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

Adotadas em 10 de novembro de 2020

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 C-311/18 (Schrems II), o Tribunal de Justiça da União Europeia (a seguir designado «TJUE») recorda-nos de que a proteção concedida aos dados pessoais no Espaço Económico Europeu (a seguir designado «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 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. O Tribunal mantém 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 declara que os responsáveis pelo tratamento dos dados ou os subcontratantes, agindo na capacidade de exportadores, são responsáveis por verificar, caso a caso e, sempre que adequado, em colaboração com o importador num país terceiro, se o direito ou as práticas do país terceiro afetam a eficiência das garantias adequadas constantes dos instrumentos de transferência do artigo 46.º do RGPD. Em tais casos, o Tribunal ainda deixa 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 não especifica quais as medidas possíveis. No entanto, o Tribunal sublinha que os exportadores terão de as identificar 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 tratem dados pessoais no âmbito de aplicação do RGPD) com a complexa tarefa de avaliar países terceiros e identificar medidas complementares adequadas sempre que necessário, o Comité Europeu para a Proteção de Dados (a seguir designado «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 aconselha-o (o utilizador, na capacidade de exportador) a **conhecer 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 lhes é concedido um nível de proteção essencialmente equivalente onde quer que estes sejam tratados. 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.

Numa **segunda** etapa, é necessário **verificar o instrumento de transferência no qual a sua transferência se baseia,** entre os enumerados no capítulo V do RGPD. Se a Comissão Europeia já declarou o país, a região ou o setor para o qual está a transferir os dados como adequado através de uma decisão de adequação ao abrigo do artigo 45.º do RGPD ou ao abrigo da anterior Diretiva 95/46 desde que a decisão esteja ainda em vigor, não é necessário adotar quaisquer medidas adicionais para além de monitorizar que a decisão de adequação permanece em vigor. Na ausência de uma decisão de adequação, é necessário recorrer a um dos instrumentos de transferência enumerados no artigo 46.º do RGPD para transferências regulares e recorrentes. Apenas poderá recorrer a uma das derrogações previstas no artigo 49.º do RGPD em alguns casos de transferências ocasionais e não recorrentes, caso cumpra as condições estipuladas.

Numa **terceira etapa**, deve **avaliar** se existe algo **no direito ou nas práticas do país terceiro** que possa afetar a eficiência das garantias adequadas dos instrumentos de transferência no qual se baseia, no contexto da transferência específica. A sua avaliação deve centrar-se principalmente na legislação de países terceiros pertinente para a sua transferência e no instrumento de transferência do artigo 46.º do RGPD no qual se baseia e que pode comprometer o seu nível de proteção. Para avaliar os elementos a ter em consideração aquando da avaliação da legislação de um país terceiro que gere o acesso aos dados pelas autoridades públicas para efeitos de vigilância, consulte as recomendações do CEPD sobre as garantias europeias indispensáveis. Nomeadamente, o que precede deve ser tido cuidadosamente em conta sempre que a legislação que rege o acesso aos dados pelas autoridades públicas é ambígua ou não está disponível ao público. Na ausência de legislação que rege as circunstâncias nas quais as autoridades públicas podem aceder aos dados pessoais, se ainda assim desejar prosseguir com a transferência, deve analisar outros fatores pertinentes e objetivos e não depender apenas de fatores subjetivos, tais como a probabilidade de acesso das autoridades públicas aos seus dados de um modo não conforme com as normas da UE. Deverá efetuar a avaliação com a devida diligência e documentá-la minuciosamente, uma vez que será responsabilizado por qualquer decisão que possa tomar com base em tal avaliação.

Numa **quarta etapa**, deve **identificar e adotar as medidas complementares** necessárias para aproximar o nível de proteção dos dados transferidos ao nível de equivalência essencial da UE. A etapa em causa apenas é necessária se a sua avaliação revelar que a legislação de um país terceiro interfere com a eficiência do instrumento de transferência do artigo 46.º do RGPD no qual se baseia, ou pretende basear, no contexto da sua 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 constantes dos instrumentos de transferência do artigo 46.º, algumas medidas complementares podem ser eficazes nuns países, mas não necessariamente noutros. O utilizador será responsável por avaliar a respetiva eficiência no contexto da transferência e à luz da lei do país terceiro e do instrumento de transferência no qual se baseia, e será responsabilizado pela decisão que tomar. Tal pode igualmente requerer a conjugação de diversas medidas complementares. Em última análise, pode descobrir que nenhuma medida complementar assegura um nível de proteção essencialmente equivalente à sua transferência específica. Nos casos em que nenhuma medida complementar é adequada, deve evitar, suspender ou pôr termo à transferência a fim de evitar comprometer o nível de proteção dos dados pessoais. O utilizador deve igualmente efetuar a referida avaliação de medidas complementares com a devida diligência e documentá-la.

Numa **quinta etapa**, deve **adotar** quaisquer **medidas processuais formais** que a adoção da sua medida complementar possa requerer, consoante o instrumento de transferência do artigo 46.º do RGPD no qual se baseia. As presentes recomendações especificam tais formalidades. Pode ser necessário consultar as autoridades de controlo competentes relativamente a algumas das referidas medidas.

Na **sexta e última etapa**, o utilizador deve 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 possa afetar. O princípio da responsabilidade exige um controlo contínuo do nível de proteção dos dados pessoais.

As autoridades de controlo continuarão a exercer o seu mandato para monitorizar a aplicação do RGPD e garantir a sua execução. As autoridades de controlo terão em devida consideração as medidas adotadas pelos exportadores a fim de assegurar que os dados transferidos têm um nível de proteção essencialmente equivalente. Conforme recorda o Tribunal, as autoridades de controlo suspenderão ou proibirão as transferências de dados sempre que, na sequência de uma investigação ou reclamação, considerarem que não pode ser garantido um nível de proteção essencialmente equivalente.

As autoridades de controlo continuarão a elaborar orientações para os exportadores e a coordenar as suas ações no CEPD, a fim de assegurar a coerência na aplicação do direito 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 designado «RGPD»),

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

Tendo em conta o artigo 12.º e o artigo 22.º do seu Regulamento Interno,

Considerando o seguinte:

(1) O Tribunal de Justiça da União Europeia (TJUE) conclui no seu Acórdão de 16 de julho de 2020 *Data Protection Commissioner contra Facebook Ireland LTD e Maximillian Schrems*, Processo C-311/18, que o artigo 46.º, n.os 1 e 2, alínea c), do RGPD deve ser interpretado no sentido de que as garantias adequadas, as vias de recurso legais eficazes e os direitos executórios exigidos pelas referidas disposições devem assegurar que os titulares dos dados cujos dados pessoais são transferidos para um país terceiro nos termos das cláusulas-tipo de proteção de dados beneficiam de um nível de proteção essencialmente equivalente ao garantido na União Europeia pelo regulamento em causa, tendo em consideração a Carta dos Direitos Fundamentais da União Europeia.[2]

(2) Tal como sublinhado pelo Tribunal, 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. Um 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 TJUE, de 16 de julho de 2020, *Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems,* [a seguir designado «C-311/18 (Schrems II)»], segunda constatação.
[3] C-311/18 (Schrems II), n.os 92 e 93.

(4) O Tribunal 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 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 afirmou que cabe sobretudo ao exportador de dados verificar, caso a caso e, se necessário, em colaboração com o importador dos dados, se a legislação do país terceiro de destino assegura um nível de proteção dos dados pessoais transferidos nos termos das cláusulas-tipo de proteção de dados essencialmente equivalente, ao abrigo da legislação da UE, prevendo medidas complementares às estipuladas em tais cláusulas, se necessário.[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 não define ou especifica as «garantias adicionais», «medidas adicionais» ou «medidas complementares» às garantias dos instrumentos de transferência ao abrigo do artigo 46.º, n.º 2, do RGPD que os responsáveis pelo tratamento e subcontratantes podem adotar a fim de 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 visam fornecer uma metodologia para os exportadores determinarem se teriam de ser aplicadas medidas adicionais para as suas transferências e quais seriam necessárias. Cabe aos exportadores a principal responsabilidade de assegurar que é atribuído aos dados transferidos um nível de proteção essencialmente equivalente ao garantido na UE no país terceiro em causa. O CEPD procura, com as presentes recomendações, incentivar a aplicação coerente do RGPD e do acórdão do Tribunal, em conformidade com o mandato do CEPD.[7]

ADOTOU A PRESENTE RECOMENDAÇÃO:

[4] C-311/18 (Schrems II), n.os 132 e 133.
[5] C-311/18 (Schrems II), n.º 134.
[6] C-311/18 (Schrems II), n.º 135.
[7] Artigo 70.º, n.º 1, alínea e), do RGPD.

1 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.

3. O direito à proteção de dados tem um carácter 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 subcontratantes devem igualmente poder demonstrar tais esforços aos titulares dos dados, ao público geral e às autoridades de controlo em matéria de proteção de dados. O que precede é o 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 uma forma de tratamento de dados.[14] Tal como sublinhado pelo Tribunal 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 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 proteção de dados e de suspender a transferência e/ou rescindir o contrato sempre que o importador dos dados não está, ou deixou 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

[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, preâmbulo, do RGPD.
[9] Artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da UE.
[10] Considerando 4 do RGPD e Processo C-507/17 Google LLC, sucessora da Google Inc., contra Commission nationale de l'informatique et des libertés (CNIL), 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 contra 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 artigo 47.º, n.º 2, alínea d), do RGPD.
[14] Acórdão do TJUE, de 6 de outubro de 2015, *Maximillian Schrems contra Data Protection Commissioner,* [a seguir designado «C-362/14 (Schrems I)»], n.º 45.
[15] C-311/18 (Schrems II), n.^{os} 92 e 93.
[16] C-311/18 (Schrems II), n.^{os} 134, 135, 139, 140, 141 e 142.

subcontratante, agindo como exportador, deve 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]

2 QUADRO DE REFERÊNCIA: APLICAÇÃO DO PRINCÍPIO DA RESPONSABILIDADE ÀS TRANSFERÊNCIAS DE DADOS NA PRÁTICA

6. O que se segue é um quadro de referência das medidas a adotar para saber se o utilizador (o exportador de dados) precisa de aplicar medidas complementares para transferir legalmente dados para fora do EEE. No presente documento, por «o utilizador» entende-se o responsável pelo tratamento ou o subcontratante que age como exportador de dados e trata dados pessoais no âmbito de aplicação do RGPD (incluindo o tratamento por entidades privadas e organismos públicos aquando da transferência de dados para entidades privadas).[19] No que respeita às transferências de dados pessoais efetuadas entre organismos públicos, estão previstas orientações específicas nas *Diretrizes 2/2020 sobre o artigo 46.º n.º 2, alínea a), e o artigo 46.º n.º 3, alínea b), do Regulamento 2016/679 no que concerne às transferências de dados pessoais entre autoridades e organismos públicos de países membros e não membros do EEE.*[20]

7. O utilizador terá de documentar adequadamente tal avaliação e as medidas complementares que selecionar e implementar e deve disponibilizar a documentação à autoridade de controlo competente, mediante pedido.[21]

2.1 Etapa 1: Conhecimento das suas transferências

8. Para saber o que lhe pode ser exigido (o exportador de dados) para poder continuar ou realizar novas transferências de dados pessoais[22], numa primeira etapa deve assegurar-se de que tem plena consciência das suas transferências (conheça as suas transferências). O levantamento e registo de todas as transferências pode ser um exercício complexo para as entidades envolvidas em múltiplas e diversas transferências regulares com países terceiros e que utilizam diversos subcontratantes e subcontratantes ulteriores. Conhecer as suas transferências é um primeiro passo essencial para cumprir as suas obrigações ao abrigo do princípio da responsabilidade.

[17] C-311/18 (Schrems II), n.º 134.
[18] Artigo 5.º, n.º 2, e artigo 28.º,n.º 3, alínea h), do RGPD.
[19] 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_pt
[20] Diretrizes 2/2020 do CEPD sobre o artigo 46.º n.º 2, alínea a), e o artigo 46.º n.º 3, alínea b), do Regulamento 2016/679 no que concerne às transferências de dados pessoais entre autoridades e organismos públicos de países membros e não membros do EEE; ver https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_pt
[21] Artigo 5.º, n.º 2, e artigo 24.º, n.º 1, do RGPD.
[22] É de salientar que o acesso remoto por uma entidade de um país terceiro aos dados localizados no EEE é igualmente considerado uma transferência.

9. Para obter conhecimento completo das suas transferências, o utilizador poderá basear-se nos registos de atividades de tratamento que poderá ser obrigado a manter enquanto responsável pelo tratamento ou subcontratante ao abrigo do artigo 30.º do RGPD.[23] Podem ser igualmente úteis as ações passadas com vista ao 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 suas transferências dos dados pessoais dos referidos titulares de dados para países terceiros.[24]

10. Aquando do levantamento das transferências, o utilizador deve igualmente ter em consideração as transferências posteriores, por exemplo, se os seus subcontratantes fora do EEE transferem os dados pessoais a estes confiados para um subcontratante ulterior noutro país terceiro ou no mesmo país terceiro[25]

11. Em consonância com o princípio da «minimização dos dados»,[26] o utilizador 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.

12. Tais 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 utilizador deve saber onde podem estar localizados os dados pessoais exportados ou onde podem ser tratados pelos importadores (mapa de destinos).

13. É preciso ter em mente 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.[27] Mais especificamente, se o utilizador estiver a utilizar uma infraestrutura de nuvem internacional, deve avaliar se os dados serão transferidos para países terceiros e para onde serão transferidos, salvo indicação clara no contrato de que o prestador de serviços na nuvem não irá tratar os dados em países terceiros.

[23] Ver artigo 30.º do RGPD e, nomeadamente, n.os 1, alínea e), e 2, alínea c). Além disso, os seus registos de tratamento devem conter uma descrição das atividades de tratamento (incluindo, sem carácter limitativo, as categorias de titulares dos dados, as categorias de dados pessoais, as finalidades do tratamento e as informações específicas sobre 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 Grupo de Trabalho do Artigo 29.º, 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 (aprovado pelo CEPD em 25 de maio de 2018).

[24] Ao abrigo das regras de transparência do RGPD, o utilizador 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]. Nomeadamente, deve informar os titulares dos dados da existência ou ausência 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, a referência às garantias adequadas ou apropriadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. As informações prestadas ao titular dos dados devem ser corretas e atuais, especialmente à luz da jurisprudência do Tribunal em matéria de transferências.

[25] Sempre que o responsável pelo tratamento tiver concedido autorização prévia específica ou geral, por escrito, em conformidade com o artigo 28.º, n.º 2, do RGPD.

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

[27] Ver pergunta frequente (FAQ) 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 e Maximillian Schrems, de 23 de julho de 2020.

2.2 Etapa 2: Identificação dos instrumentos de transferência nos quais se baseia

14. Numa segunda etapa deve identificar os instrumentos de transferência nos quais se baseia, de entre os previstos e enumerados no capítulo V do RGPD.

Decisões de adequação

15. A Comissão Europeia pode reconhecer mediante as respetivas **decisões de adequação** relativas a alguns ou todos os países terceiros para os quais está a transferir dados pessoais que estes oferecem um nível adequado de proteção dos dados pessoais.[28]

16. Tal decisão de adequação permite que os dados pessoais sejam transferidos do EEE para o país terceiro em causa sem que seja necessário qualquer 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).[29]

18. A Comissão Europeia publica a lista de decisões de adequação no respetivo sítio web.[30]

19. Se o utilizador transferir dados pessoais para países terceiros, regiões ou setores abrangidos por uma decisão de adequação da Comissão (na medida em que seja aplicável), **não precisa de adotar quaisquer medidas adicionais, conforme descrito nas presentes recomendações.**[31] No entanto, deve ainda assim verificar se as decisões de adequação pertinentes às suas transferências são revogadas ou invalidadas.[32]

20. Contudo, as decisões de adequação não impedem os titulares dos dados de apresentar uma reclamação. Estas também não impedem as autoridades de controlo de apresentar um processo perante um tribunal nacional, caso tenham dúvidas quanto à validade de uma decisão, para que um tribunal nacional possa apresentar um pedido de decisão prejudicial ao TJUE para efeitos da avaliação de tal validade.[33]

---

[28] 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. Do mesmo modo, a Comissão Europeia tem autoridade para determinar que uma organização internacional oferece um nível adequado de proteção.

[29] Artigo 45.º, n.º 1, do RGPD.

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

[31] Desde de o utilizador e o importador de dados implementarem medidas para cumprir as restantes obrigações ao abrigo do RGPD; caso contrário, devem implementar as referidas medidas.

[32] 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). Além disso, o TJUE pode invalidar decisões de adequação [ver Acórdãos nos Processos C-362/14 (Schrems I) e C-311/18 (Schrems II)].

[33] C-311/18 (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; não existe base jurídica que fundamente validamente o tratamento de dados como tal, em violação do artigo 6.º do RGPD). As autoridades de controlo podem avaliar, com total independência, se a transferência dos dados cumpre os requisitos estabelecidos pelo RGPD e, sempre que pertinente, intentar uma ação junto dos tribunais nacionais para que estes, caso tenham dúvidas quanto à validade da decisão de

Exemplo: Um cidadão da UE, Sr. 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 Facebook Ireland de transferir os 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 (TJUE). Subsequentemente, o TJUE decidiu invalidar a Decisão 2000/520/CE da Comissão relativa ao nível de proteção assegurado pelos princípios de «porto seguro».[34]

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:

- cláusulas-tipo de proteção de dados,
- regras vinculativas aplicáveis às empresas,
- códigos de conduta,
- procedimentos de certificação,
- cláusulas contratuais *ad hoc*.

22. Independentemente do instrumento de transferência do artigo 46.º do RGPD que selecionar, o utilizador deve assegurar-se de que, em termos gerais, os dados pessoais transferidos têm 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 às transferências para todos os países terceiros. A situação no país terceiro para o qual o utilizador transfere dados pode ainda requerer que complemente os referidos instrumentos de transferência e as garantias nestes contidas com medidas adicionais («medidas complementares») para assegurar um nível de proteção essencialmente equivalente.[35]

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. Sujeito a condições específicas, o utilizador pode ainda transferir dados pessoais com base numa derrogação estipulada no artigo 49.º do RGPD.

adequação da Comissão, apresentem um pedido de decisão prejudicial ao Tribunal de Justiça da União Europeia para efeitos da avaliação da sua validade.

[34] Processo C-362/14 (Schrems I).

[35] C-311/18 (Schrems II), n.^{os} 130 e 133. Ver também ponto 2.3 infra.

25. O artigo 49.º do RGPD tem carácter excecional. As derrogações neste contidas devem ser interpretadas de forma restritiva, sendo aplicáveis, principalmente, a atividades de tratamento ocasionais e não repetitivas. O CEPD emitiu as Diretrizes 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679. [36]

26. Antes de recorrer a uma derrogação do artigo 49.º do RGPD, o utilizador deve verificar se as suas transferências cumprem as rigorosas condições que a referida disposição estabelece para cada uma.

***

27. Se a sua transferência não puder ter uma derrogação do artigo 49.º ou uma decisão de adequação como base jurídica, terá de prosseguir para a etapa 3.

2.3 Etapa 3: Avaliação da eficiência do instrumento de transferência do artigo 46.º do RGPD no qual se baseia face a todas as circunstâncias da transferência

28. É possível que a seleção de um instrumento de transferência do artigo 46.º do RGPD não seja suficiente. O instrumento de transferência deve assegurar que o nível de proteção garantido pelo RGPD não é comprometido pela transferência.[37] Por outras palavras, o instrumento de transferência escolhido deve ser eficaz na prática.

29. Por eficaz entende-se que os dados pessoais transferidos têm um nível de proteção no país terceiro que é essencialmente equivalente ao que é garantido no EEE.[38] 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.

30. Por conseguinte, o utilizador deve, se necessário em colaboração com o importador, avaliar se existe algo no direito ou na prática do país terceiro que possa afetar a eficiência das garantias adequadas do instrumento de transferência do artigo 46.º do RGPD no qual se baseia, no contexto da transferência específica. Sempre que adequado, o importador de dados deve fornecer ao utilizador as fontes e informações pertinentes relacionadas com o país terceiro no qual se encontra estabelecido e as leis aplicáveis à transferência. Pode também consultar outras fontes de informação, tais como as enumeradas de forma não exaustiva no anexo 3.[39]

31. A avaliação do utilizador 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 mais responsáveis pelo tratamento, subcontratantes ou importadores estiverem envolvidos, mais complexa será a sua avaliação. Deve igualmente ter em consideração na referida avaliação qualquer possível posterior transferência.

32. Para tal, o utilizador terá de analisar as características de cada uma das suas transferências e determinar de que modo o ordenamento jurídico nacional do país para o qual os dados são transferidos (ou transferidos posteriormente) se aplica às transferências em causa.

---

[36] Para mais informações, ver https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_pt.
[37] Artigo 44.º do RGPD.
[38] C-311/18 (Schrems II), n.º 105 e segunda constatação.
[39] Ver igualmente o n.º 43 do presente documento infra.

33. O contexto jurídico aplicável dependerá das circunstâncias da transferência, nomeadamente:

- Finalidades para as quais os dados são transferidos e tratados (por exemplo, marketing, RH, armazenamento, apoio informático, ensaios clínicos),
- Tipos de entidades envolvidas no tratamento (pública/privada; responsável pelo tratamento/subcontratante),
- Setor no qual a transferência ocorre (por exemplo, tecnologia de publicidade, telecomunicações, financeiro, etc.),
- Categorias de dados pessoais transferidos (por exemplo, dados pessoais relativos a crianças podem ser abrangidos pelo âmbito de legislação específica do país terceiro),
- Se os dados serão armazenados no país terceiro ou se existe apenas acesso remoto aos dados armazenados na UE ou no EEE,
- Formato dos dados a transferir (ou seja, em texto simples/pseudonimizado ou encriptado[40]),
- Possibilidade da ocorrência de transferências posteriores dos dados do país terceiro em causa para outro país terceiro.[41]

34. Entre as leis aplicáveis, o utilizador terá de avaliar se existe alguma que afetará os compromissos constantes do instrumento de transferência do artigo 46.º do RGPD que tenha escolhido. Deve verificar se os compromissos que permitem aos titulares dos dados exercer os seus direitos no contexto de transferências internacionais (tais como pedidos de acesso, retificação e apagamento de dados transferidos) podem ser aplicados de forma eficaz na prática e não são comprometidos pela legislação do país terceiro de destino.

35. O utilizador terá de avaliar as regras de natureza geral pertinentes na medida em que tenham impacto na aplicação eficaz das garantias constantes do instrumento de transferência do artigo 46.º do RGPD e dos direitos fundamentais das pessoas (nomeadamente, o direito de recurso concedido aos titulares de dados em caso de acesso aos dados transferidos por parte de autoridades públicas de países terceiros).

36. Em qualquer caso, o utilizador deve prestar atenção a quaisquer leis pertinentes, nomeadamente, 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 e segurança nacional). Se os referidos requisitos ou poderes forem limitados ao que é necessário e proporcionado numa sociedade democrática,[42] estes não podem afetar os compromissos constantes do instrumento de transferência do artigo 46.º do RGPD no qual se baseia.

37. 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 para avaliar se tal 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.

---

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

[41] Sempre que o responsável pelo tratamento tiver concedido autorização prévia específica ou geral, por escrito, em conformidade com o artigo 28.º, n.º 2, do RGPD.

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

38. 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.[43] Por exemplo, a situação do Estado de direito num país terceiro pode ser pertinente para a avaliação da eficiência dos mecanismos disponíveis para as pessoas beneficiarem de vias de recurso (judicial) contra o acesso ilícito do Governo aos 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, pode contribuir para assegurar a proporcionalidade da interferência por parte dos governos.[44]

***

39. As recomendações do CEPD sobre as garantias europeias indispensáveis preveem os elementos que têm de ser avaliados por forma a determinar se o quadro jurídico que rege o acesso aos dados pessoais por parte das autoridades públicas de um país terceiro (sejam estas agências de segurança nacional ou autoridades responsáveis pela aplicação da lei) pode ou não ser considerado uma interferência justificável (e, por conseguinte, não afeta os compromissos assumidos no instrumento de transferência do artigo 46.º do RGPD). Nomeadamente, o que precede deve ser tido cuidadosamente em conta sempre que a legislação que rege o acesso aos dados pelas autoridades públicas é ambígua ou não está disponível ao público.

40. 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 indispensáveis podem ajudar o exportador e o importador de dados na avaliação da interferência injustificada de tais poderes com as obrigações do importador de dados para assegurar a equivalência essencial.

41. A ausência de um nível de proteção essencialmente equivalente será especialmente evidente quando o direito ou as práticas do país terceiro pertinente para a transferência do utilizador não cumprir os requisitos das garantias europeias indispensáveis.

42. A avaliação do utilizador deve basear-se primeiramente na legislação disponível ao público. No entanto, em algumas situações tal não será suficiente, porque a legislação dos países terceiros pode ter lacunas. Neste caso, se ainda assim desejar realizar a transferência, deve analisar outros fatores pertinentes e objetivos[45] e não depender apenas de fatores subjetivos, tais como a probabilidade de acesso por parte das autoridades públicas aos seus dados de um modo não conforme com as normas da UE. Deverá efetuar a avaliação com a devida diligência e documentá-la minuciosamente, uma vez que será responsabilizado por qualquer decisão que possa tomar com base em tal avaliação.[46]

[43] C-311/18 (Schrems II), n.º 104.
[44] Por exemplo: A Convenção n.º 108 (Convenção para a proteção dos indivíduos relativamente ao tratamento automatizado de dados de carácter pessoal, STE n.º 108) ou a Convenção n.º 108+ (Atualização da Convenção para a proteção dos indivíduos relativamente ao tratamento de dados de carácter pessoal, STCE n.º 223) prevê vias de recurso judiciais internacionais exequíveis em caso de violações da proteção de dados e contribui para proporcionar um nível mínimo de proteção de dados pessoais e de respeito pela vida privada.
[45] Ver o n.º 43 do presente documento infra, bem como o anexo 3.
[46] Artigo 5.º, n.º 2, do RGPD.

43. O utilizador pode finalizar a sua avaliação com informações obtidas de outras fontes[47], tais como:

- elementos que demonstram que uma autoridade de um país terceiro tentará aceder aos dados com ou sem o conhecimento do importador de dados, à luz da legislação, das práticas e dos precedentes relatados,
- elementos que demonstram que uma autoridade de um país terceiro poderá aceder aos dados através do importador de dados ou através da interceção direta do canal de comunicação, à luz dos precedentes relatados, das competências jurídicas e dos recursos técnicos, financeiros e humanos à sua disposição.

44. Em última análise, a avaliação pode demonstrar que o instrumento de transferência do artigo 46.º do RGPD no qual se baseia e as garantias adequadas neste contidas:

- asseguram de modo eficaz que os dados pessoais transferidos têm um nível de proteção no país terceiro essencialmente equivalente ao garantido no EEE. O direito e as práticas do país terceiro aplicáveis à transferência colocam o importador de dados em condições de cumprir as suas obrigações ao abrigo do instrumento de transferência escolhido. O utilizador deve realizar uma reavaliação da situação com a periodicidade adequada ou sempre que surgirem alterações significativas (ver etapa 6),
- não asseguram de modo eficaz um nível de proteção essencialmente equivalente. O importador de dados não pode cumprir as suas obrigações, devido à legislação e/ou às práticas do país terceiro aplicáveis à transferência. O TJUE sublinhou que nos casos em que os instrumentos de transferência do artigo 46.º do RGPD não são suficientes, é da responsabilidade do exportador de dados adotar medidas complementares eficazes ou não transferir dados pessoais.[48]

O TJUE considerou, por exemplo, que o artigo 702.º da Lei de Vigilância de Informações Externas dos Estados Unidos (FISA) não cumpre as garantias mínimas resultantes do princípio da proporcionalidade ao abrigo da legislação da UE e não pode ser considerada como limitada ao estritamente necessário. O que precede significa que o nível de proteção dos programas autorizados pelo artigo 702.º da FISA não é essencialmente equivalente às garantias exigidas pela legislação da UE. Consequentemente, se o importador de dados ou qualquer futuro destinatário ao qual o importador pode divulgar os dados estiver abrangido pelo artigo 702.º da FISA[49], as cláusulas contratuais-tipo ou outro instrumento de transferência do artigo 46.º do RGPD apenas são fiáveis para tais transferências caso medidas técnicas complementares adicionais impossibilitem o acesso aos dados transferidos, ou o tornem ineficaz.

[47] Ver também o anexo 3.

[48] TJUE, C-311/18 (Schrems II), n.os 134 e 135.

[49] O artigo 702.º da FISA é aplicável se os dados forem obtidos «de ou com assistência de um prestador de serviços de comunicações eletrónicas» [artigo 702.º da FISA = artigo 1881.º-A, parte h, ponto 2, alínea A), subalínea vi), do título 50 do USC], que por sua vez é definido no artigo 1881.º, parte b, ponto 4, do título 50 do USC como:
«A) um prestador de serviços de telecomunicações, na aceção do artigo 153.º do título 47;
B) um prestador de serviços de comunicações eletrónicas, na aceção do artigo 2510.º do título 18;
C) um prestador de serviços de informática remotos, na aceção do artigo 2711.º do título 18;

2.4 Etapa 4: Adoção de medidas complementares

45. Se a avaliação do utilizador no âmbito da etapa 3 revelou que o instrumento de transferência do artigo 46.º do RGPD escolhido não é eficaz, terá de considerar, se necessário em colaboração com o importador, se existem medidas complementares que em combinação com as garantias constantes dos instrumentos de transferência poderiam assegurar que os dados transferidos têm um nível de proteção essencialmente equivalente no país terceiro ao que é garantido na UE.[50] As «medidas complementares» são, por definição, complementares às garantias previstas pelo instrumento de transferência do artigo 46.º do RGPD.[51]

46. O utilizador deve identificar caso a caso quais as medidas complementares que podem ser eficazes para um conjunto de transferências para um país terceiro específico aquando da utilização de um instrumento de transferência específico do artigo 46.º do RGPD. Poderá basear-se nas suas avaliações anteriores ao abrigo das etapas 1, 2 e 3 supra e verificar mediante a comparação com as conclusões a potencial eficiência das medidas complementares para garantir o nível de proteção exigido.

47. Em princípio, as medidas complementares podem ter um carácter contratual, técnico ou organizativo. A combinação de diversas medidas de um modo que estas se desenvolvam e apoiem mutuamente pode aumentar o nível de proteção e, por conseguinte, contribuir para o cumprimento das normas da UE.

48. Normalmente, as medidas contratuais e organizativas por si só não irão ultrapassar o acesso aos dados pessoais por parte das autoridades públicas do país terceiro (sempre que tal interfira injustificadamente com as obrigações do importador de dados de assegurar a equivalência essencial). Haverá efetivamente situações em que apenas medidas técnicas podem impedir ou tornar ineficaz o acesso das autoridades públicas de países terceiros aos dados pessoais, nomeadamente para fins de vigilância.[52] Em tais situações, determinadas medidas contratuais ou organizativas podem complementar as medidas técnicas e reforçar o nível geral de proteção de dados, por exemplo, mediante a criação de obstáculos às tentativas de acesso aos dados por parte das autoridades públicas de um modo não conforme com as normas da UE.

49. O utilizador pode, se necessário em colaboração com o importador de dados, consultar a seguinte lista (não exaustiva) de fatores para identificar que medidas complementares seriam mais eficazes na proteção dos dados transferidos:

- Formato dos dados a transferir (ou seja, em texto simples/pseudonimizado ou encriptado),
- Natureza dos dados,
- Duração e complexidade do fluxo de tratamento de dados, número de intervenientes envolvidos no tratamento e relação entre os mesmos [por exemplo, as transferências

D) qualquer outro prestador de serviços de comunicação que tenha acesso a comunicações eletrónicas ou a cabo, quer à medida que tais comunicações são transmitidas, quer à medida que tais comunicações são armazenadas; ou
E) um responsável, funcionário ou agente de uma entidade descrita na alínea A), B), C) ou D).»

[50] C-311/18 (Schrems II), n.º 96.

[51] Considerando 109 do RGPD e C-311/18 (Schrems II), n.º 133.

[52] 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 do CEPD 02/2020 sobre as garantias europeias indispensáveis para medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_pt .

envolvem vários responsáveis pelo tratamento ou responsáveis pelo tratamento de dados e subcontratantes, ou envolvem subcontratantes que transferirão os dados do utilizador para o importador de dados do utilizador (considerando as disposições pertinentes que lhes são aplicáveis ao abrigo da legislação do país terceiro de destino)],[53]

- Possibilidade da ocorrência de transferências posteriores dos dados, quer seja dentro do mesmo país terceiro ou para outros países terceiros (por exemplo, envolvimento de subcontratantes ulteriores do importador de dados).[54]

Exemplos de medidas complementares

50. Alguns exemplos de medidas técnicas, contratuais e organizativas que podem ser consideradas constam das listas não exaustivas do anexo 2.

***

51. Se o utilizador 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, as suas transferências podem continuar a ser realizadas.

52. Caso não consiga encontrar ou implementar medidas complementares eficazes que assegurem que os dados pessoais transferidos têm um nível de proteção essencialmente equivalente,[55] não deve iniciar qualquer transferência de dados pessoais para o país terceiro em causa com base no instrumento de transferência do artigo 46.º do RGPD no qual se baseia. Se o utilizador já iniciou as transferências de dados pessoais, é obrigado a suspender ou pôr termo às mesmas.[56] Nos termos das garantias constantes do instrumento de transferência do artigo 46.º do RGPD no qual se baseia, os dados já transferidos para o país terceiro em causa devem ser devolvidos ao utilizador ou destruídos na sua totalidade pelo importador, bem como as respetivas cópias.[57]

Exemplo: o direito do país terceiro proíbe as medidas complementares que o utilizador identificou (por exemplo, proíbe a utilização de encriptação) ou impede de outro modo a sua eficiência. O utilizador não deve iniciar qualquer transferência de dados pessoais para o país em causa ou deve interromper as transferências existentes para o mesmo.

[53] 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.

[54] Ver nota de rodapé 25.

[55] 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 do CEPD 02/2020 sobre as garantias europeias indispensáveis para medidas de vigilância, de 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_pt .

[56] C-311/18 (Schrems II), n.º 135.

[57] Ver cláusula 12 do anexo da Decisão CCT 2010/87/UE; ver a cláusula adicional de resolução (opcional) constante do anexo B da Decisão CCT 2004/915/CE .

53. Se decidir prosseguir com a transferência não obstante o facto de o importador não poder cumprir os compromissos assumidos no instrumento de transferência do artigo 46.º do RGPD, deve notificar a autoridade de controlo competente em conformidade com as disposições específicas do instrumento de transferência do artigo 46.º do RGPD pertinente.[58] 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.[59]

54. A autoridade de controlo competente pode impor quaisquer outras medidas corretivas (por exemplo, uma coima), se, apesar de não ser capaz de demonstrar um nível de proteção essencialmente equivalente no país terceiro, o utilizador iniciar ou continuar a transferência.

2.5 Etapa 5: Medidas processuais no caso da identificação de medidas complementares eficazes

55. As medidas processuais que o utilizador pode ter de tomar caso tenha identificado medidas complementares eficazes a adotar podem ser diferentes consoante o instrumento de transferência do artigo 46.º do RGPD que está a utilizar ou que prevê utilizar.

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

56. Sempre que pretende aplicar medidas complementares para além das cláusulas contratuais-tipo, não é necessário solicitar uma autorização à autoridade de controlo competente para acrescentar 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.[60] O exportador e o importador de dados têm de assegurar que as cláusulas adicionais não podem ser interpretadas de modo a restringir os direitos e obrigações constantes das cláusulas contratuais-tipo ou de qualquer outro modo reduzir o nível de proteção de dados. O utilizador deve conseguir demonstrar o que precede, incluindo a inequivocidade de todas as cláusulas, em conformidade com o princípio da responsabilidade e a sua obrigação de providenciar um nível suficiente de proteção de dados. As autoridades de controlo competentes têm o poder de rever as referidas cláusulas complementares sempre que necessário (por exemplo, em caso de queixa ou de inquérito iniciado por vontade própria).

[58] Ver as perguntas frequentes (FAQ) do CEPD sobre o acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – Data Protection Commissioner contra Facebook Ireland Limited e Maximillian Schrems, adotado em 23 de julho de 2020, e, nomeadamente, as perguntas 5, 6 e 9. Ver igualmente a cláusula 4, alínea g), da Decisão 2010/87/UE da Comissão; a cláusula 5, alínea a), da Decisão 2001/497/CE da Comissão e o anexo, conjunto II, cláusula II, alínea c), Decisão 2004/915/CE da Comissão.

[59] C-311/18 (Schrems II), n.os 113 e 121.

[60] 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». Determinados conjuntos de cláusulas contratuais-tipo adotadas pela Comissão Europeia ao abrigo da Diretiva 95/45/CE contêm disposições semelhantes.

57. Se pretender alterar as próprias cláusulas-tipo de proteção de dados ou se as medidas complementares acrescentadas «contradizem», direta ou indiretamente, as cláusulas contratuais-tipo, deixa de se considerar que o utilizador se baseia em cláusulas-tipo contratuais[61] e deve solicitar uma autorização junto da autoridade de controlo competente, nos termos do artigo 46.º, n.º 3, alínea a), do RGPD.

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

58. O raciocínio apresentado pelo Acórdão Schrems II aplica-se igualmente a outros instrumentos de transferência nos termos 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 não podem vincular autoridades públicas de países terceiros.[62]

59. 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 assegurada por tais instrumentos. O impacto exato do Acórdão Schrems II nas regras vinculativas aplicáveis às empresas continua a ser debatido. O CEPD deve disponibilizar mais informações assim que possível relativamente à eventual necessidade de incluir quaisquer compromissos adicionais nas regras vinculativas aplicáveis às empresas nas referências dos WP256 e WP257.[63]

60. O Tribunal salientou que é da responsabilidade do exportador e do 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 esse o caso, o utilizador 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 as práticas do país terceiro não vão interferir com tais medidas complementares de forma que possa impedir a sua eficiência.

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

61. 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 não podem vincular autoridades públicas de países terceiros.[64] Por conseguinte, o Acórdão Schrems II é pertinente para as transferências de dados pessoais com base nas cláusulas

[61] Ver, por analogia, o Parecer 17/2020 do CEPD sobre o projeto de cláusulas contratuais tipo apresentado pela 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.

[62] TJUE, C-311/18 (Schrems II), n.º 132.

[63] Grupo de Trabalho do Artigo 29.º, Documento de Trabalho que estabelece um quadro com os elementos e princípios constantes das regras vinculativas aplicáveis às empresas, com a última redação que lhe foi dada e conforme adotado em 6 de fevereiro de 2018 (WP 256 rev.01); Grupo de Trabalho do Artigo 29.º, Documento de Trabalho que estabelece um quadro com os elementos e princípios constantes das regras vinculativas aplicáveis às empresas, com a última redação que lhe foi dada e conforme adotado em 6 de fevereiro de 2018 (WP 257 rev.01).

[64] TJUE, C-311/18 (Schrems II), n.º 132.

contratuais *ad hoc*, uma vez que as leis de países terceiros podem afetar a proteção assegurada por tais instrumentos. O impacto exato do Acórdão Schrems II nas cláusulas contratuais ad hoc continua a ser debatido. O CEPD irá prestar mais informações assim que possível.

2.6 Etapa 6: Reavaliação com a periodicidade adequada

62. O utilizador deve acompanhar, de forma contínua 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 possa ter tomado no contexto das suas transferências. A responsabilidade é uma obrigação contínua (artigo 5.º, n.º 2, do RGPD).

63. O utilizador deve implementar mecanismos suficientemente seguros para assegurar a suspensão ou o termo imediato 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.

3 CONCLUSÃO

64. O RGPD estabelece regras relativas ao tratamento de dados pessoais no EEE e, ao fazê-lo, permite 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 do TJUE C-311/18 (Schrems II) sublinha a necessidade de assegurar a continuidade do nível de proteção concedido aos dados pessoais transferidos para um país terceiro ao abrigo do RGPD.[65]

65. Para assegurar um nível de proteção dos seus dados essencialmente equivalente, o utilizador deve primeiramente ter um conhecimento minucioso das suas transferências. 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.

66. É igualmente necessário identificar o instrumento de transferência no qual se baseia para as suas transferências. Se o instrumento de transferência não for uma decisão de adequação, deve verificar, caso a caso, se o direito ou as práticas do país terceiro de destino comprometem (ou não) as garantias constantes do instrumento de transferência do artigo 46.º do RGPD no contexto das suas transferências. Nos casos em que o instrumento de transferência do artigo 46.º do RGPD por si só não consegue assegurar um nível de proteção essencialmente equivalente aos dados pessoais transferidos, as medidas complementares podem colmatar a lacuna.

67. Caso o utilizador não consiga encontrar ou implementar medidas complementares eficazes que assegurem que os dados pessoais transferidos têm de um nível de proteção essencialmente equivalente, não deve iniciar qualquer transferência de dados pessoais para o país terceiro em causa com base no instrumento de transferência escolhido. Se o utilizador já iniciou as transferências de dados pessoais, é obrigado a suspender ou pôr termo às mesmas de imediato.

68. A autoridade de controlo competente tem o poder de suspender ou pôr termo às transferências de dados pessoais para o país terceiro caso a proteção dos dados transferidos exigida pela legislação da UE não seja assegurada, nomeadamente, artigos 45.º e 46.º do RGPD e a Carta dos Direitos Fundamentais.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

[65] C-311/18 (Schrems II), n.º 93.

ANEXO 1: DEFINIÇÕES

- Por «país terceiro» entende-se qualquer país que não é um Estado-Membro do EEE.
- Por «EEE» entende-se o Espaço Económico Europeu e inclui os Estados-Membros da União Europeia, a Islândia, a Noruega e o Listenstaine. O RGPD é aplicável aos últimos em virtude do Acordo EEE, nomeadamente, o respetivo anexo XI e protocolo 37.
- Por «RGPD» entende-se 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).
- Por «Carta» entende-se a Carta dos Direitos Fundamentais da União Europeia (JO C 326 de 26.10.2012, p. 391–407).
- Por «TJUE» ou «Tribunal» entende-se o Tribunal de Justiça da União Europeia. Este constitui a autoridade judicial da União Europeia e, em cooperação com os tribunais dos Estados-Membros, assegura a aplicação e interpretação uniformes da legislação da UE.
- Por «exportador de dados» entende-se o responsável pelo tratamento ou subcontratante no EEE que transfere dados pessoais a um responsável pelo tratamento ou subcontratante de um país terceiro.
- Por «importador de dados» entende-se um responsável pelo tratamento ou subcontratante num país terceiro que recebe ou obtém acesso a dados pessoais transferidos do EEE.
- Por «instrumentos de transferência do artigo 46.º do RGPD» entende-se as garantias adequadas ao abrigo do artigo 46.º do RGPD que os exportadores de dados devem implementar sempre que transferem dados pessoais para um país terceiro, na ausência 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.
- Por «cláusulas contratuais-tipo» entende-se 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 são instrumentos de transferência ao abrigo do RGPD, conforme estipulado no artigo 46.º, n.º 2, alínea c), e n.º 5, do RGPD.

ANEXO 2: EXEMPLOS DE MEDIDAS COMPLEMENTARES

69. As medidas que seguem são exemplos de medidas complementares que o utilizador deve ter em consideração na etapa 4 «Adoção de medidas complementares». A presente lista não é exaustiva. A seleção e implementação de uma ou várias das referidas medidas não irão necessária e sistematicamente assegurar que a sua transferência cumpre a norma de equivalência essencial requerida pela legislação da UE. O utilizador deve selecionar medidas complementares que garantam efetivamente tal nível de proteção às suas transferências.

70. Qualquer medida complementar apenas pode ser considerada eficaz na aceção do Acórdão do TJUE «Schrems II» se e na medida em que colmatar as deficiências específicas identificadas na sua avaliação da situação jurídica do país terceiro. Se, em última análise, não for possível assegurar um nível de proteção essencialmente equivalente, não deve transferir os dados pessoais.

71. Na capacidade de responsável pelo tratamento ou subcontratante, é possível que o utilizador tenha de implementar algumas das medidas descritas no presente anexo, mesmo que o respetivo importador de dados esteja abrangido por uma decisão de adequação. É igualmente possível que tenha de as implementar aquando do tratamento de dados no EEE.[66]

Medidas técnicas

72. A presente secção descreve de forma não exaustiva exemplos de medidas técnicas, que podem complementar as garantias constantes dos 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. As medidas em causa 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 por parte das autoridades públicas de tal país terceiro.[67]

73. Para efeitos de clareza, a presente secção especifica primeiro as medidas técnicas que podem ser potencialmente eficazes em determinados cenários/casos de utilização para assegurar um nível de proteção essencialmente equivalente. A secção inclui ainda alguns cenários/casos de utilização nos quais não foi possível encontrar medidas técnicas para assegurar tal nível de proteção.

Cenários nos quais é possível encontrar medidas *eficazes*

74. As medidas indicadas infra 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 constantes dos instrumentos de transferência do artigo 46.º do RGPD. As referidas medidas são aplicáveis mesmo que o acesso das autoridades públicas cumpra a legislação do país do importador, sempre que tal acesso vá além do necessário e proporcionado numa sociedade democrática.[68] Tais medidas visam impedir o acesso potencialmente ilícito, impedindo as autoridades de identificar os titulares dos dados, inferir

[66] Artigo 5.º, n.º 2, e artigo 32.º, do RGPD.
[67] C-311/18 (Schrems II), n.º 135.
[68] Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações do CEPD sobre as garantias europeias indispensáveis no que concerne a medidas de vigilância.

informações a seu respeito, distingui-los noutro contexto ou associar os dados transferidos a outros conjuntos de dados que possam estar em sua posse e que possam conter, entre outros dados, identificadores em linha fornecidos pelos dispositivos, aplicações, ferramentas e protocolos utilizados pelos titulares dos dados noutros contextos.

75. As autoridades públicas de países terceiros podem procurar aceder aos dados transferidos:

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

b) quando na posse de um destinatário previsto dos dados, mediante o acesso às próprias instalações de tratamento ou mediante solicitação ao destinatário dos dados para localizar e recolher dados de interesse e apresentá-los às autoridades.

76. A presente secção inclui 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.

77. Os cenários descrevem circunstâncias específicas e as medidas adotadas. Quaisquer alterações aos cenários podem dar origem a diferentes conclusões.

78. Os responsáveis pelo tratamento podem ter de aplicar algumas ou todas as medidas descritas na presente secção, independentemente do nível de proteção previsto pelas leis aplicáveis ao importador de dados, uma vez que são necessárias para cumprir os artigos 25.º e 32.º do RGPD nas circunstâncias específicas da transferência. Por outras palavras, é possível que os exportadores tenham de implementar as medidas descritas no presente diploma, mesmo que os respetivos importadores de dados estejam abrangidos por uma decisão de adequação. É igualmente possível que os responsáveis pelo tratamento e os subcontratantes tenham de as implementar aquando do tratamento de dados no EEE.

Caso de utilização 1: Armazenamento de dados para cópias de segurança e outros fins que não requerem acesso aos dados não encriptados

79. Um exportador de dados utiliza um prestador de serviços de alojamento num país terceiro para armazenar dados pessoais, por exemplo, para efetuar cópias de segurança.

Se:

1. os dados pessoais forem tratados usando uma forte encriptação antes da transmissão;

2. o algoritmo de encriptação e a respetiva parametrização (por exemplo, comprimento da chave, modo de funcionamento, se aplicável) estiverem em conformidade com o estado da arte e poderem ser considerados robustos contra a criptoanálise realizada pelas autoridades públicas do país de destino, tendo em conta os recursos e as capacidades técnicas (por exemplo, poder de computação para ataques de força bruta) de que estes dispõem;
3. a robustez da encriptação tiver em consideração o período de tempo específico durante o qual a confidencialidade dos dados pessoais encriptados deve ser mantida;
4. o algoritmo de encriptação for implementado sem falhas através de software mantido de forma correta, cuja conformidade com a especificação do algoritmo escolhido tenha sido verificada, por exemplo, mediante certificação;
5. as chaves forem geridas de forma fiável (geradas, administradas, armazenadas, se aplicável, associadas à identidade de um destinatário pretendido e revogadas); e
6. as chaves forem mantidas unicamente sob o controlo do exportador de dados, ou de outras entidades responsáveis por tal tarefa que residam no EEE ou num país terceiro, território ou um ou mais setores especificados de um país terceiro ou numa organização internacional para a qual a Comissão tenha determinado que é assegurado um nível de proteção adequado, em conformidade com o artigo 45.º do RGPD,

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

Caso de utilização 2: Transferência de dados pseudonimizados

80. Primeiro, um exportador de dados pseudonimiza os dados que detém e só depois os transfere para um país terceiro para análise, por exemplo, para fins de investigação.

Se:

1. um exportador de dados transferir dados pessoais tratados de tal forma que já não podem ser atribuídos a um titular de dados específico, nem ser utilizados para identificar o titular de dados num grupo sem a utilização de informações adicionais[69];
2. as referidas informações adicionais forem detidas exclusivamente pelo exportador de dados e mantidas separadamente num Estado-Membro ou num país terceiro, território ou um ou mais setores especificados de um país terceiro ou numa organização internacional para a qual a Comissão tenha determinado que é assegurado um nível de proteção adequado, em conformidade com o artigo 45.º do RGPD;
3. a divulgação ou utilização não autorizada de tais informações adicionais for impedida mediante garantias técnicas e organizativas adequadas e for assegurado que o exportador de dados mantém o controlo exclusivo do algoritmo ou repositório que permite a reidentificação com tais informações adicionais; e

[69] 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;».

4. o responsável pelo tratamento tiver estabelecido, através de uma análise exaustiva dos dados em questão, tendo em conta quaisquer 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 comparados com tais informações,

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

81. 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[70] podem permitir a identificação da pessoa em causa, mesmo que o nome, a morada ou outros identificadores simples sejam omitidos.

82. O que precede é particularmente 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).

83. 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.

Caso de utilização 3: Dados encriptados que apenas transitam por países terceiros

84. Um exportador de dados deseja transferir dados para um destino que se considera que possui proteção adequada em conformidade com o artigo 45.º do RGPD. Os dados são transferidos através de um país terceiro.

Se:

1. um exportador de dados transferir dados pessoais para um importador de dados numa jurisdição que assegure uma proteção adequada, os dados forem transportados pela Internet e os dados poderem ser encaminhados geograficamente através de um país terceiro que não assegure um nível de proteção essencialmente equivalente;
2. for utilizada encriptação de transporte para a qual se garante que os protocolos de encriptação utilizados são os mais avançados e proporcionam uma proteção eficaz contra ataques ativos e passivos com recursos acessíveis às autoridades públicas do país terceiro;
3. a desencriptação apenas for possível fora do país terceiro em questão;
4. as partes envolvidas na comunicação acordarem numa infraestrutura ou autoridade de certificação de chave pública digna de confiança;
5. forem utilizadas medidas específicas de proteção e de estado da arte contra ataques ativos e passivos à encriptação de transporte;

[70] 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;».

6. no caso de a encriptação de transporte não proporcionar por si só a segurança adequada devido à experiência com vulnerabilidades da infraestrutura ou do software utilizado, os dados pessoais forem também encriptados de ponta a ponta na camada de aplicação utilizando métodos de encriptação do estado da arte;
7. o algoritmo de encriptação e a respetiva parametrização (por exemplo, comprimento da chave, modo de funcionamento, se aplicável) estiverem em conformidade com o estado da arte e poderem ser considerados robustos contra a criptoanálise realizada pelas autoridades públicas do país de trânsito, tendo em conta os recursos e as capacidades técnicas (por exemplo, poder de computação para ataques de força bruta) de que estes dispõem;
8. a robustez da encriptação tiver em consideração o período de tempo específico durante o qual a confidencialidade dos dados pessoais encriptados deve ser mantida;
9. o algoritmo de encriptação for implementado sem falhas através de software mantido de forma correta, cuja conformidade com a especificação do algoritmo escolhido tenha sido verificada, por exemplo, mediante certificação;
10. a existência de *backdoors* (em hardware ou software) tiver sido descartada;
11. se as chaves forem 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 proporcione 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

85. 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 isentar um importador de dados residente de um possível acesso ilícito aos dados detidos por tal destinatário para o fim em questão, por exemplo, em virtude de um 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 recorrer aos serviços de um subcontratante de forma a permitir que as autoridades públicas tenham acesso aos dados enquanto estão na posse do subcontratante ou o importador de dados transmitir 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 forem encriptados antes de serem transmitidos através de um método conforme ao estado da arte que assegure que a desencriptação não será possível sem o conhecimento da chave de desencriptação (encriptação de ponta a ponta) durante todo o período no qual os dados precisam de ser protegidos;
5. a chave de desencriptação estiver sob a custódia exclusiva do importador de dados protegidos e devidamente protegida contra utilização ou divulgação não autorizada mediante medidas técnicas e organizativas conformes com o estado da arte; e

6. o exportador de dados tiver estabelecido de forma fiável que a chave de encriptação que pretende utilizar corresponde à chave de desencriptação na posse do destinatário,

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

Caso de utilização 5: Tratamento partilhado ou com várias partes

86. 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 a que nenhum fragmento que um subcontratante individual receba seja suficiente para reconstruir os dados pessoais, no todo ou em parte. O exportador de dados recebe o resultado do tratamento de cada um dos subcontratantes independentemente e reúne os fragmentos recebidos para chegar ao resultado final, que pode constituir dados pessoais ou agregados.

Se:

1. um exportador de dados tratar dados pessoais de tal forma que estes sejam divididos em duas ou mais partes, cada uma das quais não pode ser interpretada ou atribuída a um titular de dados específico sem a utilização de informações adicionais;
2. cada um dos fragmentos for transferido para um subcontratante diferente localizado numa jurisdição diferente;
3. os subcontratantes optarem tratar os dados em conjunto, por exemplo, utilizando computação multipartidária segura, de forma a que estes não tenham acesso a qualquer informação que não possuíam antes da computação;
4. o algoritmo utilizado para a computação partilhada for seguro contra adversários ativos;
5. não houver provas de colaboração entre as autoridades públicas localizadas nas respetivas jurisdições em que se encontram os subcontratantes, o que lhes permitiria aceder a todos os conjuntos de dados pessoais na posse dos subcontratantes e lhes permitiria reconstituir e explorar o conteúdo dos dados pessoais de uma forma clara em circunstâncias em que tal exploração não respeitaria os direitos e liberdades fundamentais dos titulares dos dados. Do mesmo modo, as autoridades públicas de qualquer país não devem ter autoridade para aceder aos dados pessoais na posse dos subcontratantes em todas as jurisdições em causa.
6. o responsável pelo tratamento tiver estabelecido, 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 os fragmentos de dados pessoais transmitidos aos subcontratantes não podem ser atribuídos a uma pessoa singular identificada ou identificável, mesmo que sejam comparados com tais informações,

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

Cenários nos quais não é possível encontrar medidas *eficazes*

87. Em determinados cenários, as medidas descritas infra não seriam eficazes para assegurar um nível de proteção essencialmente equivalente dos dados transferidos para o país terceiro. Por conseguinte, não se enquadrariam como medidas complementares.

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

88. Um exportador de dados recorre a um prestador de serviços na nuvem ou outro subcontratante para que os dados pessoais sejam tratados de acordo com as suas instruções num país terceiro.

Se:

1. um responsável pelo tratamento transferir dados para um prestador de serviços na nuvem ou outro subcontratante;
2. o prestador de serviços na nuvem ou outro subcontratante precisar de obter acesso aos dados não encriptados, a fim de executar a tarefa que lhe foi atribuída; e
3. o poder concedido às autoridades públicas do país de destino para aceder aos dados transferidos for além do que é necessário e proporcionado numa sociedade democrática,[71]

o CEPD é incapaz de prever uma medida técnica eficaz para evitar que tal acesso viole os direitos do titular de dados, tendo em consideração o atual estado da arte. O CEPD não descarta que um subsequente desenvolvimento tecnológico possa prever medidas para os fins comerciais pretendidos, sem requerer o acesso não encriptado.

89. Nos cenários indicados, sempre que os dados pessoais não encriptados são tecnicamente necessários para a prestação do serviço por parte do subcontratante, a encriptação de transporte e a encriptação de dados inativos, mesmo em conjunto, não constituem uma medida complementar que assegura um nível de proteção essencialmente equivalente se o importador de dados estiver na posse das chaves criptográficas.

Caso de utilização 7: Acesso remoto aos dados para fins comerciais

90. Um exportador de dados disponibiliza dados pessoais a entidades de um país terceiro para serem utilizados para fins comerciais partilhados. Um conjunto típico pode consistir num responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro que transfira 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 para pessoal ao exportador de dados, para os quais precisa 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. se um exportador de dados transferir dados pessoais para um importador de dados num país terceiro, mediante a disponibilização dos mesmos num sistema de informação normalmente utilizado de uma forma que permita ao importador o acesso direto aos dados que pretende ou mediante a transferência dos mesmos diretamente, individualmente ou em massa, através da utilização de um serviço de comunicação;
2. o importador utilizar os dados não encriptados para os seus próprios fins;

[71] Ver artigos 47.º e 52.º da Carta dos Direitos Fundamentais da UE, artigo 23.º, n.º 1, do RGPD e Recomendações do CEPD sobre as garantias europeias indispensáveis no que concerne a medidas de vigilância.

3. o poder concedido às autoridades públicas do país de destino para aceder aos dados transferidos for além do que é necessário e proporcionado numa sociedade democrática,

o CEPD for incapaz de prever uma medida técnica eficaz para evitar que tal acesso viole os direitos do titular de dados.

91. Nos cenários indicados, sempre que os dados pessoais não encriptados são tecnicamente necessários para a prestação do serviço por parte do subcontratante, a encriptação de transporte e a encriptação de dados inativos, mesmo em conjunto, não constituem uma medida complementar que assegura um nível de proteção essencialmente equivalente se o importador de dados estiver na posse das chaves criptográficas.

Medidas contratuais adicionais

92. As medidas em causa consistirão geralmente em compromissos contratuais[72] unilaterais, bilaterais ou multilaterais.[73] Se for utilizado um instrumento de transferência do artigo 46.º do RGPD, este já contém, na maioria dos casos, vários compromissos (a maior parte contratuais) para o exportador de dados e importador de dados, que visam servir de garantia para os dados pessoais.[74]

93. Em algumas 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 na UE. Consoante a natureza das medidas contratuais, geralmente incapazes de vincular as autoridades do país terceiro quando não são partes signatárias do contrato[75], tais 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 várias das referidas medidas não irão necessária e sistematicamente assegurar que a sua transferência cumpre a norma de equivalência essencial requerida pela legislação da UE.

94. Dependendo das medidas contratuais já incluídas no instrumento de transferência do artigo 46.º do RGPD no qual se baseia, podem também ser úteis medidas contratuais adicionais para permitir que os exportadores de dados baseados no EEE tomem conhecimento de novos desenvolvimentos que afetem a proteção dos dados transferidos para países terceiros.

95. Conforme referido, as medidas contratuais não poderão excluir a aplicação da legislação de um país terceiro que não cumpre a norma das garantias europeias indispensáveis do CEPD sempre que a legislação obrigue os importadores a cumprir as intimações de divulgação de dados recebidas por parte das autoridades públicas.[76]

---

[72] Serão de natureza privada e não serão considerados acordos internacionais ao abrigo do direito internacional público. Assim, normalmente não vincularão a autoridade pública do país terceiro enquanto parte não signatária do contrato aquando da sua celebração com organismos privados em países terceiros, conforme sublinhado pelo Tribunal no seu Acórdão C-311/18 (Schrems II), n.º 125.

[73] Por exemplo, no âmbito das regras vinculativas aplicáveis às empresas que deveriam, de qualquer forma, regulamentar algumas das medidas infra.

[74] Ver Acórdão C-311/18 (Schrems II), n.º 137, no qual o Tribunal reconheceu que as cláusulas contratuais-tipo contêm *«mecanismos efetivos que permitam, 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 n.º 148.

[75] C-311/18 (Schrems II), n.º 125.

[76] Acórdão do TJUE C-311/18 (Schrems II), n.º 132.

96. Alguns exemplos de tais potenciais medidas contratuais constam da lista infra e são classificados de acordo com a sua natureza:

Estipulação da obrigação contratual de utilizar medidas técnicas específicas

97. ***Consoante as circunstâncias específicas das transferências, o contrato poderá ter de prever a adoção de medidas técnicas específicas para permitir a realização das transferências (ver as medidas técnicas sugeridas supra).***

98. ***Condições para eficiência:***

- A presente cláusula poderia ser eficaz nas situações em que a necessidade de medidas técnicas tenha sido identificada pelo exportador. Teria então de ser prevista sob uma forma jurídica a fim de assegurar que o importador também se compromete a adotar as medidas técnicas necessárias, se necessário.

Obrigações de transparência:

99. ***O exportador poderia aditar anexos ao contrato com informações prestadas pelo importador, com base nos seus melhores esforços, relativamente ao acesso aos dados por parte das autoridades públicas, incluindo no domínio das informações, desde que a legislação do país de destino esteja em conformidade com as garantias europeias indispensáveis do CEPD. O que precede pode ajudar o exportador de dados a cumprir a sua obrigação de documentar a avaliação do nível de proteção no país terceiro.***

100. Por exemplo, o importador poderia ser obrigado a:

(1) enumerar as leis e os 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 experiência do importador ou em relatórios de várias fontes (por exemplo, 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 de transferência de dados em causa (ou seja, no domínio regulamentar específico; relativamente ao tipo de entidades aos quais o importador de dados pertence;...);
(3) indicar que medidas são tomadas para impedir o acesso aos dados transferidos (caso existam);
(4) prestar informações suficientemente pormenorizadas sobre todos os pedidos de acesso a dados pessoais por parte das autoridades públicas que o importador recebeu durante um determinado período de tempo,[77] nomeadamente nas áreas mencionadas no ponto 1 supra e

[77] A duração do período deve depender do risco para os direitos e liberdades dos titulares dos dados sujeitos à transferência em causa (por exemplo, o último ano antes da revogação do instrumento de exportação de dados com o exportador de dados).

que incluam informações sobre os pedidos recebidos, os dados solicitados, o organismo requerente e a base jurídica para a divulgação e em que medida o importador divulgou o pedido de dados;[78]

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

101. As informações em causa poderiam ser prestadas mediante questionários estruturados preenchidos e assinados pelo importador e agravadas pela obrigação contratual do importador de declarar num período de tempo qualquer potencial alteração a tal informação, conforme já ocorre nos processos de diligência devida.

102. ***Condições para eficiência:***

- O importador deve ser capaz de prestar este tipo de informação ao exportador, na medida dos seus conhecimentos e depois de ter empregado os seus melhores esforços para a obter.[79]
- A presente obrigação imposta ao importador é uma forma de assegurar que o exportador se sensibiliza e se mantém consciente dos riscos associados à transferência de dados para um país terceiro. Assim, permitirá ao exportador não celebrar o contrato ou, se a informação sofrer alterações após a sua celebração, cumprir a sua obrigação de suspender a transferência e/ou rescindir o contrato, caso a legislação do país terceiro, as garantias constantes do 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 na UE. No entanto, tal obrigação não pode justificar a divulgação de dados pessoais por parte do importador, nem dar azo à expectativa de que não haverá mais pedidos de acesso.

***

103. ***O exportador pode igualmente aditar cláusulas que permitam ao importador certificar que 1) não criou propositadamente «backdoors» ou programas semelhantes que possam ser utilizados para aceder ao sistema e/ou aos dados pessoais, 2) não criou ou alterou propositadamente os seus processos comerciais de forma a facilitar o acesso a sistemas ou dados pessoais e 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 esteja na posse ou entregue a chave de encriptação.***[80]

104. ***Condições para eficiência:***

- 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 terá de notificar o exportador do facto de não poder cumprir os seus compromissos contratuais.[81]

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

[79] Ver ponto 32.5 supra.

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

[81] Ver ponto 32.5 supra.

- O contrato deve incluir sanções e/ou a possibilidade de o exportador rescindir o contrato com pouca antecedência nos casos em que o importador não demonstre a existência de *backdoors* ou programas similares, de processos comerciais manipulados ou de qualquer requisito de implementar qualquer um destes ou não informe imediatamente o exportador assim que a sua existência lhe seja comunicada.

***

105. ***O exportador poderia reforçar o seu poder de realizar auditorias[82] 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 necessário e proporcionado numa sociedade democrática), por exemplo, mediante o estabelecimento de um aviso com pouca antecedência e mecanismos que garantam a intervenção rápida dos organismos de inspeção e o reforço da autonomia do exportador na seleção dos organismos de inspeção.***

106. ***Condições para eficiência:***

- Para assegurar a total eficiência da auditoria, o âmbito de aplicação desta deve abranger, legal e tecnicamente, qualquer tratamento dos dados pessoais transmitidos no país terceiro realizado por subcontratantes ou subcontratantes ulteriores do importador.
- Os registos de acesso e outros registos semelhantes devem estar protegidos contra qualquer manipulação para que os auditores possam encontrar provas de divulgação. Os registos de acesso e outros registos semelhantes devem também distinguir entre acessos na sequência de operações comerciais regulares e acessos na sequência de intimações ou pedidos de acesso.

***

107. ***Nos casos em que o direito e as práticas 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 poderia 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, como resultado, a norma exigida relativa ao «nível de proteção de dados essencialmente equivalente».[83]***

108. A referida impossibilidade de cumprimento pode resultar de alterações na legislação ou nas práticas do país terceiro.[84] As cláusulas podem estabelecer prazos e procedimentos específicos e rigorosos para a rápida suspensão da transferência de dados e/ou a rescisão do contrato, bem como para a devolução ou eliminação dos dados recebidos pelo importador. O acompanhamento dos pedidos recebidos, do respetivo âmbito e da eficácia das medidas adotadas para os contestar deve fornecer ao exportador

[82] 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 poderiam ser previstas no âmbito de um código de conduta ou através de certificação.

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

[84] Ver Acórdão C-311/18 (Schrems II), n.º 139, no qual o Tribunal 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».*

indicações suficientes para exercer o seu dever de suspender ou pôr termo à transferência e/ou rescindir o contrato.

109. ***Condições para eficiência:***

- 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, caso o pedido tenha por base leis de tal 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 rescindir o contrato.
- O importador de dados deve monitorizar quaisquer desenvolvimentos jurídicos ou políticos que possam levar ao incumprimento das suas obrigações e deve informar de imediato o exportador de dados de tais alterações e desenvolvimentos e se possível antes da sua implementação para permitir ao exportador de dados recuperar os dados do importador de dados.
- As cláusulas devem prever um mecanismo rápido através do qual o exportador de dados autoriza o importador de dados a proteger ou devolver de imediato os dados ao exportador de dados, ou se tal não for viável, apagar ou encriptar os dados de um modo seguro sem necessariamente esperar pelas instruções do exportador, caso seja atingido um limiar específico acordado 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 assegurar que pode ser utilizado com pouco aviso prévio.
- Outras cláusulas poderiam permitir ao exportador monitorizar o cumprimento de tais obrigações por parte do importador mediante auditorias, inspeções e outras medidas de verificação e aplicá-las com sanções ao importador e/ou à possibilidade de o exportador suspender a transferência e/ou rescindir imediatamente o contrato.

***

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

111. ***Condições para eficiência:***

- 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 «warrant canary».
- O importador de dados deve assegurar que a sua chave privada para a assinatura do «warrant canary» é mantida em segurança e que não pode ser forçado a emitir falsas notificações através de regulamentos do país terceiro. Para o efeito, poderá ser útil se forem necessárias

várias assinaturas de diferentes pessoas e/ou se o «warrant canary» for emitido por uma pessoa fora da jurisdição do país terceiro.

Obrigações de adotar medidas específicas

112. ***O importador poderia comprometer-se a rever, ao abrigo da legislação do país de destino, a legalidade de qualquer intimação de divulgação de dados, nomeadamente se se mantém nos limites dos poderes concedidos à autoridade pública requerente, e a contestar a intimação se, após uma avaliação minuciosa, concluir que existem fundamentos ao abrigo da lei do país de destino para o fazer. Ao contestar uma intimação, o importador de dados deve procurar medidas provisórias para suspender os efeitos da intimação até que o tribunal tenha decidido sobre o mérito da contestação. O importador teria a obrigação de não divulgar os dados pessoais solicitados até ser obrigado a fazê-lo ao abrigo das regras processuais aplicáveis. O importador de dados também se comprometeria a prestar a quantidade mínima de informação admissível ao responder à intimação, com base numa interpretação razoável da mesma.***

113. ***Condições para eficiência:***

- O ordenamento jurídico do país terceiro deve oferecer vias jurídicas eficazes para contestar as intimações de divulgação de dados.
- Esta cláusula oferecerá sempre uma proteção adicional muito limitada, uma vez que uma intimação de divulgação de dados pode ser legal ao abrigo do ordenamento jurídico do país terceiro, mas tal ordenamento jurídico pode não cumprir as normas da UE. A medida contratual em causa terá necessariamente de ser complementar a outras medidas complementares.
- As contestações às intimações devem ter um efeito suspensivo ao abrigo da lei do país terceiro. Caso contrário, as autoridades públicas continuariam a ter acesso aos dados dos indivíduos e qualquer ação subsequente a favor do indivíduo teria o efeito limitado de lhe permitir pedir indemnizações por consequências negativas resultantes da divulgação de dados.
- O importador terá de ser capaz de documentar e demonstrar ao exportador as ações que tomou, no exercício dos seus melhores esforços para cumprir tal compromisso.

***

114. ***Na mesma situação descrita supra, o importador poderia comprometer-se a informar a autoridade pública requerente da incompatibilidade da intimação com as garantias constantes do instrumento de transferência do artigo 46.º do RGPD[85] e do conflito de obrigações daí resultante para o importador. O importador notificaria simultaneamente e logo que possível o exportador e/ou a***

[85] Por exemplo, as cláusulas contratuais-tipo preveem que o tratamento de dados, incluindo a respetiva 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 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 TJUE confirma que as disposições do RGPD, lidas à luz da Carta dos Direitos Fundamentais da UE, fazem parte desta legislação; ver TJUE, C-311/18 (Schrems II), n.º 138.

autoridade de controlo competente do EEE, na medida do possível ao abrigo do ordenamento jurídico do país terceiro.

115. ***Condições para eficiência:***

- Tais informações sobre a proteção conferida pela legislação da UE e o conflito de obrigações devem ter algum efeito jurídico no ordenamento jurídico do país terceiro, tal como um recurso a nível judicial ou administrativo da intimação ou do pedido de acesso, a exigência de um mandado judicial e/ou uma suspensão temporária da intimação para acrescentar alguma 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 receção da intimação ou do pedido de acesso.
- O importador terá de ser capaz de documentar e demonstrar ao exportador as ações que tomou, no exercício dos seus melhores esforços para cumprir tal compromisso.

Incentivar os titulares dos dados a exercer os seus direitos

116. ***O contrato poderá prever que os dados pessoais transmitidos em texto simples no decurso normal das operações comerciais (incluindo em casos de apoio) apenas podem ser acedidos com o consentimento expresso ou implícito do exportador e/ou do titular dos dados.***

117. ***Condições para eficiência:***

- A presente cláusula poderia ser eficaz nas situações em que os importadores recebem pedidos de cooperação das autoridades públicas de carácter voluntário, em oposição, por exemplo, ao acesso aos dados pelas autoridades públicas que ocorre sem o conhecimento do importador de dados ou contra a sua vontade.
- Em algumas 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 exemplo, no caso de funcionários).[86]
- As políticas ou os regulamentos nacionais que obriguem o importador a não divulgar a intimação 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 em «plant text» sejam acessíveis. As referidas medidas técnicas para a restrição do acesso podem ser previstas, nomeadamente, se o acesso apenas for concedido em casos específicos de apoio ou serviço, mas os dados forem armazenados no EEE.

***

118. ***O contrato poderá obrigar o importador e/ou o exportador a notificar imediatamente o titular dos dados do pedido ou da intimação recebida por parte das autoridades públicas do país terceiro ou da incapacidade de o importador cumprir os compromissos contratuais, a fim de permitir ao titular dos dados procurar informações e uma via de recurso eficaz (por exemplo, apresentando uma reclamação junto da respetiva autoridade de controlo competente e/ou autoridade judicial e demonstrando a sua posição nos tribunais do país terceiro).***

[86] Artigo 4.º, n.º 11, do RGPD.

119. ***Condições para eficiência:***

- Esta notificação poderia alertar o titular dos dados para possíveis acessos por parte das autoridades públicas de países terceiros aos seus dados. Assim, poderia permitir ao titular dos dados procurar informações adicionais junto dos exportadores e apresentar uma reclamação junto da sua autoridade de controlo competente. A cláusula em questão poderia igualmente abordar algumas das dificuldades que um indivíduo pode enfrentar para demonstrar a sua capacidade judiciária (*locus standi*) perante os tribunais de países terceiros para contestar o acesso das autoridades públicas aos seus dados.
- As políticas ou os regulamentos nacionais podem impedir tal notificação ao titular dos dados. No entanto, o exportador e o importador poderiam comprometer-se a informar o titular dos dados assim que as restrições à divulgação de dados sejam levantadas e a empregar os seus melhores esforços para obter a derrogação da proibição de divulgação. No mínimo, o exportador ou a autoridade de controlo competente poderia notificar o titular dos dados da suspensão ou do termo da transferência dos seus dados pessoais devido à incapacidade de o importador cumprir os seus compromissos contratuais, na sequência da receção de um pedido de acesso.

***

120. ***O contrato poderia comprometer o exportador e o importador a ajudar o titular dos dados a exercer os seus direitos na jurisdição do país terceiro através de processos de recurso «ad hoc» e aconselhamento jurídico.***

121. ***Condições para eficiência***

- As políticas ou os regulamentos nacionais podem impor condições que podem comprometer a eficiência dos processos de recurso *ad hoc* previstos.
- O aconselhamento jurídico poderia ser útil para o titular dos dados, especialmente considerando o quão complexo e dispendioso pode ser para um titular dos dados compreender o sistema jurídico de um país terceiro e exercer ações legais a partir do 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 na UE. A medida contratual em causa terá necessariamente de ser complementar a outras medidas complementares.

A referida medida complementar apenas seria eficaz se a legislação do país terceiro previsse a reparação perante os tribunais nacionais ou se existisse um processo de recurso *ad hoc*. Em qualquer caso, tal não seria, contudo, uma medida complementar eficaz contra medidas de vigilância caso não exista um processo de recurso.

Medidas organizativas

122. 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. Estas podem contribuir para assegurar a coerência na proteção dos dados pessoais durante todo o ciclo do tratamento. As medidas organizativas podem também melhorar a sensibilização dos exportadores para os riscos e as tentativas de obtenção de acesso aos dados em países terceiros, bem como a sua capacidade de reagir às mesmas. A seleção e implementação de uma ou várias das referidas medidas não irão necessária e sistematicamente assegurar que a sua transferência cumpre a norma de equivalência essencial requerida pela legislação da UE. Em função das circunstâncias específicas da transferência e da avaliação realizada com base na legislação do país terceiro, são necessárias medidas organizativas para complementar as medidas contratuais e/ou técnicas, a fim de assegurar um nível de proteção dos dados pessoais essencialmente equivalente ao garantido na UE.

123. A avaliação das medidas mais adequadas deve ser realizada caso a caso, tendo em consideração a necessidade de os responsáveis pelo tratamento e subcontratantes cumprirem o princípio da responsabilidade. De seguida, o CEPD apresenta 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 para a gestão de transferências específicas a grupos de empresas

124. ***Adoção de políticas internas adequadas com clara atribuição de responsabilidades pelas transferências de dados, canais de comunicação e procedimentos operacionais normalizados para os casos de pedidos confidenciais ou oficiais de acesso aos dados por parte das autoridades públicas. Especialmente no caso de transferências entre grupos de empresas, as políticas em causa podem incluir, entre outras, a nomeação de uma equipa específica, que deve estar baseada no EEE e ser composta por peritos em TI, proteção de dados e leis de privacidade, para tratar de pedidos que envolvam dados pessoais transferidos da UE; a notificação à gestão empresarial e jurídica e ao exportador de dados após a receção de tais pedidos; as medidas processuais para contestar pedidos desproporcionados ou ilícitos e a prestação de informações transparentes aos titulares dos dados.***

125. Desenvolvimento de procedimentos de formação específicos para o pessoal responsável pela gestão dos pedidos de acesso aos dados pessoais por parte das autoridades públicas, que 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 no que concerne ao acesso aos dados pessoais por parte das autoridades públicas, nomeadamente, conforme decorre 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 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.

126. ***Condições para eficiência:***

- As referidas políticas apenas podem ser previstas para os casos em que o pedido das autoridades públicas do país terceiro é compatível com a legislação da UE.[87] Sempre que o pedido é incompatível, tais políticas não seriam suficientes para assegurar um nível de proteção dos dados pessoais equivalente e, conforme supramencionado, as transferências devem ser interrompidas ou devem ser adotadas medidas complementares adequadas para evitar o acesso.

Medidas de transparência e responsabilidade

127. ***Documentação e registo de pedidos de acesso recebidos por parte das autoridades públicas e a respetiva resposta fornecida, juntamente com a fundamentação jurídica e os intervenientes envolvidos (por exemplo, se o exportador foi notificado e a sua resposta, a avaliação da equipa responsável pelo tratamento de tais pedidos, etc.). Os referidos registos devem ser colocados à disposição do exportador de dados, que por sua vez os deve disponibilizar aos titulares dos dados, sempre que necessário.***

128. ***Condições para eficiência:***

- 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 deve informar o exportador da sua incapacidade de disponibilizar tais documentos e registos, dando assim ao exportador a opção de suspender as transferências caso tal incapacidade resulte numa redução do nível de proteção.

***

129. ***Publicação regular de resumos ou relatórios de transparência no que concerne aos pedidos governamentais de acesso a dados e a resposta fornecida, na medida em que a publicação seja permitida pela legislação nacional.***

130. ***Condições para eficiência:***

- A informação prestada deve ser pertinente, clara e o mais detalhada possível. A legislação nacional do país terceiro pode impedir a divulgação de informações detalhadas. Em tais casos, o importador de dados deve empregar os seus melhores esforços para publicar informação estatística ou informação agregada semelhante.

Métodos organizacionais e medidas de minimização de dados

131. ***No contexto de uma transferência, os requisitos organizativos já existentes ao abrigo do princípio da responsabilidade podem ser igualmente considerados medidas úteis, tais como a adoção de políticas rigorosas e granulares de confidencialidade e de acesso aos dados e as melhores práticas que tenham por base um princípio da «necessidade de tomar conhecimento» e sejam monitorizadas mediante auditorias regulares e aplicadas através 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. Por exemplo, em alguns casos pode não ser necessário transferir determinados***

[87] Ver processos C-362/14 (Schrems I, n.º 94; C-311/18 (Schrems II), n.os 168, 174, 175 e 176.

dados (por exemplo, em caso de acesso remoto aos dados do EEE, tal como em casos de apoio, sempre que é concedido acesso restrito em vez de acesso total; ou quando a prestação de um serviço requer apenas a transferência de um conjunto limitado de dados e não uma base de dados completa).

132. ***Condições para eficiência:***

- Devem ser realizadas auditorias regulares e impostas medidas disciplinares rigorosas a fim de controlar e impor o cumprimento das medidas de minimização de 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, 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.

***

133. ***Desenvolvimento das 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 transferências internacionais de dados pessoais.***

134. ***Condições para eficiência:***

- 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 relativamente à necessidade da transferência e de garantias adicionais, caso existam.
- 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

135. ***Adoção de políticas rigorosas de segurança e privacidade de dados, que têm por base a certificação ou os códigos de conduta da UE ou normas internacionais (por exemplo, normas ISO) e melhores práticas (por exemplo, ENISA), tendo em devida conta o estado da arte, em conformidade com o risco das categorias de dados tratados e a probabilidade de tentativas de acesso aos mesmos por parte das autoridades públicas.***

Outros

136. ***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 um nível de proteção dos dados pessoais transferidos equivalente ao garantido na UE.***

***

137. ***Compromissos do importador de dados de não proceder a qualquer posterior transferência dos dados pessoais no país terceiro ou noutros países terceiros ou de suspender transferências em curso, sempre que não puder ser assegurado no país terceiro um nível de proteção dos dados pessoais equivalente ao garantido na UE.***[88]

[88] C-311/18 (Schrems II), n.os 135 e 137.

ANEXO 3: FONTES POSSÍVEIS DE INFORMAÇÃO PARA AVALIAR UM PAÍS TERCEIRO

138. O importador de dados deve estar em condições de indicar fontes ao utilizador e prestar informações pertinentes relacionadas com o país terceiro no qual está estabelecido e com a legislação que lhe é aplicável. O utilizador pode igualmente consultar diversas fontes de informação, tais como as indicadas de seguida, de forma não exaustiva:

- Jurisprudência do Tribunal de Justiça da União Europeia (TJUE) e do Tribunal Europeu dos Direitos Humanos (TEDH)[89], conforme referido nas recomendações das garantias europeias indispensáveis,[90]
- Decisões de adequação no país de destino, caso a transferência tenha por base uma base jurídica diferente,[91]
- Resoluções e relatórios de organizações intergovernamentais, tais como o Conselho da Europa,[92] outros organismos regionais[93]; e organismos e agências da ONU (por exemplo, Conselho dos Direitos Humanos da ONU[94], Comité dos Direitos Humanos[95]),
- 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 instituições académicas, e organizações da sociedade civil (por exemplo, ONG e associações setoriais).

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

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

[91] C-311/18 (Schrems II), n.º 141; ver decisões de adequação em https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt

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

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

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

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