissão e tratamento no país terceiro de destino (por exemplo, encriptação de ponta a ponta dos dados — ver exemplos de medidas técnicas complementares no anexo 2) se a análise do exportador da legislação aplicável do país terceiro de destino indicar que o acesso aos dados também pode ter lugar, mesmo na ausência da intervenção do importador, neste momento da transferência. O exportador pode já ter previsto estas medidas com o importador na qualidade de responsável pelo tratamento ou subcontratante, em conformidade com o artigo 32.º do RGPD.

[56] Ver anexo 3 para uma lista não exaustiva das fontes de informação que podem ser utilizadas pelo exportador e pelo importador.

47. O exportador também pode ter em conta a experiência prática documentada do importador em casos anteriores pertinentes de pedidos de acesso recebidos de autoridades públicas do país terceiro. O exportador só poderá utilizar a experiência do importador como fonte de informação adicional se o quadro jurídico do país terceiro não proibir o importador de fornecer informações sobre os pedidos de divulgação das autoridades públicas ou sobre a ausência de tais pedidos (e deverá também documentar essa avaliação). Refira-se, no entanto, que a ausência de ocorrências anteriores de pedidos recebidos pelo importador nunca poderá ser considerada, por si só, pelo exportador como um fator decisivo da eficácia do instrumento de transferência do artigo 46.º do RGPD que permitirá realizar a transferência sem medidas complementares. Esta informação poderá ser considerada pelo exportador juntamente com outros tipos de informações obtidas de outras fontes, como parte da sua avaliação global da legislação e das práticas do país terceiro em relação à transferência. A experiência pertinente e documentada do importador deve ser corroborada e não contrariada por informações pertinentes, objetivas, fiáveis, verificáveis e acessíveis ao público ou de outro modo acessíveis sobre a aplicação prática da legislação aplicável (por ex., a existência ou a ausência de pedidos de acesso recebidos por outros intervenientes que operam no mesmo setor e/ou relacionados com dados pessoais transferidos semelhantes[57] e/ou a aplicação da lei na prática, como a jurisprudência e os relatórios de organismos de supervisão independentes).

Resultados da avaliação do exportador

48. O exportador deve realizar esta avaliação global da legislação e da prática do país terceiro do importador aplicáveis à transferência com a devida diligência e documentá-la exaustivamente. As autoridades de controlo e/ou judiciais competentes podem solicitar a referida avaliação e responsabilizar o exportador por qualquer decisão tomada com base na mesma.[58]

49. A avaliação pode, em última análise, demonstrar que o instrumento de transferência do artigo 46.º do RGPD a que recorre o exportador:

    - garante efetivamente que os dados pessoais transferidos beneficiam de um nível de proteção no país terceiro essencialmente equivalente ao garantido no EEE. O direito e a prática do país terceiro aplicáveis à transferência permitem ao importador de dados cumprir as obrigações que lhe incumbem por força do instrumento de transferência escolhido. O exportador deve reavaliar a situação com uma frequência adequada ou sempre que ocorram alterações significativas (ver etapa 6); ou

    - não garante efetivamente um nível de proteção essencialmente equivalente. O importador de dados não pode cumprir as suas obrigações, devido à legislação e/ou práticas do país terceiro aplicáveis à transferência que não cumprem as normas da UE em matéria de direitos e liberdades fundamentais e a necessidade e proporcionalidade das respetivas restrições para salvaguardar objetivos legítimos de interesse público. O Tribunal de Justiça sublinhou que nos

[57] A experiência pode ser a de outras entidades do conhecimento direto do exportador devido a transferências anteriores do mesmo tipo ou referidas na jurisprudência pertinente, em relatórios de ONG, etc. (ver anexo 3).
[58] Artigo 5.º, n.º 2, do RGPD.

casos em que os instrumentos de transferência do artigo 46.º do RGPD não são suficientes cabe ao exportador de dados adotar medidas complementares eficazes ou não transferir dados pessoais.[59]

Exemplo:

Contexto:
O Tribunal de Justiça considerou, por exemplo, que o artigo 702.º da Lei de Vigilância de Informações Externas dos Estados Unidos (FISA) não cumpre os requisitos mínimos inerentes, no direito da União, ao princípio da proporcionalidade e não se pode considerar que se limite ao estritamente necessário. Por conseguinte, o nível de proteção dos programas autorizados pelo artigo 702.º da FISA não é essencialmente equivalente às garantias exigidas pela legislação da UE.

Avaliação:
Se a sua avaliação da legislação pertinente dos EUA levar o exportador a considerar que a transferência pode ser abrangida pelo âmbito de aplicação do artigo 702.º da FISA, mas o mesmo tiver dúvidas de que a transferência seja abrangida pelo âmbito de aplicação prática deste artigo, o exportador poderá decidir:

1. Interromper a transferência;
2. Adotar medidas complementares adequadas que assegurem efetivamente um nível de proteção dos dados transferidos essencialmente equivalente ao garantido no EEE; ou
3. Considerar outras informações objetivas, fiáveis, pertinentes, verificáveis e, de preferência, acessíveis ao público (que podem incluir informações que lhe tenham sido fornecidas pelo importador de dados), para clarificar o âmbito da aplicação prática do artigo 702.º da FISA à transferência específica. Estas informações devem dar resposta a algumas perguntas pertinentes, tais como:

- As informações publicamente disponíveis mostram que existe uma proibição legal de informar sobre um pedido específico recebido de acesso a dados e restrições importantes à prestação de informações gerais sobre os pedidos recebidos de acesso a dados ou sobre a ausência de pedidos recebidos?

- O importador de dados confirmou ter recebido pedidos de acesso a dados das autoridades públicas dos EUA no passado? Ou o importador de dados confirmou que, no passado, não recebeu pedidos de acesso a dados das autoridades públicas dos EUA e que não está proibido de fornecer informações sobre esses pedidos ou sobre a sua ausência?

- As informações acessíveis ao público obtidas pelo exportador sobre a jurisprudência dos EUA e os relatórios de organismos de supervisão, organizações da sociedade civil e instituições académicas[60] revelam que importadores de dados do mesmo setor que o importador em causa receberam no passado pedidos de acesso relativamente a dados transferidos semelhantes?

[59] Acórdão Schrems II, n.os 134 e 135.

[60] Por ex., disposições do artigo 702.º da FISA; regulamento interno do Foreign Intelligence Surveillance Court (FISC), pareceres e decisões não confidenciais do FISC, jurisprudência dos tribunais dos EUA; relatórios e transcrições de audiências da Privacy and Civil Liberties Oversight Board (PCLOB); relatórios do Office of the Inspector General - U.S. Department of Justice; relatórios do NSA Director of Civil Liberties and Privacy Office; relatórios elaborados pelo Congressional Research Service; relatórios da American Civil Liberties Union Foundation (ACLU).

As respostas a estas perguntas obtidas através da avaliação global do exportador levam-no a concluir que:

- O artigo 702.º da FISA aplica-se, na prática, à transferência específica e, por conseguinte, colide com a eficácia do instrumento de transferência do artigo 46.º do RGPD utilizado. Por conseguinte, se o exportador pretender proceder à transferência, deve considerar, caso necessário em colaboração com o importador, se pode adotar medidas complementares que assegurem efetivamente um nível de proteção dos dados transferidos essencialmente equivalente ao garantido no EEE. Se não encontrar medidas complementares eficazes, não deve transferir os dados pessoais.

Ou

- O artigo 702.º da FISA não se aplica, na prática, à transferência específica e, por conseguinte, não afeta a eficácia do instrumento de transferência do artigo 46.º do RGPD utilizado. Nesse caso, o exportador pode realizar a transferência sem quaisquer medidas complementares.

Etapa 4: Adotar medidas complementares

50. Se resultar da avaliação efetuada pelo exportador na etapa 3 que o instrumento de transferência do artigo 46.º do RGPD escolhido não é eficaz, o exportador deverá determinar, caso necessário em colaboração com o importador, se existem medidas complementares que, em combinação com as garantias contidas nos instrumentos de transferência, possam assegurar que os dados transferidos beneficiem no país terceiro de um nível de proteção essencialmente equivalente ao que é garantido na UE.[61] As «medidas complementares» são, por definição, complementares das garantias já previstas no instrumento de transferência do artigo 46.º do RGPD e de quaisquer outros requisitos de segurança aplicáveis (por ex., medidas técnicas de segurança) estabelecidos no RGPD[62].

51. O exportador deve identificar, caso a caso, as medidas complementares que podem ser eficazes para um conjunto de transferências para um país terceiro específico quando utiliza um instrumento de transferência específico do artigo 46.º do RGPD. O exportador não precisa de repetir a avaliação sempre que efetuar a mesma transferência de um tipo específico de dados para o mesmo país terceiro. Alguns dos dados previstos para transferência podem exigir medidas complementares, ao passo que outros podem não exigir essas medidas (tendo em conta a aplicação formal e/ou prática da legislação do país terceiro). O exportador poderá basear-se nas suas avaliações e conclusões anteriores nas etapas 1, 2 e 3 supra e verificar, com base nas suas conclusões, a potencial eficácia das medidas complementares para garantir o nível de proteção exigido.

52. Em princípio, as medidas complementares podem ter um caráter contratual, técnico ou organizativo. A combinação de diferentes medidas de um modo que estas se suportem e reforcem

[61] Acórdão Schrems II, n.º 96.
[62] Considerando 109 do RGPD e Acórdão Schrems II, n.º 133.

mutuamente pode aumentar o nível de proteção e, por conseguinte, contribuir para o cumprimento das normas da UE.

53. As medidas contratuais e organizativas não poderão, por si só, regra geral, obstar ao acesso aos dados pessoais das autoridades públicas do país terceiro com base em legislação e/ou práticas problemáticas.[63] Com efeito, em determinadas situações, apenas as medidas técnicas implementadas de forma adequada poderão impedir ou tornar ineficaz o acesso das autoridades públicas de países terceiros aos dados pessoais, nomeadamente para fins de vigilância.[64] Nessas situações, determinadas medidas contratuais ou organizativas podem complementar as medidas técnicas e reforçar o nível geral de proteção dos dados (por ex., mediante a introdução de controlos e a eliminação de automatismos em relação às tentativas de acesso aos dados das autoridades públicas não conformes com as normas da UE.

54. O exportador pode, caso necessário em colaboração com o importador de dados, consultar a seguinte lista (não exaustiva) de fatores para identificar as medidas complementares mais eficazes na proteção dos dados transferidos contra os pedidos de acesso a dados das autoridades públicas baseados em legislação problemática aplicada na prática:

    - formato dos dados a transferir (ou seja, texto corrido/pseudonimizado ou encriptado),
    - natureza dos dados (por ex., é concedido um nível de proteção mais elevado no EEE às categorias de dados abrangidas pelos artigos 9.º e 10.º do RGPD);[65]
    - duração e complexidade do fluxo de tratamento de dados, número de intervenientes envolvidos no tratamento e relação entre os mesmos (por ex., as transferências envolvem vários responsáveis pelo tratamento ou responsáveis pelo tratamento de dados e subcontratantes, ou envolvem subcontratantes que transferirão os dados do exportador para o importador de dados, considerando as disposições pertinentes que lhes são aplicáveis ao abrigo da legislação do país terceiro de destino);[66]
    - técnica ou parâmetros de aplicação prática da legislação do país terceiro concluída na etapa 3;

---

[63] Entende-se por «legislação problemática» a legislação que 1) impõe ao destinatário de dados pessoais provenientes da União Europeia obrigações e/ou afeta os dados transferidos de uma forma que pode colidir com a garantia contratual dos instrumentos de transferência de um nível de proteção essencialmente equivalente e 2) não respeita a essência dos direitos e liberdades fundamentais reconhecidos pela Carta dos Direitos Fundamentais da UE ou excede o que é necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos importantes também reconhecidos no direito da União ou dos Estados-Membros da UE, como os enumerados no artigo 23.º, n.º 1, do RGPD.

[64] Sempre que tal acesso vá além do que é necessário e proporcionado numa sociedade democrática; ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[65] Ver nota de rodapé 42.

[66] O RGPD atribui obrigações diferentes aos responsáveis pelo tratamento e aos subcontratantes. As transferências podem ser de responsável pelo tratamento para responsável pelo tratamento, entre responsáveis pelo tratamento conjuntos, de responsável pelo tratamento para subcontratante, e, mediante autorização do responsável pelo tratamento, de subcontratante para responsável pelo tratamento ou de subcontratante para subcontratante.

- possibilidade da ocorrência de transferências ulteriores dos dados, no mesmo país terceiro ou mesmo para outros países terceiros (por ex., envolvimento de subcontratantes ulteriores do importador de dados).[67]

Exemplos de medidas complementares

55. Alguns exemplos de medidas técnicas, contratuais e organizativas que poderão ser consideradas, se já não estiverem incluídas no instrumento de transferência do artigo 46.º do RGPD, constam das listas não exaustivas do anexo 2.

***

56. Se o exportador tiver adotado medidas complementares eficazes que em combinação com o instrumento de transferência do artigo 46.º do RGPD escolhido atinjam um nível de proteção essencialmente equivalente ao garantido no EEE, poderá realizar as transferências.

57. Caso não consiga encontrar ou implementar medidas complementares eficazes que garantam que os dados pessoais transferidos beneficiem de um nível de proteção essencialmente equivalente[68], o exportador não deverá iniciar qualquer transferência de dados pessoais para o país terceiro em causa utilizando o instrumento de transferência do artigo 46.º do RGPD por si escolhido. Se o exportador já tiver iniciado transferências, deve suspender ou cessar a transferência de dados pessoais.[69] Nos termos das garantias contidas no instrumento de transferência do artigo 46.º do RGPD a que recorreu o exportador, os dados já transferidos para o país terceiro em causa, bem como as respetivas cópias, devem ser-lhe devolvidos ou ser integralmente destruídos pelo importador.[70]

Exemplo:

O direito do país terceiro proíbe as medidas complementares que o exportador identificou (por exemplo, proíbe a utilização de encriptação) ou impede, de outro modo, a sua eficácia. O exportador não deve iniciar qualquer transferência de dados pessoais para o país em causa ou deve interromper as transferências em curso para esse país.

58. A autoridade de controlo competente pode impor quaisquer outras medidas corretivas (por ex., uma coima) se, apesar de não poder demonstrar um nível de proteção essencialmente equivalente no país terceiro, o exportador iniciar ou prosseguir a transferência.

[67] Ver nota de rodapé 26.
[68] Sempre que tal acesso vá além do necessário e proporcionado numa sociedade democrática; ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.
[69] Acórdão Schrems II, n.º 135.
[70] Ver, por exemplo, a cláusula 12 do anexo da Decisão 2010/87/UE relativa às CCT; ver a cláusula adicional de resolução (opcional) do anexo B da Decisão 2004/915/CE relativa às CCT.

Etapa 5: Etapas do processo a seguir quando o exportador identifica medidas complementares eficazes

59. As etapas do processo que o exportador pode ter de seguir se tiver identificado medidas complementares eficazes a adotar variam consoante o instrumento de transferência do artigo 46.º do RGPD que estiver a utilizar ou pretender utilizar.

Cláusulas-tipo de proteção de dados [artigo 46.º, n.º 2, alíneas c) e d), do RGPD]

60. Se o exportador pretender adotar medidas complementares em combinação com as cláusulas contratuais-tipo, não é necessário solicitar autorização à autoridade de controlo competente para adicionar este tipo de cláusulas ou garantias complementares, desde que as medidas complementares identificadas não contradigam, direta ou indiretamente, as cláusulas-tipo de proteção de dados e sejam suficientes para assegurar que o nível de proteção garantido pelo RGPD não é comprometido.[71] O exportador e o importador de dados devem assegurar que as cláusulas adicionais não podem ser interpretadas de modo a restringir os direitos e obrigações previstos nas cláusulas contratuais-tipo ou, de qualquer outro modo, reduzir o nível de proteção dos dados. O exportador deve poder demonstrar o que precede, incluindo a inequivocidade de todas as cláusulas, em conformidade com o princípio da responsabilidade e a sua obrigação de proporcionar um nível suficiente de proteção dos dados. As autoridades de controlo competentes têm o poder de rever as cláusulas complementares sempre que necessário (por ex., em caso de reclamação ou de um inquérito de iniciativa própria).

61. Se o exportador pretender alterar as próprias cláusulas-tipo de proteção de dados ou se as medidas complementares adicionadas «contradisserem», direta ou indiretamente, as cláusulas contratuais-tipo, deixa de se considerar que o exportador recorreu às cláusulas-tipo contratuais[72] e este deve solicitar uma autorização à autoridade de controlo competente, nos termos do artigo 46.º, n.º 3, alínea a), do RGPD.

[71] O considerando 109 do RGPD estipula: «A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados.» Os conjuntos de cláusulas contratuais-tipo adotados pela Comissão Europeia ao abrigo da Diretiva 95/45/CE contêm disposições semelhantes.

[72] Ver, por analogia, o Parecer 17/2020 do CEPD sobre o projeto de cláusulas contratuais tipo apresentado pela autoridade de controlo (AC) eslovena (artigo 28.º, n.º 8, do RGPD) relativamente à cláusula contratual-tipo do artigo 28.º já adotada que contém uma disposição semelhante («Além disso, o Comité recorda que a possibilidade de utilizar cláusulas contratuais-tipo adotadas por uma autoridade de controlo não impede as partes de acrescentarem outras cláusulas ou salvaguardas adicionais, desde que estas não contradigam, direta ou indiretamente, as cláusulas contratuais-tipo adotadas, nem prejudiquem os direitos ou liberdades fundamentais dos titulares de dados. Além disso, caso as cláusulas-tipo de proteção de dados sejam alteradas, deixará de se considerar que as partes aplicaram as cláusulas contratuais-tipo adotadas»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_pt.pdf.

Regras vinculativas aplicáveis às empresas [artigo 46.º, n.º 2, alínea b), do RGPD]

62. O raciocínio apresentado pelo Acórdão Schrems II aplica-se igualmente a outros instrumentos de transferência nos termos do artigo 46.º, n.º 2, do RGPD, uma vez que todos estes instrumentos são basicamente de natureza contratual, de modo que as garantias previstas e os compromissos assumidos pelas partes não podem vincular autoridades públicas de países terceiros[73].

63. O Acórdão Schrems II é pertinente para as transferências de dados pessoais com base em regras vinculativas aplicáveis às empresas, uma vez que as leis de países terceiros podem afetar a proteção proporcionada por esses instrumentos.

64. Todos os compromissos que devem ser incluídos serão referidos nas referências atualizadas do documento de trabalho WP256/257[74] do Grupo de Trabalho do Artigo 29.º, com as quais todos os grupos que utilizam as regras vinculativas para as empresas como instrumentos de transferência devem alinhar os respetivos instrumentos de transferência atuais e futuras.

65. O Tribunal de Justiça salientou que incumbe ao exportador e ao importador de dados avaliar se o nível de proteção exigido pela legislação da UE é respeitado no país terceiro em causa, a fim de determinar se as garantias fornecidas pelas cláusulas contratuais-tipo ou pelas regras vinculativas aplicáveis às empresas podem ser cumpridas na prática. Se não for o caso, o exportador deve avaliar se é possível prever medidas complementares para assegurar um nível de proteção essencialmente equivalente ao garantido no EEE e se o direito ou a prática do país terceiro não afetarão as medidas complementares, comprometendo a sua eficácia.

Cláusulas contratuais *ad hoc* [artigo 46.º, n.º 3, alínea a), do RGPD]

66. O raciocínio apresentado pelo Acórdão Schrems II aplica-se igualmente a outros instrumentos de transferência nos termos do artigo 46.º, n.º 2, do RGPD, uma vez que todos estes instrumentos são basicamente de natureza contratual, pelo que as garantias previstas e os compromissos assumidos pelas partes nestes instrumentos não podem vincular autoridades públicas de países terceiros[75]. Por conseguinte, o Acórdão Schrems II é pertinente para as transferências de dados pessoais com base nas cláusulas contratuais *ad hoc*, uma vez que as leis de países terceiros podem afetar a proteção assegurada por tais instrumentos.

Etapa 6: Reavaliar com frequência adequada

67. O exportador deve controlar, permanentemente e sempre que adequado em colaboração com os importadores de dados, os desenvolvimentos no país terceiro para o qual transferiu dados pessoais que possam afetar a sua avaliação inicial do nível de proteção e as decisões que tenha consequentemente adotado em relação às suas transferências. A responsabilidade é uma obrigação permanente (artigo 5.º, n.º 2, do RGPD).

---

[73] Acórdão Schrems II, n.º 132.

[74] Grupo de Trabalho do Artigo 29.º, Documento de trabalho que cria uma tabela com os elementos e os princípios que constam das regras vinculativas para as empresas, com a última redação revista e adotada em 6 de fevereiro de 2018 (WP 256 rev.01); Grupo de Trabalho do Artigo 29.º,Documento de trabalho que cria uma tabela com os elementos e os princípios que constam das regras vinculativas para as empresas destinadas aos subcontratantes, com a última redação revista e adotada em 6 de fevereiro de 2018 (WP 257 rev.01).

[75] Acórdão Schrems II, n.º 132.

68. O exportador deve implementar mecanismos suficientemente seguros para assegurar a suspensão ou a cessação imediatas das transferências sempre que:

    - o importador tenha violado ou não possa honrar os compromissos que assumiu no instrumento de transferência do artigo 46.º do RGPD; ou
    - as medidas complementares deixem de ser aplicáveis ao país terceiro em causa.

CONCLUSÃO

69. O RGPD estabelece regras relativas ao tratamento de dados pessoais no EEE, permitindo, deste modo, a livre circulação de dados pessoais no EEE. O capítulo V do RGPD rege as transferências de dados pessoais para países terceiros e estabelece uma fasquia elevada: a transferência não deve comprometer o nível de proteção das pessoas singulares garantido pelo RGPD (artigo 44.º do RGPD). O Acórdão Schrems II sublinha a necessidade de assegurar a continuidade do nível de proteção concedido pelo RGPD aos dados pessoais transferidos para um país terceiro.[76]

70. Para garantir um nível de proteção essencialmente equivalente dos seus dados, o exportador deve, antes de mais, conhecer perfeitamente as suas transferências. O exportador deve igualmente verificar se os dados transferidos são adequados, pertinentes e limitados ao que é necessário relativamente aos fins para os quais estes são tratados.

71. Deve também identificar o instrumento de transferência a que recorreu para as suas transferências. Se o instrumento de transferência não for uma decisão de adequação, o exportador deve verificar, caso a caso, se o direito ou a prática do país terceiro de destino comprometem (ou não) as garantias contidas no instrumento de transferência do artigo 46.º do RGPD no contexto das suas transferências. Sempre que o instrumento de transferência do artigo 46.º do RGPD não permita atingir, por si só, em relação aos dados pessoais transferidos, um nível de proteção essencialmente equivalente, a lacuna pode ser colmatada por medidas complementares.

72. Caso não consiga encontrar ou implementar medidas complementares eficazes que garantam que os dados pessoais transferidos beneficiem de um nível de proteção essencialmente equivalente, o exportador não deve iniciar a transferência de dados pessoais para o país terceiro em causa com base no instrumento de transferência por si escolhido. Se o exportador já tiver iniciado transferências, deve suspender ou cessar imediatamente a transferência de dados pessoais.

73. A autoridade de controlo competente pode suspender ou cessar as transferências de dados pessoais para o país terceiro se estiver assegurada a proteção dos dados transferidos exigida pela legislação da UE e, nomeadamente, pelos artigos 45.º e 46.º do RGPD e pela Carta dos Direitos Fundamentais.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

[76] Acórdão Schrems II, n.º 93.

ANEXO 1: DEFINIÇÕES

- «País terceiro», qualquer país que não é um Estado-Membro do EEE.
- «EEE», o Espaço Económico Europeu; inclui os Estados-Membros da União Europeia, a Islândia, a Noruega e o Listenstaine. O RGPD aplica-se a estes últimos por força do Acordo EEE, em especial os seus anexo XI e protocolo 37.
- «RGPD», o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
- «Carta», a Carta dos Direitos Fundamentais da União Europeia, JO C 326 de 26.10.2012, p. 391–407.
- «Tribunal de Justiça», o Tribunal de Justiça da União Europeia. Constitui a autoridade judicial da União Europeia e assegura, em cooperação com os tribunais dos Estados-Membros, a aplicação e interpretação uniformes da legislação da UE.
- «Exportador de dados», o responsável pelo tratamento ou subcontratante no EEE que transfere dados pessoais para um responsável pelo tratamento ou subcontratante de um país terceiro.
- «Importador de dados», o responsável pelo tratamento ou subcontratante num país terceiro que recebe ou obtém acesso a dados pessoais transferidos do EEE.
- «Instrumento de transferência do artigo 46.º do RGPD», as garantias adequadas ao abrigo do artigo 46.º do RGPD que os exportadores de dados implementam quando transferem dados pessoais para um país terceiro, na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, do RGPD. O artigo 46.º, n.^{os} 2 e 3, do RGPD contém uma lista dos instrumentos de transferência do artigo 46.º do RGPD que os responsáveis pelo tratamento e subcontratantes podem utilizar.
- «Cláusulas contratuais-tipo», as cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia para as transferências de dados pessoais entre responsáveis pelo tratamento ou subcontratantes no EEE e responsáveis pelo tratamento ou subcontratantes fora do EEE. As cláusulas contratuais-tipo adotadas pela Comissão Europeia constituem um instrumento de transferência nos termos do RGPD, conforme previsto no artigo 46.º, n.º 2, alínea c), e n.º 5, do RGPD.

ANEXO 2: EXEMPLOS DE MEDIDAS COMPLEMENTARES

74. As medidas apresentadas a seguir constituem exemplos de medidas complementares que o exportador de dados deve considerar na etapa 4 «Adotar medidas complementares». A presente lista não é exaustiva. O exportador pode procurar outras medidas complementares. Os futuros desenvolvimentos tecnológicos, jurídicos ou organizacionais podem conduzir ao surgimento de novas medidas complementares a considerar pelo exportador. A seleção e implementação de uma ou mais das referidas medidas não garantem necessária e sistematicamente que a transferência cumpre a norma de equivalência essencial exigida pela legislação da UE. O exportador deve selecionar medidas complementares que possam garantir efetivamente este nível de proteção em relação às suas transferências.

75. Qualquer medida complementar só pode ser considerada eficaz na aceção do acórdão do Tribunal de Justiça «Schrems II» se e na medida em que — por si só ou em combinação com outras — corrija deficiências específicas identificadas na avaliação do exportador da situação no país terceiro no que diz respeito à sua legislação e práticas aplicáveis à sua transferência. Se, em última análise, o exportador não puder garantir um nível de proteção essencialmente equivalente, não deve transferir os dados pessoais.

76. Enquanto responsável pelo tratamento ou subcontratante, o exportador pode já estar obrigado a aplicar algumas das medidas descritas no presente anexo para cumprir o RGPD. Isto significa que poderão ser necessárias medidas semelhantes para os dados pessoais tratados no EEE, transferidos para um importador de dados abrangido por uma decisão de adequação ou para outros países terceiros[77].

2.1 Medidas técnicas

77. A presente secção descreve de forma não exaustiva exemplos de medidas técnicas que podem complementar as garantias contidas nos instrumentos de transferência do artigo 46.º do RGPD por forma a assegurar o cumprimento do nível de proteção exigido pela legislação da UE no contexto de uma transferência de dados pessoais para um país terceiro. Estas medidas serão especialmente necessárias nos casos em que a legislação do país imponha aos importadores de dados obrigações contrárias às garantias dos instrumentos de transferência do artigo 46.º do RGPD e, nomeadamente, suscetíveis de afetar a garantia contratual de um nível de proteção essencialmente equivalente contra o acesso aos dados pelas autoridades públicas do país terceiro[78].

78. Para maior clareza, a presente secção descreve, em primeiro lugar, alguns exemplos de cenários em relação aos quais algumas medidas técnicas poderão potencialmente ser eficazes para assegurar um nível de proteção essencialmente equivalente. A secção prossegue com alguns cenários em relação aos quais não foram identificadas medidas técnicas para assegurar este nível de proteção.

[77] Artigo 5.º, n.º 2, e artigo 32.º, do RGPD.
[78] Acórdão Schrems II, n.º 135.

Exemplos de cenários referentes a casos em que são identificadas medidas *eficazes*

79. As medidas abaixo enumeradas destinam-se a assegurar que o acesso aos dados transferidos por parte das autoridades públicas de países terceiros não afeta a eficácia das garantias adequadas contidas nos instrumentos de transferência do artigo 46.º do RGPD. Estas medidas serão necessárias para garantir um nível de proteção essencialmente equivalente ao garantido no EEE, mesmo que o acesso das autoridades públicas seja conforme com a legislação do país do importador, sempre que, na prática, esse acesso exceda o que é necessário e proporcionado numa sociedade democrática[79]. Estas medidas visam impedir o acesso potencialmente ilícito, impedindo as autoridades de identificar os titulares dos dados, inferir informações a seu respeito, distingui-los noutro contexto ou associar os dados transferidos a outros conjuntos de dados que possam conter, entre outros dados, identificadores em linha fornecidos pelos dispositivos, aplicações, ferramentas e protocolos utilizados pelos titulares dos dados noutros contextos.

80. As autoridades públicas de países terceiros podem tentar aceder aos dados transferidos:

    a) Durante o trânsito, mediante o acesso às linhas de comunicação utilizadas para transmitir os dados para o país de destino. O referido acesso pode ser passivo, sendo o conteúdo da comunicação simplesmente copiado, eventualmente após um processo de seleção. No entanto, o acesso também pode ser ativo, no sentido de que as autoridades públicas intervêm no processo de comunicação não só lendo o conteúdo, mas também manipulando ou suprimindo partes do mesmo;

    b) Durante a detenção dos dados por um destinatário previsto dos mesmos, mediante o acesso às próprias instalações de tratamento ou mediante a solicitação ao destinatário dos dados de que localize e extraia dados com interesse e os envie às autoridades.

81. A presente secção analisa cenários nos quais são aplicadas medidas eficazes em ambos os casos. Podem ser aplicáveis diferentes medidas complementares e estas podem ser suficientes numa transferência específica, caso a legislação do país de destino preveja apenas um tipo de acesso. Por conseguinte, é necessário que o exportador de dados analise cuidadosamente, com o apoio do importador de dados, as obrigações impostas a este último.

A título de exemplo, os importadores de dados dos Estados Unidos abrangidos pelo artigo 1881.º-A do título 50 do USC (artigo 702.º da FISA) têm a obrigação direta de conceder acesso ou entregar dados pessoais importados que se encontrem na sua posse, custódia ou controlo. O que precede pode aplicar-se a quaisquer chaves criptográficas necessárias para tornar os dados inteligíveis.

82. Os cenários descrevem circunstâncias específicas e são indicadas, a título de exemplo, as medidas tomadas. Quaisquer alterações dos cenários podem conduzir a diferentes conclusões. Os cenários referem situações em que se concluiu que eram, desde logo, necessárias medidas

[79] Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020.

complementares, ou seja, quando, na prática, é aplicada legislação problemática do país terceiro à transferência em causa.

83. Os responsáveis pelo tratamento podem ser obrigados a aplicar algumas ou todas as medidas descritas na presente secção, independentemente do nível de proteção previsto nas leis aplicáveis ao importador de dados, porque são necessárias para cumprir os artigos 25.º e 32.º do RGPD nas circunstâncias específicas da transferência. Por outras palavras, os exportadores podem ser obrigados a implementar as medidas descritas no presente diploma, mesmo que os respetivos importadores de dados estejam abrangidos por uma decisão de adequação, tal como os responsáveis pelo tratamento e os subcontratantes podem ser obrigados a implementar essas medidas quanto os dados são tratados no EEE.

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

84. Um exportador de dados utiliza um prestador de serviços de alojamento num país terceiro para armazenar dados pessoais, por exemplo, para fins de cópia de segurança.

Se:

1. os dados pessoais são tratados utilizando uma encriptação forte antes da transmissão e a identidade do importador é verificada,
2. o algoritmo de encriptação e a respetiva parametrização (por ex., comprimento da chave, modo de funcionamento, se aplicável) estão em conformidade com os últimos avanços e podem ser considerados robustos contra a criptoanálise realizada pelas autoridades públicas do país de destino, tendo em conta os recursos e as capacidades técnicas (por ex., poder de computação face a «ataques de força bruta») de que estes dispõem[80];
3. a robustez da encriptação e a extensão da chave têm em consideração o período de tempo específico durante o qual a confidencialidade dos dados pessoais encriptados deve ser mantida[81];

[80] Para a avaliação da solidez dos algoritmos de encriptação, da sua conformidade com os últimos avanços e da sua robustez em relação à análise criptográfica ao longo do tempo, os exportadores de dados podem basear-se em orientações técnicas publicadas pelas autoridades oficiais da cibersegurança da UE e dos seus Estados-Membros. Ver, por exemplo, o relatório da ENISA «What is "state of the art" in IT security?» (O que é o «estado-da-arte» em matéria de segurança informática?), 2019,https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; orientações do Gabinete Federal alemão em matéria de segurança informática nas suas Orientações Técnicas da série TR-02102 e «Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018» at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] A capacidade de proteção dos algoritmos criptográficos está sujeita a declínio ao longo do tempo, devido à descoberta de novas técnicas criptanalíticas, à emergência de novos paradigmas de computação, como a computação quântica, e ao aumento geral da capacidade computacional disponível, a menos que se prove que os algoritmos aplicados são teoricamente seguros em relação à informação. Esta preocupação aplica-se, em especial, aos algoritmos de chave pública que, no momento da redação, são de utilização comum. Por conseguinte, o exportador de dados deve ter em conta que as autoridades públicas podem aceder aos dados encriptados nas circunstâncias descritas no ponto 80 e armazená-los até que os seus recursos sejam suficientes para a desencriptação. A medida complementar só pode ser considerada eficaz se a desencriptação e o

4. o algoritmo de encriptação é implementado sem falhas através de software mantido de forma correta, cuja conformidade com a especificação do algoritmo escolhido foi verificada, por exemplo, mediante certificação;
5. as chaves são geridas de forma fiável (geradas, administradas, armazenadas, se aplicável, associadas à identidade de um destinatário pretendido e revogadas)[82] e
6. as chaves são conservadas exclusivamente sob o controlo do exportador de dados, ou por uma entidade de confiança do exportador no EEE ou sob uma jurisdição que ofereça um nível de proteção essencialmente equivalente ao garantido no EEE,

o CEPD considera que a encriptação efetuada constitui uma medida complementar eficaz.

Caso de utilização 2: Transferência de dados pseudonimizados

85. Um exportador de dados pseudonimiza primeiro os dados que detém e transfere-os, em seguida, para um país terceiro para análise, por exemplo para fins de investigação.

Se:

1. o exportador de dados transfere dados pessoais tratados de tal modo que já não podem ser atribuídos a um titular de dados específico, nem ser utilizados para identificar o titular de dados num grupo mais vasto sem a utilização de informações adicionais[83];
2. essas informações adicionais são detidas exclusivamente pelo exportador de dados e conservadas separadamente num Estado-Membro ou num país terceiro, por uma entidade de confiança do exportador no EEE ou numa jurisdição que ofereça um nível de proteção essencialmente equivalente ao garantido no EEE,
3. a divulgação ou utilização não autorizada de tais informações adicionais são impedidas mediante garantias técnicas e organizativas adequadas, é assegurado que o exportador de dados mantém o controlo exclusivo do algoritmo ou repositório que permite a reidentificação utilizando as informações adicionais; e
4. o responsável pelo tratamento determinou, através de uma análise exaustiva dos dados em questão, tendo em conta as informações que as autoridades públicas do país de destino possam possuir, que os dados pessoais pseudonimizados não podem ser atribuídos a uma pessoa singular identificada ou identificável, mesmo que sejam combinados com tais informações,

---

tratamento posterior subsequente já não constituir, nessa data, uma violação dos direitos dos titulares dos dados, por exemplo, porque os dados já não podem ser utilizados para identificá-los direta ou indiretamente.

[82] NIST Special Publication 800-57, *Recommendation for Key Management*https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] Em consonância com o artigo 4.º, ponto 5), do RGPD: «"Pseudonimização", o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;» Os dados adicionais podem consistir em quadros que justapõem pseudónimos com os atributos identificadores que substituem, chaves criptográficas ou outros parâmetros para a transformação de atributos, ou outros dados que permitam a atribuição dos dados pseudonimizados a pessoas singulares identificadas ou identificáveis.

o CEPD considera que a pseudonimização efetuada constitui uma medida complementar eficaz.

86. É de salientar que em muitas situações, os fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social de uma pessoa singular, a localização física ou a sua interação com um serviço baseado na Internet em momentos específicos[84] podem permitir a identificação da pessoa em causa, mesmo que o nome, a morada ou outros identificadores simples sejam omitidos.

87. O que é especialmente verdade nos casos em que os dados dizem respeito à utilização de serviços de informação (tempo de acesso, sequência de funcionalidades acedidas, características do dispositivo utilizado, etc.). Os referidos serviços podem perfeitamente ser, no que concerne ao importador de dados pessoais, abrangidos pela obrigação de conceder acesso às mesmas autoridades públicas na sua jurisdição, que por sua vez provavelmente possuem dados sobre a utilização de tais serviços de informação pela(s) pessoa(s) visada(s).

88. Além disso, dada a utilização de alguns serviços de informação ser pública por natureza, ou a sua explorabilidade por partes com recursos substanciais, os responsáveis pelo tratamento terão de ter um cuidado adicional considerando que as autoridades públicas na respetiva jurisdição provavelmente possuem dados sobre a utilização de serviços de informação por uma pessoa por estes visada.

89. Se, no decurso da execução da pseudonimização, os atributos contidos nos dados pessoais forem transformados utilizando um algoritmo criptográfico, aplicam-se as orientações constantes das notas de rodapé 80 e 81. Doravante, recomenda-se a renúncia à utilização exclusiva da criptografia e a aplicação de transformações baseadas em mecanismos de «*look up table*».

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

90. O exportador de dados pretende transferir dados para um destino onde a legislação e/ou as práticas permitem o acesso das autoridades públicas aos dados durante o trânsito entre o país do exportador e o país de destino.

Se:

1. o exportador de dados transfere dados pessoais para um importador de dados numa jurisdição onde a legislação e/ou a prática permitem que as autoridades públicas acedam aos dados durante o seu transporte através da Internet para o país terceiro sem as garantias essenciais europeias relativas a esse acesso, sendo utilizada encriptação de transporte em relação à qual é garantido que os protocolos de encriptação utilizados são de última geração e proporcionam uma proteção eficaz contra ataques ativos e passivos com recursos que se sabe estarem à disposição das autoridades públicas desse país terceiro,

[84] Artigo 4.º, ponto 1), do RGPD: «"Dados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;».

2. as partes envolvidas na comunicação acordam uma infraestrutura ou autoridade de certificação de chave pública digna de confiança,
3. são utilizadas medidas específicas de proteção de última geração contra ataques ativos e passivos contra os sistemas de envio e de receção que fornecem encriptação de transporte, incluindo testes de vulnerabilidades do software e de eventuais *backdoors*,
4. para o caso de a encriptação de transporte não proporcionar por si só a segurança adequada devido a experiência com vulnerabilidades da infraestrutura ou do software utilizado, os dados pessoais são também encriptados de ponta a ponta na camada de aplicação utilizando métodos de encriptação de última geração;
5. o algoritmo de encriptação e a respetiva parametrização (por ex., comprimento da chave, modo de funcionamento, se aplicável) estão em conformidade com os últimos avanços e podem ser considerados robustos contra a criptoanálise realizada pelas autoridades públicas quando os dados transitam para este país terceiro, tendo em conta os recursos e as capacidades técnicas (por ex., poder de computação face a «ataques de força bruta») de que estes dispõem (ver nota de rodapé 80 supra)[85];
6. a robustez da encriptação tiver em consideração o período de tempo específico durante o qual a confidencialidade dos dados pessoais encriptados deve ser mantida;
7. o algoritmo de encriptação é implementado sem falhas através de software mantido de forma correta, cuja conformidade com a especificação do algoritmo escolhido foi verificada, por exemplo, mediante certificação;
8. as chaves são geridas de forma fiável (geradas, administradas, armazenadas, se aplicável, associadas à identidade de um destinatário pretendido e revogadas) pelo exportador ou por uma entidade de confiança do exportador sob uma jurisdição que proporciona um nível de proteção essencialmente equivalente,

o CEPD considera que a encriptação de transporte efetuada, se necessário em combinação com a encriptação de ponta a ponta do conteúdo, constitui uma medida complementar eficaz.

Caso de utilização 4: Destinatário protegido

91. Um exportador de dados transfere dados pessoais para um importador de dados num país terceiro especificamente protegido pela legislação de tal país, por exemplo, com a finalidade de providenciar conjuntamente tratamento médico a um paciente ou serviços jurídicos a um cliente.

Se:

1. a lei de um país terceiro isenta o importador de dados residente de um possível acesso ilícito aos dados detidos por tal destinatário para o fim em questão, por exemplo, em virtude do dever de sigilo profissional aplicável ao importador de dados,
2. tal isenção abrange todas as informações na posse do importador de dados que podem ser utilizadas para contornar a proteção de informações privilegiadas (chaves criptográficas, palavras-passe, outras credenciais, etc.),
3. o importador de dados não recorre aos serviços de um subcontratante de forma a permitir que as autoridades públicas tenham acesso aos dados na posse do subcontratante e o

[85] Ver nota de rodapé 80 para algumas referências às orientações técnicas publicadas pelas autoridades oficiais da cibersegurança da UE e dos seus Estados-Membros.

importador de dados não transmite os dados a outra entidade que não esteja protegida com base nos instrumentos de transferência do artigo 46.º do RGPD,

4. os dados pessoais são encriptados antes de serem transmitidos através de um método conforme com os últimos avanços que assegura que a desencriptação não será possível sem o conhecimento da chave de desencriptação (encriptação de ponta a ponta) durante todo o período de tempo durante o qual os dados precisam de ser protegidos,
5. a chave de decifragem está sob o controlo exclusivo do importador de dados protegido e, eventualmente, do próprio exportador ou de outra entidade de confiança do exportador, situada no EEE ou numa jurisdição que oferece um nível de proteção essencialmente equivalente ao garantido no EEE, e está devidamente protegida contra a utilização ou divulgação não autorizadas através de medidas técnicas e organizativas conformes com os últimos avanços, e
6. o exportador de dados determinou de forma fiável que a chave de encriptação que pretende utilizar corresponde à chave de desencriptação detida pelo destinatário,

o CEPD considera que a encriptação de transporte efetuada constitui uma medida complementar eficaz.

Caso de utilização 5: Tratamento fracionado ou multipartido

92. O exportador de dados pretende que os dados pessoais sejam tratados conjuntamente por dois ou mais subcontratantes independentes localizados em jurisdições diferentes, sem lhes revelar o conteúdo dos dados. Antes da transmissão, o exportador divide os dados de modo que nenhum dos subcontratantes receba dados suficientes para reconstruir os dados pessoais, no todo ou em parte. O exportador de dados recebe o resultado do tratamento de cada um dos subcontratantes de forma independente e reúne as partes recebidas para obter o resultado final, que pode consistir em dados pessoais ou agregados.

Se:

1. o exportador de dados trata dados pessoais dividindo-os em duas ou mais frações, cada uma das quais não pode ser interpretada ou atribuída a um titular de dados específico sem a utilização de informações adicionais,
2. cada uma das frações dos dados é transferida para um subcontratante diferente localizado numa jurisdição diferente,
3. os subcontratantes tratam, opcionalmente, os dados em conjunto, por exemplo, utilizando cálculos seguros multipartes, de forma que estes não tenham acesso a qualquer informação que não possuíssem antes da computação,
4. o algoritmo utilizado para a computação partilhada é seguro contra adversários ativos;
5. o responsável pelo tratamento determinou, através de uma análise exaustiva dos dados em questão, tendo em conta quaisquer informações que as autoridades públicas dos países de destino possam possuir, que as frações dos dados pessoais transmitidas aos subcontratantes não podem ser atribuídas a uma pessoa singular identificada ou identificável, mesmo que sejam comparadas com tais informações,
6. não há indícios de colaboração entre as autoridades públicas localizadas nas respetivas jurisdições onde se encontram os subcontratantes, que lhes permitisse aceder a todos os conjuntos de dados pessoais na posse dos subcontratantes e reconstituir e analisar o conteúdo dos dados pessoais de uma forma clara em circunstâncias em que tal análise não respeitasse os direitos e liberdades fundamentais dos titulares dos dados. De igual modo, as autoridades

públicas de cada um destes países não devem estar habilitadas a aceder aos dados pessoais na posse dos subcontratantes em todas as jurisdições em causa.

o CEPD considera que o tratamento partilhado efetuado constitui uma medida complementar eficaz.

Exemplos de cenários referentes a casos em que não são identificadas medidas *eficazes*

93. As medidas abaixo descritas não serão eficazes em determinados cenários para assegurar um nível de proteção essencialmente equivalente dos dados transferidos para o país terceiro. Por conseguinte, não são elegíveis como medidas complementares.

Caso de utilização 6: Transferência para prestadores de serviços na nuvem ou outros subcontratantes que necessitam de acesso aos dados não encriptados

94. O exportador de dados transfere dados pessoais, quer por transmissão eletrónica, quer disponibilizando-os a um prestador de serviços de computação em nuvem ou a outro subcontratante para que os dados pessoais sejam tratados de acordo com as suas instruções num país terceiro (por ex., para a prestação de apoio técnico ou qualquer tipo de tratamento em nuvem), e esses dados não são — ou não podem ser — pseudonimizados, conforme descrito no Caso de Utilização 2, ou encriptados, conforme descrito no Caso de Utilização 1 porque o tratamento exige acesso aos dados não encriptados,

Se:

1. o responsável pelo tratamento transfere dados pessoais para um prestador de serviços na nuvem ou outro subcontratante;
2. o prestador de serviços na nuvem ou outro subcontratante precisa de obter acesso aos dados não encriptados, a fim de executar a tarefa que lhe foi atribuída, e
3. o poder conferido às autoridades públicas do país destinatário para aceder aos dados transferidos em questão vai além do que é necessário e proporcionado numa sociedade democrática, aplicando-se, na prática, a legislação problemática do país terceiro às transferências em questão (ver etapa 3)[86].

o CEPD não pode prever uma medida técnica eficaz para evitar que tal acesso viole os direitos do titular de dados, tendo em consideração o conhecimento atual. O CEPD não exclui que um desenvolvimento tecnológico futuro possa oferecer medidas que permitam alcançar os objetivos operacionais pretendidos, sem necessidade do acesso aos dados não encriptados.

95. Nos cenários indicados, sempre que os dados pessoais não encriptados sejam tecnicamente necessários para a prestação do serviço pelo subcontratante, a encriptação do transporte e a encriptação de dados estáticos, mesmo consideradas no seu conjunto, não constituem uma

[86] Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020.

medida complementar que assegura um nível de proteção essencialmente equivalente se o importador de dados dispuser das chaves criptográficas.

Caso de utilização 7: Transferência de dados pessoais para fins operacionais, incluindo através de acesso remoto

96. O exportador de dados transfere dados pessoais para entidades — num país terceiro para serem utilizados para fins operacionais partilhados — quer por transmissão eletrónica, quer disponibilizando-os para acesso remoto pelo importador de dados, e esses dados não são — ou podem ser - pseudonimizados, conforme descrito no Caso de Utilização 2, ou encriptados, conforme descrito no Caso de Utilização 1, porque o tratamento exige acesso aos dados não encriptados. Uma configuração típica pode consistir num responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro que transfere dados pessoais para um responsável pelo tratamento ou subcontratante num país terceiro pertencente ao mesmo grupo de empresas, ou grupo de empresas envolvidas numa atividade económica conjunta. O importador de dados pode, por exemplo, utilizar os dados que recebe para prestar serviços de pessoal ao exportador de dados, para os quais necessita de dados de recursos humanos, ou para comunicar com os clientes do exportador de dados que vivem na União Europeia por telefone ou correio eletrónico.

Se:

1. o exportador de dados transfere dados pessoais para o importador de dados num país terceiro, mediante a disponibilização dos mesmos num sistema informático que permita ao importador o acesso direto aos dados que pretende, mediante a transferência direta dos mesmos, individualmente ou em massa, através da utilização de um serviço de comunicação;
2. o importador[87] trata os dados não encriptados no país terceiro (incluindo para os seus próprios fins, quando o importador é responsável pelo tratamento),
3. o poder conferido às autoridades públicas do país destinatário para aceder aos dados transferidos vai além do que é necessário e proporcionado numa sociedade democrática, aplicando-se, na prática, a legislação problemática do país terceiro às transferências em questão (ver etapa 3),

o CEPD não pode prever uma medida técnica eficaz para evitar que tal acesso viole os direitos fundamentais do titular dos dados.

97. Nos cenários indicados, sempre que os dados pessoais não encriptados sejam tecnicamente necessários para a prestação do serviço pelo subcontratante, a encriptação do transporte e a encriptação de dados estáticos, mesmo consideradas no seu conjunto, não constituem uma medida complementar que assegura um nível de proteção essencialmente equivalente se o importador de dados dispuser das chaves criptográficas.

[87] Quer seja responsável pelo tratamento ou subcontratante num país terceiro que recebe ou obtém acesso a dados pessoais transferidos do EEE.

2.2 Medidas contratuais adicionais

98. As medidas em causa consistirão, geralmente, em compromissos contratuais[88] unilaterais, bilaterais ou multilaterais.[89] Se for utilizado um instrumento de transferência do artigo 46.º do RGPD, este já contém, na maioria dos casos, vários compromissos (essencialmente contratuais) do exportador e do importador de dados destinados a proteger os dados pessoais.[90]

99. Em determinadas situações, as referidas medidas podem complementar e reforçar as garantias previstas no instrumento de transferência e na legislação pertinente do país terceiro, sempre que, tendo em conta as circunstâncias da transferência, estas não cumpram todas as condições necessárias para assegurar um nível de proteção essencialmente equivalente ao garantido no EEE. Tendo em conta a natureza das medidas contratuais, que não são, regra geral, suscetíveis de vincular as autoridades do país terceiro uma vez que estas não são partes no contrato[91] estas medidas devem ser combinadas com outras medidas técnicas e organizativas para proporcionar o nível de proteção de dados exigido. A seleção e implementação de uma ou mais das referidas medidas não garantem necessária e sistematicamente que a transferência cumpre a norma de equivalência essencial exigida pela legislação da UE.

100. Dependendo das medidas contratuais já incluídas no instrumento de transferência do artigo 46.º do RGPD utilizado, podem também ser úteis medidas contratuais adicionais para permitir aos exportadores de dados baseados no EEE tomar conhecimento dos novos desenvolvimentos que afetam a proteção dos dados transferidos para países terceiros.

101. Conforme referido, estas medidas contratuais não poderão excluir a aplicação da legislação de um país terceiro que não cumpre a norma das Garantias Essenciais Europeias do CEPD nos casos em que esta legislação obriga os importadores a cumprir as ordens de divulgação de dados que recebem das autoridades públicas.[92]

102. Alguns exemplos destas potenciais medidas contratuais são enumerados a seguir e classificados de acordo com a sua natureza:

Cláusula que prevê a obrigação contratual de utilizar medidas técnicas específicas

103. Consoante as circunstâncias específicas das transferências (incluindo a aplicação prática da legislação do país terceiro), o contrato poderá ter de prever a implementação de medidas técnicas específicas para permitir a realização das transferências (ver as medidas técnicas sugeridas supra).

104. Condições de eficácia:

---

[88] Por exemplo, nas regras vinculativas aplicáveis às empresas que deverão, em todo o caso, regular algumas das medidas a seguir referidas.

[89] Serão de natureza privada e não serão considerados acordos internacionais nos termos do direito internacional público. Por conseguinte, não vincularão, em princípio, as autoridades públicas do país terceiro uma vez que não são partes no contrato celebrado com organismos privados em países terceiros, conforme sublinhado pelo Tribunal de Justiça no seu acórdão Schrems II, n.º 125.

[90] Ver Acórdão Schrems II, n.º 137, no qual o Tribunal de Justiça reconheceu que as cláusulas contratuais-tipo contêm «mecanismos efetivos que permit[e]m, na prática, garantir que o nível de proteção exigido pelo direito da União seja respeitado e que as transferências de dados pessoais, baseadas nessas cláusulas, sejam suspensas ou proibidas em caso de violação dessas cláusulas ou de impossibilidade de as honrar»; ver também o n.º 148.

[91] Acórdão Schrems II, n.º 125.

[92] Acórdão Schrems II, n.º 132.

- Esta cláusula poderá ser eficaz nas situações em que o exportador identificou a necessidade de medidas técnicas. Deve revestir forma jurídica para garantir que o importador também se compromete a adotar as medidas técnicas necessárias, caso necessário.

Obrigações de transparência:

105. O exportador poderá adicionar anexos ao contrato com informações fornecidas pelo importador antes da conclusão do contrato, com base nos seus melhores esforços, relativamente ao acesso aos dados pelas autoridades públicas, incluindo no domínio da informação, desde que a legislação do país de destino cumpra as garantias essenciais europeias do CEPD. O que poderá ajudar o exportador de dados a cumprir a sua obrigação de documentar a avaliação do nível de proteção no país terceiro. Pode igualmente sublinhar a obrigação do importador de ajudar o exportador na sua avaliação e de assumir a sua responsabilidade na prestação de informações objetivas, fiáveis, pertinentes, verificáveis e acessíveis ao público ou de outro modo acessíveis.

106. O importador poderá, por exemplo, ser obrigado a:

(1) enumerar as leis e regulamentos do país de destino aplicáveis ao importador ou aos respetivos subcontratantes (ulteriores) que permitiriam o acesso das autoridades públicas aos dados pessoais sujeitos à transferência, nomeadamente, no domínio das informações, da aplicação da lei, da supervisão administrativa e regulamentar aplicável aos dados transferidos;

(2) na ausência de leis que regulamentem o acesso das autoridades públicas aos dados, prestar informações e estatísticas baseadas na sua experiência ou em relatos de várias fontes (por ex., parceiros, fontes abertas, jurisprudência nacional e decisões dos organismos de controlo) no que concerne ao acesso das autoridades públicas aos dados pessoais em situações do tipo da transferência de dados em causa (ou seja, no domínio regulamentar específico, relativamente ao tipo de entidades a que pertence o importador de dados, etc.);

(3) indicar as medidas adotadas para impedir o acesso aos dados transferidos (caso aplicável);

(4) fornecer informações suficientemente pormenorizadas sobre todos os pedidos de acesso a dados pessoais das autoridades públicas recebidos pelo importador num determinado período de tempo[93], em especial nas áreas acima mencionadas no ponto 1), incluindo informações sobre os pedidos recebidos, os dados solicitados, o organismo requerente e a base jurídica da divulgação e a divulgação pelo importador do pedido de dados[94];

(5) especificar se e em que medida o importador está legalmente proibido de fornecer as informações mencionadas nos pontos 1) a 5) supra.

[93] A duração do período deverá depender do risco para os direitos e liberdades dos titulares dos dados cujos dados são objeto da transferência em causa (por ex., o último ano antes da revogação do instrumento de exportação de dados com o exportador de dados).

[94] O cumprimento deste dever não equivale a proporcionar um nível de proteção adequado. Além, qualquer divulgação inadequada que tenha efetivamente ocorrido torna necessária a implementação de medidas complementares.

107. Estas informações poderão ser prestadas por meio de questionários estruturados preenchidos e assinados pelo importador e reforçadas pela obrigação contratual do importador de declarar, num determinado prazo, qualquer potencial alteração desta informação, como é prática corrente nos processos de diligência devida.

108. Condições de eficácia:

- O importador deve poder prestar este tipo de informação ao exportador, na medida dos seus conhecimentos e depois de ter desenvolvido os seus melhores esforços para a obter.
- Esta obrigação imposta ao importador é uma forma de assegurar que o exportador se consciencializa e se mantém consciente dos riscos associados à transferência de dados para um país terceiro. Por conseguinte, permitirá ao exportador abster-se de celebrar o contrato ou, se a informação sofrer alterações após a sua celebração, permitir-lhe-á cumprir a obrigação de suspender a transferência e/ou rescindir o contrato, caso a legislação do país terceiro, as garantias contidas no instrumento de transferência do artigo 46.º do RGPD utilizado e quaisquer garantias adicionais que possa ter adotado deixem de assegurar um nível de proteção essencialmente equivalente ao garantido no EEE. No entanto, tal obrigação não pode justificar a divulgação de dados pessoais pelo importador, nem criar a expectativa de que não haverá novos pedidos de acesso.

***

109. O exportador pode igualmente adicionar cláusulas que permitam ao importador certificar que 1) não criou deliberadamente «*backdoors*» ou programações semelhantes que possam ser utilizados para aceder ao sistema e/ou aos dados pessoais, 2) não criou ou alterou propositadamente os seus processos operacionais de forma a facilitar o acesso a sistemas ou dados pessoais, e que 3) a legislação nacional ou a política do Governo não exige que o importador crie ou mantenha «*backdoors*», facilite o acesso a sistemas ou dados pessoais ou que o importador detenha ou transmita a chave de encriptação[95].

110. Condições de eficácia:

- A existência de legislação ou políticas do Governo que impeçam os importadores de divulgar esta informação pode tornar esta cláusula ineficaz. Por conseguinte, o importador não poderá celebrar o contrato ou deverá notificar o exportador da impossibilidade de cumprir os seus compromissos contratuais.
- O contrato deve incluir sanções e/ou a possibilidade de o exportador rescindir o contrato a curto prazo nos casos em que o importador não revelar a existência de *backdoors* ou programas similares, de processos comerciais manipulados ou de qualquer obrigação de adoção de qualquer um destes procedimentos ou não informar imediatamente o exportador logo que tenha conhecimento da sua existência.
- Nos casos em que o importador de dados divulgou dados pessoais transferidos em violação dos compromissos contidos no instrumento de transferência escolhido, o contrato pode

[95] A presente cláusula é importante para garantir um nível adequado de proteção dos dados pessoais transferidos e deve ser normalmente obrigatória.

também incluir a indemnização pelo importador de dados do titular de dados pelos danos materiais e morais sofridos.

***

111. O exportador poderá reforçar o seu poder de realizar auditorias[96] ou inspeções das instalações de tratamento de dados do importador, no local e/ou à distância, por forma a verificar se os dados foram divulgados às autoridades públicas e em que condições (acesso que não vai além do que é necessário e proporcionado numa sociedade democrática), por exemplo, mediante o estabelecimento de um pré-aviso a curto prazo e de mecanismos que garantam a intervenção rápida dos organismos de inspeção e o reforço da autonomia do exportador na seleção dos organismos de inspeção.

112. Condições de eficácia:

- Para que esta seja totalmente eficaz, o âmbito de aplicação da auditoria deve abranger, legal e tecnicamente, qualquer tratamento dos dados pessoais transmitidos no país terceiro pelos subcontratantes ou subcontratantes ulteriores do importador.
- Os registos de acesso e outras pistas semelhantes devem ser invioláveis (por ex., devem ser inalteráveis utilizando técnicas de encriptação de ponta, como o *hashing* e ser sistematicamente transmitidos ao exportador com uma determinada frequência), de modo que os auditores possam encontrar elementos de prova da divulgação. Os registos de acesso e outros registos semelhantes devem também distinguir entre os acessos devidos a operações normais e os acessos devidos a ordens ou pedidos de acesso.

***

113. Nos casos em que o direito e a prática do país terceiro do importador foram inicialmente avaliados e se considerou que asseguravam um nível de proteção dos dados transferidos pelo exportador essencialmente equivalente ao garantido na UE, o exportador poderá ainda reforçar a obrigação do importador de dados de informar imediatamente o exportador de dados do facto de não poder cumprir os compromissos contratuais e, por conseguinte, a norma exigida do «nível de proteção de dados essencialmente equivalente».[97]..

114. A referida impossibilidade de cumprimento pode resultar de alterações da legislação ou da prática do país terceiro[98]. As cláusulas podem estabelecer prazos e procedimentos específicos e rigorosos para a suspensão rápida da transferência de dados e/ou rescisão do contrato, bem como para a devolução ou eliminação dos dados recebidos pelo importador. O rastreamento dos pedidos

[96] Ver, por exemplo, a cláusula 5, alínea f), das cláusulas contratuais-tipo entre responsáveis pelo tratamento e subcontratantes da Decisão 2010/87/UE; as auditorias também podem ser previstas no âmbito de um código de conduta ou através da certificação.

[97] Cláusula 5, alíneas a) e d), i), da Decisão 2010/87/UE.

[98] Ver Acórdão Schrems II, n.º 139, no qual o Tribunal de Justiça afirma que «embora a cláusula 5, alínea d), i), permita ao destinatário da transferência de dados pessoais não comunicar ao responsável pelo tratamento estabelecido na União um pedido juridicamente vinculativo de divulgação dos dados pessoais por parte de uma autoridade competente para a aplicação da lei, em caso de legislação que o impeça, como uma proibição de caráter penal que vise preservar o segredo de um inquérito policial, está, no entanto, obrigado, em conformidade com a cláusula 5, alínea a), do anexo da Decisão CPT a informar o responsável pelo tratamento do facto de não poder cumprir as cláusulas-tipo de proteção de dados».

recebidos, do respetivo âmbito e da eficácia das medidas adotadas para contrariá-los devem fornecer ao exportador indicações suficientes para exercer o seu dever de suspensão ou cessação da transferência e/ou de rescisão do contrato.

115. Condições de eficácia:

- A notificação deve ser realizada antes de ser concedido o acesso aos dados. Caso contrário, quando o exportador recebe a notificação, os direitos do indivíduo podem já ter sido violados, se o pedido se basear em leis do país terceiro que vão além do nível de proteção de dados permitido pela legislação da UE. A notificação pode ainda servir para prevenir futuras violações e permitir ao exportador cumprir o seu dever de suspender a transferência de dados pessoais para o país terceiro e/ou de rescindir o contrato.
- O importador de dados deve monitorizar os desenvolvimentos jurídicos ou políticos suscetíveis de impedi-lo de cumprir as suas obrigações e deve informar imediatamente o exportador de dados de tais alterações e desenvolvimentos, se possível antes da sua implementação, para permitir ao exportador de dados recuperar os dados junto do importador de dados.
- As cláusulas deverão prever um mecanismo rápido através do qual o exportador de dados autoriza o importador de dados a proteger ou a devolver-lhe imediatamente os dados ou, se tal não for viável, a apagar ou encriptar os dados de um modo seguro sem necessariamente esperar pelas instruções do exportador, caso seja atingido um limiar específico[99] a acordar entre o exportador de dados e o importador de dados. O importador de dados deve implementar o referido mecanismo no início da transferência de dados e testá-lo regularmente a fim de se assegurar de que este pode executado num curto prazo de tempo.
- Outras cláusulas poderão permitir ao exportador monitorizar o cumprimento destas obrigações pelo importador por meio de auditorias, inspeções e outras medidas de verificação e impor a sua observância mediante a aplicação de sanções ao importador e/ou do recurso à possibilidade de o exportador suspender a transferência e/ou rescindir imediatamente o contrato.

***

116. Na medida do permitido pela legislação nacional do país terceiro, o contrato poderá reforçar as obrigações de transparência do importador prevendo um método «*warrant canary*», segundo o qual o importador se compromete a publicar regularmente (por ex., pelo menos cada 24 horas) uma mensagem com uma assinatura encriptada a informar o exportador de que até uma determinada data e hora não recebeu uma ordem de divulgação de dados pessoais ou afins. A ausência de uma atualização desta notificação indicará ao exportador que o importador pode ter recebido uma ordem nesse sentido.

117. Condições de eficácia:

- Os regulamentos do país terceiro devem permitir que o importador de dados emita esta forma de notificação passiva ao exportador.
- O exportador de dados deve monitorizar automaticamente as notificações do tipo «*warrant canary*».

[99] Este limiar deverá assegurar que os titulares dos dados continuam a beneficiar de um nível de proteção equivalente ao garantido no EEE.

- O importador de dados deve assegurar que a sua chave privada de assinatura do «*warrant canary*» é mantida em segurança e não pode ser forçada para emitir falsas notificações «w*arrant canary*» pelos regulamentos do país terceiro. Para o efeito, poderá ser útil a utilização de várias assinaturas por diferentes pessoas e/ou que o «*warrant canary*» seja emitido por uma pessoa fora da jurisdição do país terceiro.

Obrigações de adotar medidas específicas

118. O importador poderá comprometer-se a examinar, ao abrigo da legislação do país de destino, a legalidade de qualquer ordem de divulgação de dados, nomeadamente se se enquadra nos limites dos poderes concedidos à autoridade pública requerente, e a impugnar a ordem se, após uma avaliação minuciosa, concluir que existem fundamentos ao abrigo da lei do país de destino para o fazer. No caso de impugnar uma ordem, o importador de dados deverá solicitar medidas provisórias para suspender os efeitos da ordem até que o tribunal decida quanto ao mérito. O importador não poderá divulgar os dados pessoais solicitados enquanto não for a tal obrigado por força das regras processuais aplicáveis. O importador de dados comprometer-se-á igualmente a fornecer a menor quantidade possível de informações permitida ao dar cumprimento à ordem, com base numa interpretação razoável da mesma.

119. Condições de eficácia:

- O ordenamento jurídico do país terceiro deve oferecer vias jurídicas eficazes para impugnação das ordens de divulgação de dados.
- Esta cláusula oferecerá sempre uma proteção adicional muito limitada, uma vez que uma ordem de divulgação de dados pode ser legal ao abrigo do ordenamento jurídico do país terceiro, mas o ordenamento jurídico pode não cumprir as normas da UE. Esta medida contratual deverá necessariamente ser complementada por outras medidas complementares.
- A impugnação de uma ordem deve ter efeito suspensivo nos termos do direito do país terceiro. Caso contrário, as autoridades públicas continuariam a ter acesso aos dados dos particulares e qualquer ação subsequente a favor do particular teria o efeito limitado de lhe permitir apresentar um pedido de indemnização pelas consequências negativas resultantes da divulgação dos dados.
- O importador deve poder documentar e demonstrar ao exportador as medidas que adotou, desenvolvendo os seus melhores esforços para cumprir tal compromisso.

***

120. Na mesma situação acima descrita, o importador poderá obrigar-se a informar a autoridade pública requerente da incompatibilidade da ordem com as garantias contidas no instrumento de transferência do artigo 46.º do RGPD[100] e do conflito de obrigações daí resultante para o

[100] Por exemplo, as cláusulas contratuais-tipo preveem que o tratamento dos dados, incluindo a sua transferência, foi e continuará a ser efetuado em conformidade com a «*legislação sobre proteção de dados aplicável*». A referida legislação é definida como «*a legislação que protege os direitos e as liberdades fundamentais das pessoas e, em especial, o seu direito à proteção da vida privada no que diz respeito ao*

importador. O importador informará simultaneamente e logo que possível o exportador e/ou a autoridade de controlo competente do EEE, na medida em que tal seja permitido pelo ordenamento jurídico do país terceiro.

121. Condições de eficácia:

- Estas informações sobre a proteção conferida pela legislação da UE e o conflito de obrigações deverão produzir efeitos jurídicos no ordenamento jurídico do país terceiro, como a fiscalização jurisdicional ou administrativa da ordem ou do pedido de acesso, a exigência de um mandado judicial e/ou a suspensão temporária da ordem para permitir adicionar proteção aos dados.
- O sistema jurídico do país não deve impedir o importador de notificar o exportador ou, pelo menos, a autoridade de controlo competente do EEE da ordem ou do pedido de acesso recebidos.
- O importador deve poder documentar e demonstrar ao exportador as medidas que adotou, no exercício dos seus melhores esforços para cumprir tal compromisso.

Conferir aos titulares dos dados os meios para exercerem os seus direitos

122. O contrato poderá prever que os dados pessoais transmitidos em texto corrido no desempenho normal da atividade (incluindo nos casos de apoio) só podem ser acedidos com o consentimento expresso ou implícito do exportador e/ou do titular dos dados.

123. Condições de eficácia:

- Esta cláusula poderá ser eficaz nas situações em que os importadores recebem pedidos das autoridades públicas de cooperação voluntária, por oposição, por exemplo, ao acesso das autoridades públicas aos dados que ocorre sem o conhecimento do importador de dados ou contra a sua vontade.
- Em determinadas situações, o titular dos dados pode não estar em condições de se opor ao acesso ou de dar um consentimento que satisfaça todas as condições estabelecidas na legislação da UE (livre, específico, informado e inequívoco) (por ex., no caso de funcionários).[101]
- As políticas ou os regulamentos nacionais que obriguem o importador a não divulgar a ordem de acesso podem tornar a presente cláusula ineficaz, a menos que possa ser complementada com métodos técnicos que exijam a intervenção do exportador ou do titular dos dados para que os dados possam ser acessíveis em «texto corrido». As referidas medidas técnicas de restrição do acesso podem ser previstas nomeadamente se o acesso apenas for concedido em casos específicos de apoio ou assistência, mas os dados propriamente ditos estiverem armazenados no EEE.

---

tratamento dos seus dados pessoais, aplicável a um responsável pelo tratamento dos dados no Estado-Membro em que o exportador de dados está estabelecido». O Tribunal de Justiça confirma que as disposições do RGPD, lidas à luz da Carta dos Direitos Fundamentais da UE, fazem parte desta legislação (ver acórdão Schrems II, n.º 138).

[101] Artigo 4.º, n.º 11, do RGPD.

***

124. O contrato poderá obrigar o importador e/ou o exportador a notificar imediatamente o titular dos dados do pedido ou da ordem recebida das autoridades públicas do país terceiro ou da impossibilidade de o importador cumprir os compromissos contratuais, a fim de permitir ao titular dos dados procurar informações e uma via de recurso eficaz (por ex., apresentando uma reclamação junto da respetiva autoridade de controlo competente e/ou autoridade judicial e demonstrando a sua legitimidade processual nos tribunais do país terceiro), incluindo a indemnização pelo importador de dados dos eventuais danos materiais e morais sofridos por causa da divulgação dos dados pessoais do titular dos dados transferidos ao abrigo do instrumento de transferência escolhido em violação dos compromissos que este contém.

125. Condições de eficácia:

- Esta notificação poderá alertar o titular dos dados para possíveis acessos das autoridades públicas de países terceiros aos seus dados. Poderá, por conseguinte, permitir ao titular dos dados solicitar informações adicionais aos exportadores e apresentar uma reclamação à autoridade de controlo competente. Esta cláusula poderá igualmente abordar e compensar algumas das dificuldades que um indivíduo poderá enfrentar para demonstrar a sua legitimidade processual (*locus standi*) nos tribunais de países terceiros para contestar o acesso das autoridades públicas aos seus dados.
- A regulamentação e as políticas nacionais podem impedir a referida notificação do titular dos dados. O exportador e o importador poderão, no entanto, comprometer-se a informar o titular dos dados logo que as restrições de divulgação dos dados sejam levantadas e a desenvolver os seus melhores esforços para obter a derrogação da proibição de divulgação. No mínimo, o exportador ou a autoridade de controlo competente poderão notificar o titular dos dados da suspensão ou da cessação da transferência dos seus dados pessoais devido à impossibilidade de o importador cumprir os seus compromissos contratuais, na sequência da receção de um pedido de acesso.

***

126. O exportador e o importador poderão obrigar-se contratualmente a auxiliar o titular dos dados no exercício dos seus direitos na jurisdição do país terceiro através de mecanismos de recurso *ad hoc* e de aconselhamento jurídico.

127. Condições de eficácia

- Algumas regulamentações nacionais podem não permitir que o importador de dados preste este tipo de assistência diretamente aos titulares dos dados, embora possam permitir que o importador de dados obtenha esta assistência aos titulares dos dados.
- As políticas ou os regulamentos nacionais podem impor condições que podem comprometer a eficácia dos processos de recurso *ad hoc* previstos.
- O aconselhamento jurídico poderá ser útil ao titular dos dados, sobretudo tendo em conta a complexidade e o custo que poderão representar para um titular dos dados a compreensão do sistema jurídico de um país terceiro e os processos legais instaurados no estrangeiro, possivelmente numa língua estrangeira. No entanto, esta cláusula proporcionará sempre uma proteção adicional limitada, uma vez que a prestação de assistência e aconselhamento jurídico aos titulares dos dados não pode, por si só, corrigir o facto de o ordenamento jurídico de um

país terceiro não prever um nível de proteção essencialmente equivalente ao garantido no EEE. Esta medida contratual deverá necessariamente ser complementada por outras medidas complementares.

- Esta medida complementar apenas será eficaz se a legislação do país terceiro disponibilizar a vias de recurso nos tribunais nacionais ou se existir um mecanismo de recurso *ad hoc*, incluindo para impugnação das medidas de vigilância.

2.3. Disposições organizativas

128. As medidas organizativas adicionais podem consistir em políticas internas, métodos organizativos e normas que os responsáveis pelo tratamento e subcontratantes podem aplicar e impor aos importadores de dados em países terceiros. Podem contribuir para assegurar a coerência na proteção dos dados pessoais ao longo de todo o ciclo de tratamento. As medidas organizativas também podem melhorar a sensibilização dos exportadores para os riscos e tentativas de obtenção de acesso aos dados em países terceiros, bem como a sua capacidade de reação. A seleção e implementação de uma ou várias das referidas medidas não asseguram necessária e sistematicamente que a transferência cumpre a norma de equivalência essencial exigida pela legislação da UE. Em função das circunstâncias específicas da transferência e da avaliação da legislação do país terceiro, são necessárias medidas organizativas para complementar as medidas contratuais e/ou técnicas, a fim de garantir um nível de proteção dos dados pessoais essencialmente equivalente ao garantido na UE.

129. A avaliação das medidas mais adequadas deve ser realizada caso a caso, tendo presente a necessidade de os responsáveis pelo tratamento e subcontratantes cumprirem o princípio da responsabilidade. O CEPD apresenta a seguir alguns exemplos de medidas organizativas que os exportadores podem implementar, embora a lista não seja exaustiva e outras medidas possam ser igualmente adequadas.

Políticas internas de gestão de transferências, em especial entre grupos de empresas

130. Adoção de políticas internas adequadas com a atribuição clara de responsabilidades em matéria de transferências de dados, canais de comunicação e procedimentos operacionais normalizados no caso de pedidos formais ou informais das autoridades públicas de acesso aos dados. Em especial no caso de transferências entre grupos de empresas, estas políticas podem incluir, entre outras, a nomeação de uma equipa específica, composta por peritos de informática, legislação em matéria de proteção de dados e de privacidade, para tratar os pedidos que envolvam dados pessoais transferidos do EEE; a notificação à direção jurídica e à direção geral da empresa após a receção de tais pedidos; as medidas processuais de impugnação dos pedidos desproporcionados ou ilícitos e a prestação de informações transparentes aos titulares dos dados.

131. Desenvolvimento de procedimentos de formação específicos para o pessoal responsável pela gestão dos pedidos de acesso a dados pessoais das autoridades públicas, os quais devem ser atualizados periodicamente para refletir os novos desenvolvimentos legislativos e jurisprudenciais no país terceiro e no EEE. Os procedimentos de formação devem incluir os requisitos da legislação da UE quanto ao acesso aos dados pessoais pelas autoridades públicas, nomeadamente por força do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais. É necessária uma maior sensibilização do pessoal, nomeadamente mediante a avaliação de exemplos práticos de pedidos de acesso aos dados por parte das autoridades públicas e da aplicação da norma decorrente do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais a tais exemplos práticos. A referida formação deve ter em conta a situação específica do importador de dados, por exemplo, a legislação e a regulamentação do país terceiro a que o importador de dados está sujeito, e deve ser desenvolvida, sempre que possível, em cooperação com o exportador de dados.

132. Condições de eficácia:

- Estas políticas apenas podem ser consideradas nos casos em que o pedido das autoridades públicas do país terceiro é compatível com a legislação da UE[102]. Sempre que o pedido seja incompatível, tais políticas não serão suficientes para assegurar um nível de proteção dos dados pessoais equivalente, e, conforme referido, as transferências devem ser interrompidas ou devem ser adotadas medidas complementares adequadas para evitar o acesso.

Medidas de transparência e responsabilidade

133. Documentação e registo dos pedidos de acesso recebidos das autoridades públicas e da resposta fornecida, juntamente com a fundamentação jurídica e os intervenientes envolvidos (por ex., se o exportador foi notificado e a sua resposta, a avaliação da equipa responsável pelo tratamento dos pedidos, etc.). Estes registos deverão ser colocados à disposição do exportador de dados que, por sua vez, deverá disponibilizá-los aos titulares dos dados.

134. Condições de eficácia:

- A legislação nacional do país terceiro pode impedir a divulgação dos pedidos ou de informações pertinentes dos mesmos e, por conseguinte, tornar esta prática ineficaz. O importador de dados deverá informar o exportador da sua impossibilidade de fornecer estes documentos e registos, a fim de dar ao exportador a possibilidade de interromper as transferências se daí resultar a impossibilidade de proporcionar um nível adequado de proteção.

***

135. Publicação regular de relatórios sobre a transparência ou de resumos dos pedidos de acesso a dados da administração pública e o tipo de resposta fornecida, na medida em que a publicação seja permitida pelo direito nacional.

136. Condições de eficácia:

- As informações fornecidas devem ser pertinentes, claras e o mais detalhadas possível. A legislação nacional do país terceiro pode impedir a divulgação de informações detalhadas. Nesses casos, o importador de dados deve desenvolver os seus melhores esforços para publicar informação estatística ou informação agregada semelhante.

Métodos organizativos e medidas de minimização dos dados

137. No contexto de uma transferência, podem ser igualmente úteis os requisitos organizativos já existentes ao abrigo do princípio da responsabilidade, como a adoção de políticas e melhores práticas rigorosas e detalhadas sobre o acesso aos dados e a confidencialidade, baseadas na aplicação do princípio da «necessidade estrita de saber», controladas por auditorias regulares e impostas por meio de medidas disciplinares. A minimização dos dados deve ser considerada a este respeito, a fim de limitar a exposição dos dados pessoais a acessos não autorizados. Em alguns casos, por exemplo, poderá não ser necessário transferir determinados dados (por ex., em

[102] Ver Acórdão Schrems I, n.º 94; Acórdão Schrems II, n.os 168, 174, 175 e 176.

caso de acesso remoto a dados do EEE, como em casos de apoio, em que é concedido acesso restrito em vez de acesso total; ou quando a prestação de um serviço exige apenas a transferência de um conjunto limitado de dados e não da base de dados completa).

138. Condições de eficácia:

- Devem ser realizadas auditorias regulares e impostas medidas disciplinares rigorosas a fim de controlar e impor o cumprimento das medidas de minimização dos dados também no contexto da transferência.
- O exportador de dados deve realizar uma avaliação dos dados pessoais na sua posse antes da transferência, a fim de identificar os conjuntos de dados que não são necessários para os fins da transferência e que, por conseguinte, não serão partilhados com o importador de dados.
- As medidas de minimização de dados devem ser acompanhadas de medidas técnicas para assegurar que os dados não são sujeitos a acessos não autorizados. Por exemplo, a implementação de mecanismos de computação multipartidária segura e a propagação de conjuntos de dados encriptados entre diferentes entidades de confiança podem impedir por defeito que qualquer acesso unilateral conduza à divulgação de dados identificáveis.

***

139. Desenvolvimento de melhores práticas para envolver de forma adequada e atempada e dar acesso à informação ao encarregado da proteção de dados, caso exista, e aos serviços jurídicos e de auditoria interna em matérias relacionadas com as transferências internacionais de dados pessoais.

140. Condições de eficácia:

- O encarregado da proteção de dados, caso exista, e a equipa jurídica e de auditoria interna devem receber todas as informações pertinentes antes da transferência e devem ser consultados sobre a necessidade da transferência e de garantias adicionais, caso aplicável.
- As informações pertinentes devem incluir, por exemplo, a avaliação da necessidade da transferência dos dados pessoais específicos, uma visão geral da legislação do país terceiro aplicável e as garantias que o importador se comprometeu a implementar.

Adoção de normas e melhores práticas

141. Adoção de políticas rigorosas em matéria de segurança e de confidencialidade dos dados, baseadas na certificação da UE, nos códigos de conduta europeus ou nas normas internacionais (por ex., normas ISO) e nas melhores práticas (por ex., ENISA), tendo em devida conta os últimos avanços, em conformidade com o risco das categorias de dados tratados.

Outros

142. Adoção e revisão regular das políticas internas para avaliar a adequação das medidas complementares implementadas e para identificar e implementar soluções adicionais ou alternativas sempre que necessário, por forma a assegurar a manutenção de um nível de proteção dos dados pessoais transferidos equivalente ao garantido no EEE.

***

143. Compromissos do importador de dados de não proceder a qualquer transferência ulterior dos dados pessoais no país terceiro ou noutros países terceiros ou de suspender as transferências em curso sempre que não puder ser assegurado no país terceiro um nível de proteção dos dados pessoais equivalente ao garantido no EEE.[103]

[103] Acórdão Schrems II, n.os 135 e 137.

ANEXO 3: POSSÍVEIS FONTES DE INFORMAÇÃO PARA A AVALIAÇÃO DE UM PAÍS TERCEIRO

144. O importador de dados deve poder fornecer ao exportador as fontes e as informações pertinentes relativas ao país terceiro onde está estabelecido e à legislação que lhe é aplicável. O exportador e o importador podem consultar várias fontes de informação, tais como as que a seguir se enumeram de forma não exaustiva e por ordem de preferência:

- jurisprudência do Tribunal de Justiça da União Europeia (Tribunal de Justiça) e do Tribunal Europeu dos Direitos Humanos (TEDH)[104], conforme referido nas recomendações das Garantias Essenciais Europeias[105];
- decisões de adequação no país de destino se a transferência assentar numa base jurídica diferente[106];
- deliberações e relatórios de organizações intergovernamentais, tais como o Conselho da Europa[107], outros organismos regionais[108]; e organismos e agências da ONU (por ex., o Conselho dos Direitos Humanos da ONU[109] e o Comité dos Direitos Humanos[110]);
- relatórios e análises de redes reguladoras competentes, como a Assembleia Mundial da Privacidade (GPA)[111];
- jurisprudência nacional ou decisões adotadas por autoridades judiciais ou administrativas independentes competentes em matéria de privacidade e proteção de dados de países terceiros;
- relatórios de órgãos parlamentares ou de supervisão independentes;
- relatórios baseados na experiência prática com casos anteriores de pedidos de divulgação de autoridades públicas ou, na ausência de tais pedidos, de entidades ativas no mesmo setor que o importador;
- *Warrant canaries* de outras entidades que tratam dados no mesmo domínio que o importador;
- relatórios elaborados ou encomendados por câmaras de comércio, associações empresariais, profissionais e comerciais, agências governamentais diplomáticas, comerciais e de investimento do exportador ou de outros países terceiros que exportam para o país terceiro para o qual a transferência é efetuada;

---

[104] Ver ficha da jurisprudência do TEDH sobre vigilância em grande escala: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Ver Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] Acórdão Schrems II, n.º 141; ver decisões de adequação emhttps://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Ver, por exemplo, os relatórios nacionais da Comissão Interamericana de Direitos Humanos (CIDH), https://www.oas.org/en/iachr/reports/country.asp.

[109] Ver https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Ver: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Ver, por exemplo, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- relatórios de instituições académicas, e organizações da sociedade civil (por ex., ONG).
- relatórios de fornecedores privados de informações empresariais sobre os riscos financeiros, regulamentares e de reputação para as empresas;
- *Warrant canaries* do próprio importador[112];
- relatórios sobre a transparência, na condição de mencionarem expressamente o facto de não terem sido recebidos pedidos de acesso. Os relatórios sobre a transparência omissos sobre este aspeto não serão considerados elementos de prova suficientes, uma vez que estes relatórios se centram, na maior parte dos casos, nos pedidos de acesso recebidos das autoridades policiais e fornecem dados apenas sobre este aspeto, não se pronunciando sobre os pedidos de acesso recebidos para fins da segurança nacional. Tal não significa que não tenham sido recebidos pedidos de acesso, mas que estas informações não podem ser partilhadas[113];
- Declarações internas ou registos do importador que indiquem expressamente que não foram recebidos pedidos de acesso durante um período suficientemente longo; de preferência que incluam a assunção da responsabilidade pelo importador e/ou emitidos por cargos internos com alguma autonomia como auditores internos, encarregados da proteção de dados, etc.[114]

[112]Ver condições para a consideração da experiência prática documentada do importador com casos anteriores relevantes de pedidos de acesso recebidos de autoridades públicas do país terceiro no n.º 47.
[113] *Ibid.*
[114] *Ibid.*