



18/PT

WP 254 rev.01

Grupo de trabalho do artigo 29.º

Documento de referência relativo à adequação

Adotado em 28 de novembro de 2017

Última redação revista e adotada em 6 de fevereiro de 2018

Este grupo de trabalho foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Cidadania da União) da Comissão Europeia, Direção-Geral de Justiça, B-1049 Bruxelas, Bélgica, Gabinete n.º MO-59 02/013.

Sítio: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Introdução

O grupo de trabalho das autoridades de proteção de dados da UE¹ (o GT29) publicou anteriormente um documento de trabalho sobre as transferências de dados pessoais para países terceiros (WP12)². Com a substituição desta diretiva pelo Regulamento Geral da Proteção de Dados (RGPD)³ da UE, o GT29 revisita o documento WP12, onde forneceu as suas orientações anteriores, para o atualizar no contexto da nova legislação e da recente jurisprudência do Tribunal de Justiça Europeu (TJUE)⁴.

O presente documento de trabalho pretende atualizar o capítulo I do WP12 relacionado com a questão central do nível adequado de proteção de dados num país terceiro, num território ou num ou mais setores específicos desse país terceiro ou numa organização internacional (doravante: «países terceiros ou organizações internacionais»). Este documento será continuamente revisto e, se necessário, atualizado nos próximos anos, com base na experiência prática adquirida com a aplicação do RGPD. Os capítulos II (*Aplicação da abordagem em questão aos países que ratificaram a Convenção 108 do Conselho da Europa*) e III (*Aplicação da abordagem em questão à autorregulamentação por parte de um setor*) do documento WP12 serão atualizados numa fase posterior.

O presente documento de trabalho centra-se exclusivamente nas decisões relativas à adequação, que constituem atos de execução⁵ da Comissão Europeia, de acordo com o artigo 45.º do RGPD. Outros aspetos das transferências de dados pessoais para países terceiros e organizações internacionais serão analisados em documentos de trabalho futuros, publicados separadamente (as BCR, as interrogações).

O presente documento visa fornecer orientações à Comissão Europeia e ao GT29, ao abrigo do RGPD, com vista à avaliação do nível de proteção de dados em países terceiros e organizações internacionais, estabelecendo quais os princípios centrais da proteção de dados que devem ser incluídos no quadro normativo de um país terceiro ou organização internacional para assegurar uma equivalência substancial em relação ao quadro normativo europeu. Além disso, pode servir para orientar os países terceiros e as organizações internacionais interessados em alcançar a adequação. Contudo, os princípios definidos no presente documento de trabalho não se destinam diretamente aos responsáveis pelo tratamento nem aos processadores de dados (subcontratantes).

O presente documento é composto por quatro capítulos:

Capítulo 1: Informações genéricas sobre o conceito de adequação

Capítulo 2: Aspetos processuais das decisões de adequação ao abrigo do RGPD

Capítulo 3: Princípios gerais em matéria de proteção de dados. Este capítulo inclui os principais princípios gerais em matéria de proteção de dados para assegurar que o nível de proteção de dados num país terceiro ou organização internacional é substancialmente equivalente ao estabelecido na legislação da UE.

Capítulo 4: Garantias essenciais em relação ao acesso para fins de aplicação coerciva da lei e de segurança nacional para limitar as interferências nos direitos fundamentais. Este capítulo inclui as garantias essenciais em relação ao acesso para fins de aplicação coerciva da lei e segurança nacional, no seguimento do acórdão Schrems do TJUE, de 2015, e com base no documento de trabalho do GT29 sobre garantias essenciais, adotado em 2016.

¹Tal como estabelecido nos termos do artigo 29.º da Diretiva 95/46/CE relativa à proteção de dados na UE.

²WP12, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25º e 26º da Diretiva comunitária relativa à proteção dos dados», adotado pelo grupo de trabalho em 24 de julho de 1998.

³Regulamento (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) (Texto relevante para efeitos do EEE).

⁴Nomeadamente, o Processo C-362/14, Maximilian Schrems/Data Protection Commissioner, 6 de outubro de 2015.

⁵Ver os artigos 45.º, n.º 3, e 93.º, n.º 2, do RGPD que são pertinentes para mais informações sobre os atos de execução.

Capítulo 1: Informações genéricas sobre o conceito de adequação

O artigo 45.º, n.º 1, do RGPD determina o princípio de que as transferências de dados para um país terceiro ou organização internacional só podem realizar-se se o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegurar um nível de proteção adequado.

Este conceito de «nível de proteção adequado», que já existia na Diretiva 95/46/CE, foi mais desenvolvido pelo TJUE. Chegamos a este ponto, é importante lembrar a norma definida pelo TJUE no processo Schrems, designadamente que, embora o «*nível de proteção*» num país terceiro deva ser «*substancialmente equivalente*» ao garantido dentro da UE, «*os meios a que esse país recorre para assegurar tal nível de proteção [podem] ser diferentes dos implementados dentro da [UE]*»⁶. Por conseguinte, o objetivo não é imitar ponto por ponto a legislação europeia, mas sim estabelecer o essencial – os principais requisitos dessa legislação.

A finalidade da decisão de adequação da Comissão Europeia é confirmar formalmente, com efeitos vinculativos para os Estados-Membros⁷, que o nível de proteção de dados de um país terceiro ou organização internacional é substancialmente equivalente ao nível de proteção de dados da União Europeia⁸. A adequação pode ser alcançada através de uma combinação de direitos conferidos aos titulares dos dados e de deveres impostos a quem trata os dados ou quem exerce o controlo sobre esse tratamento e supervisão por organismos independentes. Contudo, as normas relativas à proteção de dados só são eficazes se tiverem carácter executório e forem aplicadas na prática. Por conseguinte, é necessário ter em conta não apenas o conteúdo das normas aplicáveis aos dados pessoais transferidos para um país terceiro ou organização internacional, mas também o sistema existente para assegurar a eficácia dessas normas. A existência de mecanismos executórios eficientes é extremamente importante para a eficácia das normas de proteção de dados.

O artigo 45.º, n.º 2, do RGPD estabelece os elementos que a Comissão Europeia deve ter em conta ao avaliar a adequação do nível de proteção num país terceiro ou organização internacional.

Por exemplo, a Comissão deve tomar em consideração o primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação vigente na matéria, a existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes e os compromissos internacionais assumidos pelo país terceiro ou organização internacional.

Por conseguinte, fica claro que qualquer análise significativa do nível de proteção adequado deve englobar dois elementos básicos: o conteúdo das normas aplicáveis e a forma como é assegurada a sua aplicação efetiva. Cabe à Comissão Europeia verificar, periodicamente, se as normas vigentes são eficazes na prática.

O «essencial» dos princípios relativos ao «conteúdo» no que toca à proteção de dados e dos requisitos «processuais/de execução», que pode ser visto como um requisito mínimo para a proteção de dados ser adequada, advém da Carta dos Direitos Fundamentais da União Europeia e do RGPD. Além disso, também importa ter em consideração outros acordos internacionais em matéria de proteção de dados, por exemplo, a Convenção n.º 108⁹.

Importa igualmente ter em atenção o quadro normativo de acesso das autoridades públicas a dados pessoais. São fornecidas orientações adicionais no documento de trabalho WP237 (ou seja, o documento sobre as garantias essenciais)¹⁰ sobre as salvaguardas no contexto da supervisão.

A existência de disposições gerais de proteção de dados e privacidade no país terceiro não é suficiente. Pelo contrário, o quadro normativo do país terceiro ou organização internacional deve

⁶ Processo C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 de outubro de 2015 (n.ºs 73 e 74).

⁷ Artigo 288.º, n.º 2, do TFUE.

⁸ Processo C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 de outubro de 2015 (n.º 52).

⁹ Considerando 105 do RGPD.

¹⁰ Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237, 13 de abril de 2016. [Documento disponível apenas na versão inglesa].

incluir disposições específicas que regulem necessidades concretas relativas a aspetos práticos pertinentes do direito à proteção de dados. Estas disposições devem ter caráter executório.

Capítulo 2: Aspetos processuais das decisões de adequação ao abrigo do RGPD

Para o Comité Europeu para a Proteção de Dados (CEPD) cumprir as funções de aconselhamento à Comissão Europeia de acordo com o artigo 70.º, n.º 1, alínea s), do RGPD, o CEPD deve receber toda a documentação pertinente, incluindo correspondência pertinente e conclusões formuladas pela Comissão Europeia. Se o quadro normativo for complexo, importa incluir qualquer relatório preparado sobre o nível de proteção de dados do país terceiro ou organização internacional. Em todo o caso, as informações da Comissão Europeia devem ser exaustivas e permitir que o CEPD possa proceder à sua própria avaliação do nível de proteção de dados no país terceiro. O CEPD emitirá um parecer sobre as conclusões da Comissão Europeia em tempo útil e identificará eventuais insuficiências no âmbito da adequação. O CEPD procurará igualmente propor alterações ou modificações com vista a dar resposta às eventuais insuficiências.

De acordo com o artigo 45.º, n.º 4, do RGPD, cabe à Comissão Europeia controlar, de forma continuada, os desenvolvimentos que possam prejudicar a aplicação de uma decisão de adequação.

O artigo 45.º, n.º 3, do RGPD prevê a realização de uma avaliação periódica, no mínimo de quatro em quatro anos. Contudo, trata-se de um intervalo temporal geral que deve ser ajustado a cada país terceiro ou organização internacional com uma decisão de adequação. Dependendo das circunstâncias específicas em causa, pode justificar-se um ciclo de revisão mais curto. Além disso, alguns incidentes ou outras informações ou alterações do quadro normativo do país terceiro ou organização internacional em causa podem levar à necessidade de proceder a uma revisão antes da data prevista. Parece também ser adequado realizar a primeira revisão de uma decisão de adequação totalmente nova bastante cedo e, gradualmente, ajustar o ciclo de revisão em função dos resultados.

Atendendo ao mandato de dar à Comissão Europeia um parecer quanto ao facto de um país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou uma organização internacional, ter deixado de garantir um nível adequado de proteção, o CEPD deve, oportunamente, receber informações úteis em relação ao seguimento, por parte da Comissão Europeia, dos desenvolvimentos nesse país terceiro ou organização internacional. Como tal, o CEPD deve ser informado de qualquer processo de revisão e missão de revisão no país terceiro ou organização internacional. O CEPD gostaria de ser convidado a participar nestes processos e missões de revisão.

Importa também referir que, de acordo com o artigo 45.º, n.º 5, do RGPD, a Comissão Europeia tem direito a revogar, alterar ou suspender decisões de adequação existentes. O processo de revogação, alteração ou suspensão deve, consequentemente, incluir a participação do CEPD, uma vez que o seu parecer é necessário nos termos do artigo 70.º, n.º 1, alínea s).

Além disso, como passou a ser reconhecido no artigo 58.º, n.º 5, do RGPD e de acordo com o acórdão do TJUE no processo Schrems, as autoridades de proteção de dados devem poder intentar processos judiciais se considerarem bem fundamentada a reclamação de uma pessoa contra uma decisão de adequação: *«[...] incumbe ao legislador nacional prever vias de recurso que permitam à autoridade nacional de controlo em causa invocar as críticas que considera fundadas perante os órgãos jurisdicionais nacionais, para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão da Comissão, procedam a um reenvio prejudicial para efeitos da apreciação da validade dessa decisão.»*¹¹

¹¹ Processo C-362/14, Maximilian Schrems/Data Protection Commissioner, 6 de outubro de 2015 (n.º 65).

Capítulo 3: Princípios gerais de proteção de dados para assegurar que o nível de proteção num país terceiro, num território ou num ou mais setores específicos desse país terceiro ou numa organização internacional é substancialmente equivalente ao estabelecido na legislação da UE

O sistema de um país terceiro ou organização internacional deve conter os seguintes princípios e mecanismos básicos relativos ao conteúdo e aos requisitos processuais/de execução em matéria de proteção de dados:

A. Princípios relativos ao conteúdo:

1) Conceitos

Devem existir conceitos e/ou princípios básicos em matéria de proteção de dados. Estes não têm de imitar a terminologia do RGPD, mas devem refletir e ser coerentes com os conceitos consagrados na legislação europeia em matéria de proteção de dados. A título de exemplo, o RGPD inclui os seguintes conceitos importantes: «dados pessoais», «tratamento dos dados pessoais», «responsável pelo tratamento dos dados», «subcontratante», «destinatário» e «dados sensíveis».

2) Fundamento para o tratamento lícito e leal para fins legítimos

Os dados devem ser tratados de forma lícita, leal e legítima.

Os fundamentos legítimos, ao abrigo dos quais os dados pessoais podem ser tratados lícita, leal e legitimamente, devem ser estabelecidos de forma suficientemente clara. O quadro europeu reconhece vários desses fundamentos legítimos, nomeadamente disposições do direito nacional, o consentimento do titular dos dados, a execução de um contrato ou o interesse legítimo do responsável pelo tratamento dos dados ou de um terceiro que não se sobrepõe aos interesses individuais.

3) Princípio da limitação da finalidade do tratamento

Os dados devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento.

4) Princípio da qualidade e proporcionalidade dos dados

Os dados devem ser exatos e, quando necessário, objeto de atualização. Os dados devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados.

5) Princípio da conservação de dados

Regra geral, os dados não devem ser conservados mais tempo do que o necessário para as finalidades para as quais são tratados.

6) Princípio da segurança e da confidencialidade

Qualquer entidade que proceda ao tratamento de dados pessoais deve assegurar que os dados são tratados de modo a garantir a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou

organizativas adequadas. O nível de segurança deve ter em consideração o estado atual dos conhecimentos e os custos conexos.

7) Princípio da transparência

Todos os titulares devem ser informados de todos os principais elementos do tratamento dos seus dados pessoais de forma clara, facilmente acessível, concisa, transparente e inteligível. As referidas informações devem incluir a finalidade do tratamento, a identidade do responsável pelo tratamento de dados, os direitos à sua disposição e outras informações, uma vez que tal é necessário para assegurar a lealdade. Em determinadas condições, podem existir algumas exceções a este direito de informação, designadamente para acautelar investigações penais, a segurança nacional, a independência judicial e processos judiciais ou outros objetivos importantes de interesse público geral, como é o caso do artigo 23.º do RGPD.

8) Direito de acesso, retificação, apagamento e oposição

O titular dos dados deve ter o direito de obter confirmação do eventual tratamento dos dados que lhe dizem respeito, bem como de aceder a esses dados, nomeadamente obtendo cópia de todos os dados que lhe dizem respeito que são objeto de tratamento.

O titular dos dados deve ter o direito de obter a retificação dos seus dados consoante adequado, por razões específicas, por exemplo quando estes estiverem incorretos ou incompletos, e o apagamento dos seus dados pessoais quando, por exemplo, o seu tratamento deixar de ser necessário ou for ilícito.

O titular dos dados deve também ter o direito de se opor, por motivos legítimos imperiosos relacionados com a sua situação particular, a qualquer momento, ao tratamento dos seus dados em condições específicas estabelecidas no quadro normativo do país terceiro. No RGPD, por exemplo, essas condições incluem situações em que o tratamento for necessário para a realização de uma tarefa executada com base no interesse público, ou para o exercício de autoridade oficial investida no responsável pelo tratamento, ou em que o tratamento é necessário para efeitos dos interesses legítimos do responsável pelo tratamento ou por terceiro.

O exercício desses direitos não deve ser excessivamente complexo para o titular dos dados. Podem existir exceções a estes direitos, nomeadamente para acautelar investigações penais, a segurança nacional, a independência judicial e processos judiciais ou outros objetivos importantes de interesse público geral, como é o caso do artigo 23.º do RGPD.

9) Restrições relativas a transferências subsequentes

Outras transferências dos dados pessoais por parte do destinatário inicial da transferência de dados original só devem ser permitidas se o destinatário seguinte (ou seja, o destinatário da transferência subsequente) também estiver sujeito a normas (incluindo normas contratuais) que garantam um nível de proteção adequado e seguir as instruções pertinentes aquando do tratamento de dados em nome do responsável pelo tratamento dos dados. O nível de proteção das pessoas singulares cujos dados são transferidos não deve ser prejudicado pela transferência subsequente. O destinatário inicial dos dados transferidos a partir da UE é responsável por assegurar que existem salvaguardas adequadas no que toca às transferências subsequentes de dados na ausência de uma decisão de adequação. Algumas transferências subsequentes só devem ocorrer para finalidades limitadas e específicas, e desde que existam fundamentos jurídicos para o tratamento em causa.

B. Exemplos de princípios adicionais relativos ao conteúdo que devem ser aplicados a tipos específicos de tratamento:

1) Categorias especiais de dados

Devem existir salvaguardas específicas aplicáveis a categorias especiais de dados¹². Estas categorias devem refletir as que se encontram previstas nos artigos 9.º e 10.º do RGPD. Esta proteção deve ser aplicada mediante requisitos mais exigentes em matéria de tratamento de dados, como por exemplo o consentimento explícito do titular dos dados, ou medidas de segurança adicionais.

2) Comercialização direta

Se os dados forem tratados para efeitos de comercialização direta, o titular deve poder opor-se sem qualquer custo ao tratamento dos dados para essa finalidade, em qualquer momento.

3) Decisões automatizadas e definição de perfis

As decisões baseadas unicamente no tratamento automatizado (decisões individuais automatizadas), incluindo definição de perfis, que produzem efeitos jurídicos ou afetam significativamente o titular dos dados, só podem ser tomadas nas condições fixadas no quadro normativo do país terceiro. No quadro europeu, as referidas condições incluem, por exemplo, a necessidade de obter consentimento explícito do titular dos dados ou a necessidade dessa decisão para a celebração do contrato. Caso a decisão não esteja em conformidade com as condições fixadas no quadro normativo do país terceiro, o titular dos dados deve ter o direito de não estar sujeito a nenhuma dessas decisões. O direito do país terceiro deve, em todo o caso, prever as salvaguardas necessárias, incluindo o direito de ser informado dos motivos subjacentes à decisão e da lógica em questão, por forma a corrigir informações erradas ou incompletas e contestar a decisão caso esta tenha sido tomada com base em factos incorretos.

C. Mecanismos processuais e de aplicação efetiva:

Embora os meios aos quais o país terceiro recorre para assegurar um nível de proteção adequado possam diferir dos meios empregues na União Europeia¹³, um sistema coerente com o europeu deve caracterizar-se pela existência dos seguintes elementos:

1) Autoridade de controlo competente e independente

Deve existir uma ou mais autoridades de controlo independentes, responsáveis pelo seguimento e por assegurar e aplicar a conformidade com as disposições de proteção de dados e privacidade no país terceiro. A autoridade de controlo deve atuar com total independência e imparcialidade quando desempenha as suas funções e exerce os seus poderes, não devendo procurar nem aceitar instruções para o fazer. Nesse contexto, a autoridade de controlo deve ter à sua disposição todos os poderes e mandatos necessários para assegurar a conformidade com os direitos ligados à proteção de dados e promover a sensibilização. Importa também ter em conta o pessoal e o orçamento da autoridade de controlo. A autoridade de controlo deve igualmente ter meios para realizar inquéritos por iniciativa própria.

2) O sistema de proteção de dados deve assegurar um bom nível de conformidade

¹² Estas categorias especiais são designadas também como «dados sensíveis» no considerando 10 do RGPD.

¹³ Processo C-362/14, Maximilian Schrems/Data Protection Commissioner, 6 de outubro de 2015 (n.º 74).

O sistema do país terceiro deve assegurar um nível elevado de responsabilização e de sensibilização entre os responsáveis pelo tratamento e aqueles que tratam dados pessoais em seu nome em relação aos seus deveres, funções e responsabilidades, bem como entre os titulares dos dados em relação aos seus direitos e aos modos de exercício desses direitos. A existência de sanções efetivas e dissuasivas é uma forma importante de assegurar o cumprimento das normas, assim como os sistemas de controlo direto por autoridades, auditores ou funcionários independentes encarregados da proteção de dados.

3) Responsabilização

O quadro de proteção de dados do país terceiro deve obrigar os responsáveis pelo tratamento dos dados e/ou aqueles que tratam dados pessoais em seu nome a cumprir esse mesmo quadro e conseguir comprovar esse cumprimento, em especial junto da autoridade de controlo competente. Tais medidas podem incluir, por exemplo, a avaliação de impacto sobre a proteção de dados, a conservação de registos ou arquivos das atividades de tratamento de dados durante um período de tempo adequado, a designação de um responsável pela proteção de dados ou a proteção de dados desde a conceção e por defeito.

4) O sistema de proteção de dados deve prever apoio e ajuda destinada aos titulares de dados no exercício dos seus direitos e mecanismos de reparação adequados

As pessoas singulares devem ter acesso a vias de recurso para fazer valer os seus direitos rápida e eficazmente, e sem custos proibitivos, bem como assegurar a conformidade. Para tal, devem existir mecanismos de controlo que permitam a realização de investigações independentes acerca das reclamações e a identificação e punição de quaisquer violações do direito à proteção de dados e respeito pela vida privada.

Se as regras não forem cumpridas, o titular dos dados deve também deve dispor de vias de recurso eficazes, administrativas e judiciais, incluindo indemnizações em resultado do tratamento ilícito dos seus dados pessoais. Trata-se de um elemento crucial, que pressupõe um sistema de apreciação independente ou de arbitragem, que possa decidir a atribuição de uma indemnização e a eventual aplicação de sanções.

Capítulo 4: Garantias essenciais em países terceiros em relação ao acesso para fins de aplicação coerciva da lei e segurança nacional, para limitar interferências nos direitos fundamentais

Ao avaliar a adequação do nível de proteção nos termos do artigo 45.º, n.º 2, alínea a), a Comissão deve ter em conta *«legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação [...]»*.

O TJUE, no processo Schrems, referiu que *«a expressão “nível de proteção adequado” deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União nos termos da Diretiva 95/46, lida à luz da Carta»*. Ainda que, a este respeito, os meios a que esse país recorre possam ser diferentes dos implementados dentro da União, tais meios devem, todavia, revelar-se eficazes na prática¹⁴.

Neste contexto, o tribunal também referiu criticamente que a anterior decisão relativa ao porto seguro *«não contém qualquer referência à existência, nos Estados Unidos, de normas de caráter estatal destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados pessoais sejam transferidos da União para os Estados Unidos, ingerências essas que as autoridades estatais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional»*.

O GT29 identificou no seu parecer WP237, adotado em 13 de abril de 2016, garantias essenciais que refletem a jurisprudência do TJUE e da TEDH no domínio da vigilância. Ainda que as recomendações que constam do documento WP237 continuem válidas e devam ser tidas em conta ao avaliar a adequação de um país terceiro no domínio da vigilância, a aplicação dessas garantias pode diferir nos domínios do acesso aos dados para fins de execução coerciva da lei e segurança nacional. Ainda assim, as quatro garantias indicadas devem ser respeitadas quando se trata de acesso aos dados, seja para fins de segurança nacional seja para fins de execução coerciva da lei, por todos os países terceiros para que esse acesso seja considerado adequado:

- 1) O tratamento deve basear-se em regras claras, precisas e acessíveis (base jurídica)**
- 2) A necessidade e a proporcionalidade relativamente aos objetivos legítimos prosseguidos devem ser demonstradas**
- 3) O tratamento tem de estar sujeito a supervisão independente**
- 4) Devem existir meios de recurso eficazes ao dispor das pessoas singulares**

¹⁴ Processo C-362/14, Maximilian Schrems/Data Protection Commissioner, 6 de outubro de 2015 (n.º 74).