Parecer da Autoridade Europeia para a Protecção de Dados sobre a comunicação da Comissão sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros

(2010/C 357/02)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [1],

Tendo em conta o pedido de parecer apresentado nos termos do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, nomeadamente o artigo 41.º [2],

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Consulta da AEPD

1. Em 21 de Setembro de 2010, a Comissão adoptou uma comunicação sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros [3]. Essa comunicação foi enviada à AEPD para consulta no mesmo dia.

2. A AEPD congratula-se com o facto de ter sido consultada pela Comissão. Antes da adopção da comunicação, já lhe tinha sido oferecida a possibilidade de formular observações informais. Algumas dessas observações foram tidas em conta na versão final do documento, embora outros aspectos continuem a suscitar preocupação no que respeita à protecção dos dados.

2. A proposta no seu contexto

3. A abordagem global às questões em matéria de PNR que a Comissão apresenta na sua comunicação pretende estabelecer um quadro coerente relativo à transferência de dados PNR para os países terceiros. Para além da necessidade de segurança jurídica desenvolvida na comunicação, esta abordagem harmonizada também recebeu um forte apoio do Parlamento Europeu, ao qual o novo quadro institucional confia a competência de ratificar acordos PNR com países terceiros [4].

4. A comunicação é complementada por recomendações com vista à negociação de acordos PNR com países terceiros específicos. Essas recomendações são restritas e não são analisadas no presente parecer. Contudo, a relação entre a comunicação geral e as recomendações é objecto de algumas observações no capítulo II.

5. Para além da abordagem global à transferência de dados PNR para países terceiros, a Comissão também está a elaborar uma abordagem revista em matéria de PNR para a UE. Uma proposta para um tal quadro da UE já tinha sido intensamente debatida no Conselho, no âmbito do antigo terceiro pilar, antes da entrada em vigor do Tratado de Lisboa [5]. Esses debates não permitiram chegar a um consenso sobre vários elementos essenciais do sistema PNR, como, por exemplo, a utilização da base de dados criada ao abrigo desse sistema. O Programa de Estocolmo instou então a Comissão a apresentar uma nova proposta, mas não focou os elementos essenciais da mesma. A apresentação de uma proposta de directiva relativa a um sistema PNR da UE está prevista para o início de 2011.

6. O presente parecer centra-se na comunicação da Comissão. Na primeira parte, analisa a comunicação no contexto da actual evolução no domínio da protecção de dados, na segunda parte, aborda a legitimidade do sistema PNR e na terceira centra-se nas questões mais específicas de protecção de dados contidas na comunicação.

[1] JO L 281 de 23.11.1995, p. 31.
[2] JO L 8 de 12.1.2001, p. 1.
[3] COM(2010) 492 final.

[4] Foram assinados acordos com:
— Os Estados Unidos: Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento (Acordo PNR 2007) (JO L 204 de 4.8.2007, p. 18);
— O Canadá: Acordo entre a Comunidade Europeia e o Governo do Canadá sobre o tratamento dos dados relativos às informações antecipadas sobre os passageiros e aos registos de identificação dos passageiros (JO L 82 de 21.3.2006, p. 15);
— A Austrália: Acordo entre a União Europeia e a Austrália sobre o tratamento de dados originários da União Europeia contidos nos Registos de Identificação dos Passageiros (PNR) e a transferência desses dados pelas transportadoras aéreas para os serviços aduaneiros da Austrália (JO L 213 de 8.8.2008, p. 49-57).

[5] Em 6 de Novembro de 2007, a Comissão adoptou uma proposta de decisão-quadro relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name record* — PNR) para efeitos de aplicação da lei [COM(2007) 654 final]. A AEPD apresentou o seu parecer sobre esta proposta em 20 de Dezembro de 2007 (JO C 110 de 1.5.2008, p. 1).

II. ANÁLISE DA PROPOSTA

1. Observações gerais

7. A AEPD congratula-se com a abordagem horizontal da comunicação, consentânea com os recentes pedidos do Parlamento Europeu para que se realize uma análise minuciosa e se elabore uma perspectiva coerente dos sistemas PNR existentes e previstos. Um nível elevado e harmonizado de protecção aplicável a todos estes sistemas é um objectivo que deve ser fortemente apoiado.

8. A AEPD questiona, todavia, o calendário geral das diversas iniciativas directa ou indirectamente relacionadas com o tratamento dos dados PNR.

9. Embora a comunicação mencione os acordos internacionais relativos aos sistemas PNR e a iniciativa com vista a um PNR da UE, as normas propostas na comunicação dizem exclusivamente respeito aos acordos internacionais. O quadro da UE será debatido e desenvolvido posteriormente.

10. Uma agenda mais lógica e oportuna deveria incluir, no entender da AEPD, uma reflexão aprofundada sobre um eventual sistema da UE que contivesse garantias de protecção de dados conformes com o quadro jurídico da UE, e desenvolver, nesta base, uma abordagem para os acordos com países terceiros.

11. A AEPD também destaca o trabalho em curso relativo a um acordo geral entre a UE e os EUA sobre a partilha de dados para efeitos de aplicação da lei [1], cujo objectivo é estabelecer um conjunto de princípios que garantam um nível elevado de protecção dos dados pessoais como condição para o intercâmbio desses dados com os Estados Unidos. Os resultados das negociações entre a UE e os EUA deveriam servir de referência a futuros acordos bilaterais celebrados pela União Europeia e os seus Estados-Membros, incluindo o acordo PNR entre a UE e os EUA.

12. Outro elemento a tomar em consideração neste contexto é a reflexão geral sobre o quadro de protecção de dados da UE, que está a ser conduzida pela Comissão, tendo em vista a apresentação de uma comunicação antes de finais de 2010, a que se deverá seguir uma proposta de novo quadro regulamentar em 2011 [2]. Este processo de revisão tem lugar no quadro «pós-Lisboa», que tem um impacto directo na aplicação horizontal dos princípios de protecção de dados aos antigos pilares da UE, incluindo a cooperação policial e judiciária em matéria penal.

13. Para garantir a coerência, a UE deve chegar a acordo sobre os seus instrumentos internos e, com base nestes instrumentos, negociar acordos com países terceiros. A agenda global deve começar, assim, por se concentrar no quadro geral de protecção de dados da UE, depois na eventual necessidade de um sistema PNR da UE e, por último, nas condições para o intercâmbio de dados com países terceiros, com base no quadro da UE actualizado. Nesta fase, as garantias previstas num futuro acordo UE-EUA também devem ser tidas em conta aquando do estabelecimento das condições de transferência de dados PNR para países terceiros.

14. A AEPD está ciente do facto de que, por diversas razões processuais e políticas, esta ordem ideal não está a ser seguida na prática. Considera, no entanto, que a lógica subjacente a estas diversas etapas não deve ser esquecida pelos diversos intervenientes da Comissão, do Conselho e do Parlamento. Dado que estes processos, nomeadamente em relação ao quadro da UE e às negociações UE-EUA, estão a progredir em paralelo, há que ter devidamente em conta essa necessidade de coerência e de uma perspectiva harmonizada sobre as garantias de protecção de dados na UE e no contexto das transferências. Em concreto, isto implicaria, nomeadamente:

— Ter em conta os resultados da avaliação de impacto relativa ao PNR da UE antes de finalizar quaisquer negociações PNR com países terceiros;

— Garantir que se retiram ensinamentos das revisões dos acordos PNR actuais;

— E, no que diz respeito às negociações com os Estados Unidos, ligar as negociações relativas ao PNR com as referentes ao acordo geral sobre a partilha de dados para efeitos de aplicação da lei. Só assim se poderá assegurar a existência de garantias coerentes em ambos os acordos.

15. Por último, a AEPD levanta a questão da ligação entre a comunicação e as orientações elaboradas pela Comissão. Trata-se de saber em que medida se devem especificar garantias e condições precisas nas normas desenvolvidas na comunicação ou nas orientações estabelecidas por país: se o objectivo global é harmonizar as condições de tratamento e intercâmbio de dados PNR, a AEPD considera que a margem de manobra para cada acordo internacional deve ser o mais limitada possível e que as normas devem estabelecer um quadro preciso. As normas devem ter um impacto efectivo no conteúdo dos acordos. Várias observações a seguir apresentadas exigem mais precisão nesse sentido.

---

[1] Ver, nomeadamente, a consulta lançada pela Comissão em Janeiro de 2010 sobre o futuro acordo internacional entre a União Europeia (UE) e os Estados Unidos da América (EUA) sobre a protecção dos dados pessoais e a partilha de informações para efeitos de aplicação da lei, e os contributos do Grupo de Trabalho do artigo 29.º e da AEPD, que podem ser encontrados no endereço Internet: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0005_en.htm

[2] A Comissão lançou um processo de revisão do actual quadro jurídico, que principiou com uma conferência de alto nível em Maio de 2009. Subsequentemente, realizou-se uma consulta pública até ao final de 2009 e várias reuniões de consulta das partes interessadas em Julho de 2010. A contribuição do Grupo de Trabalho do artigo 29.º, na qual a AEPD participou activamente, está disponível no seguinte endereço Internet: http://ec.europa.eu/justice/policies//privacy/workinggroup/wpdocs/index_en.htm#general_issues

2. **Legitimidade do sistema**

16. A AEPD e o Grupo de Trabalho do artigo 29.º já insistiram, em vários pareceres ([1]) que é necessário justificar claramente o desenvolvimento dos sistemas PNR, quer no âmbito da UE quer para o intercâmbio de dados com países terceiros. A necessidade das medidas deve ser determinada e sustentada por provas concretas, e depois avaliada e ponderada face ao grau de invasão da vida privada das pessoas, a fim de garantir um resultado proporcional e o menos invasivo possível. O facto de a recente evolução tecnológica ter tornado esse acesso e análise possíveis, como é afirmado no fim do ponto 2.2 da comunicação, não é em si mesmo uma justificação para o desenvolvimento de um sistema que visa rastrear todos os viajantes. Por outras palavras: a disponibilidade de meios não deve justificar os fins.

17. Como é a seguir explicado, a AEPD considera que a transferência em bloco de dados sobre pessoas inocentes para efeitos de avaliação dos riscos suscita graves questões de proporcionalidade. A AEPD questiona em particular a utilização pró-activa de dados PNR. Enquanto a utilização «reactiva» dos dados não causa preocupações de maior, desde que faça parte da investigação de um crime já cometido, a utilização em tempo real e pró-activa suscita uma avaliação mais crítica.

18. Nos termos da comunicação, mesmo no contexto «em tempo real», os dados PNR serão utilizados «para fins de prevenção da criminalidade, vigilância ou detenção de pessoas antes da prática de um crime», com base em «indicadores pré-determinados baseados no risco» ([2]). A ideia principal de tomar medidas em relação às pessoas, antes de um crime ter sido cometido, com base em indicadores de risco é, no entender da AEPD, uma medida pró-activa, cuja utilização num contexto de aplicação da lei é tradicionalmente definida e limitada de forma rigorosa.

19. Além disso, nem a noção de indicadores de risco nem a noção de «avaliação do risco» estão suficientemente desenvolvidas, e a segunda pode ser facilmente confundida com a noção de «caracterização». Esta semelhança é mesmo reforçada pelo alegado objectivo de criar «padrões de viagem e de comportamento geral». A AEPD põe em questão o nexo entre os dados iniciais e os padrões deduzidos desses dados. O processo visa impor a uma pessoa uma avaliação do risco — e possivelmente medidas coercivas — com base em dados que não estão relacionados com essa pessoa. Como já foi afirmado no seu parecer anterior sobre uma proposta de PNR da UE, a principal preocupação da AEPD prende-se com o facto de as «decisões relativas a pessoas serem tomadas com base em padrões e critérios estabelecidos utilizando os dados sobre passageiros em geral. Assim sendo, as decisões relativas a uma pessoa poderão ser tomadas, tomando como referência (pelo menos parcialmente) padrões derivados dos dados de outras pessoas. É portanto com referência a um contexto abstracto que serão tomadas decisões que podem afectar grandemente as pessoas em causa. É extremamente difícil para um indivíduo defender-se contra tais decisões» ([3]).

20. A utilização dessas técnicas em grande escala, envolvendo o rastreio de todos os passageiros suscita, por isso, sérias questões de conformidade com os princípios fundamentais de privacidade e protecção de dados, nomeadamente os estabelecidos no artigo 8.º da CEDH, nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE e no artigo 16.º do TFUE.

21. Qualquer decisão final sobre a legitimidade dos sistemas PNR deve ter em conta estes elementos, que devem ser analisados e desenvolvidos na avaliação de impacto realizada no âmbito do projecto PNR da UE. A agenda deve ser estabelecida de modo a permitir uma análise cuidadosa dos resultados desta avaliação na elaboração dos requisitos globais dos sistemas PNR.

3. **Conteúdo das normas propostas**

22. Sem prejuízo das observações de fundo precedentes sobre a legitimidade dos sistemas PNR, a AEPD congratula-se com a extensa lista de normas, visivelmente inspiradas pelos princípios de protecção de dados da UE, que em vários aspectos deverão reforçar a protecção prevista nos acordos específicos. O valor acrescentado e as insuficiências identificadas nessas normas são a seguir analisados.

Adequação e carácter vinculativo de qualquer acordo

23. A AEPD entende da redacção da comunicação que a avaliação da adequação se pode basear no quadro geral de protecção dos dados do país destinatário ou ser contextual, dependendo dos compromissos juridicamente vinculativos contidos num acordo internacional aplicável ao tratamento dos dados pessoais. Considerando o papel decisivo dos acordos internacionais relativamente às avaliações da adequação, a AEPD sublinha a necessidade de estabelecer claramente o carácter vinculativo dos acordos para todas as partes envolvidas e considera que este deve ser complementado por uma indicação explícita de que os acordos garantem direitos directamente aplicáveis para as pessoas em causa. A AEPD considera que estes elementos constituem um aspecto essencial da avaliação da adequação.

Âmbito e finalidade

24. Os primeiros dois pontos da lista de princípios referem-se à limitação da finalidade. No subtítulo «utilização dos dados», o primeiro ponto menciona os efeitos repressivos e de

([1]) Parecer da AEPD, de 20 de Dezembro de 2007, sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei (JO C 110 de 1.5.2008, p. 1). Os pareceres do Grupo de Trabalho do artigo 29.º estão disponíveis no seguinte endereço Internet: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

([2]) Página 4 da comunicação, capítulo 2.1.

([3]) Parecer de 20 de Dezembro de 2007 sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei (JO C 110 de 1.5.2008, p. 4).

segurança, referindo depois o terrorismo e outra criminalidade transnacional grave, tendo por base «a abordagem» das definições estabelecidas em instrumentos da UE. A AEPD põe em causa esta redacção, que poderia sugerir a ideia de que os futuros acordos não seriam baseados com precisão nessas definições, mas apenas inspiradas por elas. É essencial, por razões de segurança jurídica, que o terrorismo e a criminalidade transnacional grave sejam definidos de forma precisa e que os instrumentos da UE referidos na comunicação sejam identificados. Além disso, a AEPD recorda que, antes de os diferentes tipos de crimes serem incluídos no sistema PNR, devem ser previamente considerados necessários e proporcionais.

25. O segundo ponto parece referir-se mais ao âmbito (a natureza dos dados recolhidos) do que ao princípio da finalidade. A AEPD constata que a comunicação não inclui uma lista dos dados que podem ser objecto de intercâmbio, uma vez que deixa a cada acordo específico a determinação das categorias de dados a transferir. Para evitar divergências e a inclusão de categorias de dados desproporcionadas em alguns acordos com países terceiros, a AEPD considera que às normas deve ser adicionada uma lista comum e exaustiva de categorias de dados, consentânea com a finalidade do intercâmbio de dados. Recorda os pareceres do Grupo de Trabalho do artigo 29.º a este respeito, os quais indicam as categorias de dados que seriam admissíveis e aquelas que são consideradas excessivas em relação aos direitos fundamentais das pessoas em causa ([1]). As categorias de dados a excluir são, nomeadamente, aquelas que podem ser consideradas como dados sensíveis — e que estão protegidas pelo artigo 8.º da Directiva 95/46/CE, os dados SSR/SSI (informações sobre pedidos de serviços especiais/informações de serviços especiais), os dados OSI (outras informações de serviços), os campos em aberto ou de texto livre (como as «observações gerais», onde podem figurar dados de natureza sensível), e as informações relativas aos passageiros frequentes e aos «dados de comportamento».

Dados sensíveis

26. A comunicação afirma que os dados sensíveis não devem ser utilizados, salvo em circunstâncias excepcionais. A AEPD lamenta esta excepção. Considera que as condições da excepção são excessivamente amplas e não dão quaisquer garantias: a utilização dos dados caso a caso apenas é apresentada a título de exemplo; além disso, a limitação da finalidade deve ser um princípio geral aplicável a qualquer tratamento de dados PNR e não uma garantia apenas aplicável aos dados sensíveis. A AEPD considera que a autorização do tratamento de dados sensíveis, mesmo em casos limitados, nivelaria a protecção de todos os sistemas PNR pelo sistema menos conforme com a protecção de dados e não pelo mais conforme. Exorta, por isso, à exclusão total do tratamento de dados sensíveis, como princípio.

Segurança dos dados

27. A obrigação geral de segurança desenvolvida na comunicação é considerada satisfatória. A AEPD entende, no entanto, que poderia ser complementada por uma obrigação de informação mútua em caso de violação da segurança: os destinatários ficariam responsáveis por informar os seus congéneres caso os dados recebidos tivessem sido objecto de divulgação ilegal. Essa obrigação contribuirá para aumentar a responsabilidade em relação a um tratamento seguro dos dados.

Aplicação da lei

28. A AEPD apoia o sistema de supervisão previsto na comunicação, incluindo as medidas de fiscalização e responsabilidade. O direito de cada indivíduo a vias de recurso administrativo e judicial também é fortemente apoiado. Quanto aos direitos de acesso, a AEPD entende que não podem ser previstas limitações, o que é positivo. Caso seja necessária uma limitação em casos excepcionais, o seu âmbito preciso e as garantias necessárias, incluindo nomeadamente um direito de acesso indirecto, devem ser claramente mencionados nas normas.

Transferências ulteriores

29. A AEPD manifesta satisfação pela restrição das transferências ulteriores à revelação caso a caso, seja a outras autoridades governamentais ou a países terceiros. Considera que, complementarmente a este princípio, a limitação da finalidade aplicável às transferências para países terceiros também deve ser aplicada às transferências, dentro do país terceiro, para outras autoridades governamentais. Prevenir-se-ia, assim, qualquer utilização posterior ou o cruzamento dos dados PNR com informações tratadas para fins diferentes. A AEPD está preocupada, em especial, com o risco de cruzamento dos dados com informações provenientes de outras bases de dados, como a do ESTA, no que respeita aos Estados Unidos. Faz notar que a recente decisão dos EUA de exigir uma taxa pela utilização do ESTA leva à recolha de informações sobre os cartões de crédito dos viajantes. A AEPD insta a que se introduza uma limitação clara para impedir a comparação inadequada de informações fora do âmbito do acordo PNR.

Conservação dos dados

30. O período de conservação dos dados não é objecto de uma harmonização eficaz. A AEPD considera que, por princípio, os dados PNR devem ser apagados se os controlos efectuados aquando da sua transmissão não tiverem desencadeado quaisquer medidas de aplicação. Caso o contexto nacional justifique a necessidade de um período de conservação limitado, a AEPD entende que as normas devem estabelecer um período máximo de conservação. Além disso, o princípio de limitação dos direitos de acesso dos funcionários em

([1]) Parecer de 23 de Junho de 2003 sobre o nível de protecção garantido nos Estados Unidos para a transferência dos dados dos passageiros, WP78. Este parecer e os pareceres subsequentes do Grupo de Trabalho sobre esta questão estão disponíveis no endereço Internet: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

termos temporais deve ser reforçado e a anonimização gradual dos dados deve ser considerada como uma obrigação e não como um exemplo.

As modalidades de transmissão

31. A AEPD apoia a utilização exclusiva do sistema de transferência por exportação («push») para transmitir os dados PNR. Insta à adopção de garantias concretas que assegurem que o sistema «push» é efectivamente o único sistema utilizado na prática. A experiência e as inspecções realizadas pelas autoridades de protecção de dados mostraram, na verdade, que não obstante as obrigações previstas nos acordos já em vigor, designadamente em relação ao «PNR EUA», ainda subsiste uma transferência por extracção («pull») residual e que, em paralelo com a transferência por exportação, as autoridades dos EUA têm um acesso mais vasto aos dados PNR através de sistemas informatizados de reserva. Devem ser tomadas medidas jurídicas e técnicas para evitar que o sistema «push» seja contornado.

32. A frequência («razoável») das transmissões de dados pelas companhias aéreas deve ser definida e um número máximo de transmissões estabelecido. Os sistemas actuais que prevêem as disposições mais compatíveis com a privacidade devem constituir o parâmetro de referência para esse exercício.

Conceitos gerais

33. A AEPD também solicita uma maior precisão no que respeita a alguns elementos essenciais da aplicação dos acordos PNR. O período de duração dos acordos («determinado», «necessário») e a sua revisão («periódica») devem ser definidos com maior clareza, numa perspectiva horizontal. A periodicidade das revisões conjuntas, em especial, poderia ser especificada, bem como a obrigação de realizar uma primeira revisão num prazo específico após a entrada em vigor dos acordos: por exemplo, um período máximo de três anos.

III. **CONCLUSÃO**

34. A AEPD congratula-se com a abordagem horizontal que a Comissão apresenta na sua comunicação. Trata-se de um passo fundamental em direcção a um quadro global para o intercâmbio de dados PNR. Algumas preocupações importantes moderam, todavia, esta apreciação geral.

35. Os sistemas PNR apresentados na comunicação não respeitam, só por si, os critérios de necessidade e proporcionalidade desenvolvidos no presente parecer e nos anteriores pareceres da AEPD e do Grupo de Trabalho do artigo 29.º. Para serem admissíveis, as condições de recolha e tratamento de dados pessoais devem ser consideravelmente restringidas. A AEPD está, sobretudo, preocupada com a utilização dos sistemas PNR para efeitos de avaliação dos riscos ou de caracterização.

36. O desenvolvimento de normas PNR deve ter em conta o quadro geral de protecção de dados e a respectiva evolução jurídica na UE, bem como a negociação de acordos de intercâmbio de dados a um nível mais geral, sobretudo com os Estados Unidos. Deve assegurar-se que um futuro acordo com os Estados Unidos sobre o PNR respeitará o acordo geral sobre protecção de dados celebrado com os EUA. Os acordos em matéria de PNR com outros países terceiros também devem ser coerentes com esta abordagem.

37. É essencial que qualquer acordo com países terceiros tenha em conta os novos requisitos de protecção de dados, tal como estão a ser desenvolvidos no quadro institucional «pós-Lisboa».

38. A AEPD insta também a uma maior precisão na abordagem global relativa às garantias mínimas aplicáveis a todos os acordos: devem ser aplicadas condições mais rigorosas, em especial no que diz respeito ao tratamento de dados sensíveis, ao princípio de limitação da finalidade, às condições das transferências ulteriores e à conservação dos dados.

39. Por último, a AEPD insiste no facto de que todos os acordos devem prever direitos directamente aplicáveis para as pessoas em causa. A eficácia dos procedimentos de aplicação, tanto pelas pessoas em causa como pelas autoridades de controlo, é uma condição essencial para se avaliar a adequação de qualquer acordo.

Feito em Bruxelas, em 19 de Outubro de 2010.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados