COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 4.10.2005
COM (2005) 475 final

2005/0202 (CNS)

Proposta de

DECISÃO-QUADRO DO CONSELHO

relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal

{SEC(2005)1241}

(apresentada pela Comissão)

EXPOSIÇÃO DE MOTIVOS

1) CONTEXTO DA PROPOSTA

- **Justificação e objectivos da proposta**

Em 4 de Novembro de 2004, o Conselho Europeu adoptou o Programa da Haia relativo ao reforço da liberdade, da segurança e da justiça na União Europeia[1]. Neste programa, a Comissão é convidada a apresentar propostas, o mais tardar até ao final de 2005, para a aplicação do princípio da disponibilidade, a fim de melhorar a partilha transfronteiras de informações sobre a aplicação da legislação entre os Estados-Membros. O Programa da Haia sublinha que as condições essenciais na área da protecção de dados devem ser rigorosamente cumpridas nestas propostas.

Em Junho de 2005, o Conselho e a Comissão adoptaram o Plano de Acção de aplicação do Programa da Haia[2]. Baseou-se na Comunicação da Comissão ao Conselho e ao Parlamento - O Programa de Haia: dez prioridades para os próximos cinco anos. Parceria para a renovação europeia no domínio da liberdade, segurança e justiça[3]. Segundo o Plano de Acção, a Comissão apresentará *propostas em 2005 sobre 1) a consagração do princípio da disponibilidade no que se refere às informações relevantes em matéria de aplicação da lei e 2) o estabelecimento das salvaguardas adequadas e de vias de recurso eficazes para a transferência de dados pessoais para efeitos de cooperação policial e judiciária em matéria penal.* Em 13 de Julho de 2005, o Conselho (Justiça e Assuntos Internos) na sua Declaração sobre a resposta da UE aos atentados de Londres[4] apelou à Comissão para que esta apresentasse estas propostas até Outubro de 2005.

A presente decisão-quadro garantirá a protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal entre os Estados-Membros da União Europeia (TUE, Título VI). Destina-se a melhorar esta cooperação, em especial no que diz respeito à prevenção e luta contra o terrorismo, e na estrita observância das condições essenciais na área da protecção de dados. Garantirá que os direitos fundamentais, em especial o direito ao respeito pela vida privada e à protecção de dados pessoais, serão respeitados em toda a União Europeia, nomeadamente, a luz da aplicação do princípio da disponibilidade. Garantirá igualmente que o intercâmbio de informações relevantes entre os Estados-Membros não será entravado por níveis diferentes de protecção de dados nos Estados-Membros.

- **Contexto geral**

Na sequência da iniciativa da Itália[5], a protecção dos dados pessoais no âmbito do terceiro pilar fora já discutida em 1998. Nessa ocasião, o Conselho Justiça e Assuntos Internos adoptou o denominado Plano de Acção de Viena[6]. Este determinava que – no que diz respeito aos problemas horizontais no contexto da cooperação policial e judiciária em matéria penal – deviam ser analisadas as possibilidades de adoptar regras harmonizadas sobre a protecção de dados num prazo de dois anos a contar da data de entrada em vigor do Tratado. Todavia, em 2001, não foi possível adoptar[7] um projecto de resolução relativa às regras de protecção dos

---

1 JO C 53 de 3.3.2005, p. 1.
2 JO C 198 de 12.08.2005, p. 1.
3 COM(2005) 184 final, Bruxelas, 10.5.2005.
4 Documento de trabalho do Conselho 11158/1/05 REV 1 JAI 255
5 Documento de trabalho do Conselho 8321/98JAI 15
6 JO C 19 de 23.01.1999, p. 1.
7 Documento de trabalho do Conselho 6316/2/01 REV 2 JAI 13

dados pessoais em instrumentos no âmbito do terceiro pilar da União Europeia. Em Junho de 2003, a Presidência grega propôs um conjunto de princípios gerais em matéria de protecção de dados pessoais no terceiro pilar[8], inspirados na Directiva 95/46/CE sobre a protecção de dados e na Carta dos Direitos Fundamentais da União Europeia. Em 2005, as autoridades competentes em matéria de protecção de dados dos Estados-Membros da União Europeia e a Autoridade Europeia para a Protecção de Dados (a seguir denominada AEPD) defenderam veementemente a adopção de um novo instrumento jurídico para a protecção dos dados pessoais no âmbito do terceiro pilar[9]. O Parlamento Europeu recomendou a harmonização das regras em vigor em matéria de protecção de dados pessoais nos instrumentos do terceiro pilar, reunindo-as num instrumento único, que garanta o mesmo nível de protecção de dados que a assegurada no primeiro pilar[10].

De acordo com o Programa da Haia, a introdução do princípio da disponibilidade depende da adopção de condições essenciais na área da protecção de dados. O Conselho Europeu reconheceu obviamente que as disposições em matéria de protecção de dados actualmente em vigor a nível europeu não seriam suficientes face à aplicação do princípio da disponibilidade, que podia incluir modalidades como o acesso recíproco a bases de dados nacionais ou respectiva interoperabilidade ou o acesso directo (em linha).

As preocupações suscitadas em relação a um nível suficiente de protecção de dados reflectiram-se igualmente num acordo de cooperação assinado por sete Estados-Membros, em 27 de Maio de 2005 em Prüm (Alemanha, Áustria, Bélgica, Países Baixos, Luxemburgo, França e Espanha) e recomendado como modelo para o intercâmbio de informações entre os Estados-Membros da União em geral. O acordo prevê, em determinadas condições específicas, um acesso automatizado directo para as autoridades responsáveis pela aplicação da lei de uma Parte Contratante aos dados pessoais detidos por uma outra Parte Contratante. No entanto, esta forma de cooperação só será aplicável quando as disposições do acordo relativas à protecção de dados tiverem sido transpostas para o direito interno das Partes.

- **Disposições em vigor no domínio da proposta**

A Carta dos Direitos Fundamentais da União Europeia[11] reconhece expressamente o direito ao respeito pela vida privada (artigo 7º) e o direito à protecção dos dados pessoais (artigo 8º). Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

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[12], inclui regras fundamentais sobre a licitude do tratamento de dados pessoais, bem como sobre os direitos da pessoa em causa. Inclui

---

8 2514ª reunião do Conselho Justiça e Assuntos Internos, Luxemburgo, 5-6 de Junho de 2003, Documento do Conselho 9845/03 (Presse 150), p. 32.

9 Declaração e documento de síntese sobre a aplicação da lei e intercâmbios de informações na UE, adoptado pela conferência da Primavera das Autoridades Responsáveis pela Protecção dos Dados, Cracóvia, 25-26 de Abril de 2005.

10 Ponto 1 h) da Recomendação do Parlamento Europeu ao Conselho Europeu e ao Conselho·relativa à troca de informações e à cooperação em matéria de infracções terroristas. (2005/2046(INI)), adoptada em 7 de Junho de 2005.

11 JO C 364 de 18.12.2000, pp. 1,10.

12 JO L 281 de 23.11.1995, p. 31.

disposições relativas a recursos judiciais, responsabilidade e sanções, transferência de dados pessoais para países terceiros, códigos de conduta, autoridades de controlo específicas e um grupo de trabalho e finalmente regras de execução comunitárias. Todavia, a directiva não é aplicável a actividades não abrangidas pelo âmbito do direito comunitário, tal como as previstas no Título VI do Tratado da União Europeia (TUE). Por conseguinte, os Estados-Membros podem decidir eles próprios das normas adequadas para o tratamento e protecção dos dados. No contexto do Título VI do TUE, a protecção de dados pessoais é estabelecida em vários instrumentos específicos, em especial, em instrumentos que estabelecem sistemas de informação comuns a nível europeu, tais como: a Convenção de Aplicação do Acordo de Schengen de 1990 incluindo disposições específicas relativas à protecção dos dados pessoais aplicáveis ao Sistema de Informação de Schengen[13], a Convenção Europol de 1995[14] e, nomeadamente, a regulamentação relativa à transmissão de dados pessoais pela Europol a Estados e organismos terceiros[15], a Decisão de 2002 relativa à criação da Eurojust[16] e as disposições do regulamento interno da Eurojust relativas ao tratamento e à protecção de dados pessoais[17], a Convenção sobre a utilização da informática no domínio aduaneiro de 1995, incluindo disposições relativas à protecção de dados pessoais aplicáveis ao Sistema de Informação Aduaneira[18] e a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia de 2000, em especial o artigo 23º[19]. No que diz respeito ao Sistema de Informação de Schengen, deve ser dada especial atenção ao estabelecimento, funcionamento e utilização do Sistema de Informação de Schengen de segunda geração (SIS II), relativamente ao qual a Comissão já apresentou propostas de uma decisão do Conselho[20] e de dois regulamentos[21].

Além disso, deve ser considerado o artigo 8º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e a Convenção nº 108 do Conselho da Europa relativa à protecção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais de 1981, o seu Protocolo Adicional de 2001, no que respeita às autoridades de controlo e às transferências transfronteiras de dados, e a Recomendação nº R (87) 15 de 1987, que regulamenta a utilização dos dados pessoais no sector da polícia. Todos os Estados-Membros são Parte na Convenção, mas nem todos o são no Protocolo Adicional.

- **Coerência com as outras políticas e objectivos da União**

As especificidades do tratamento e da protecção de dados pessoais no contexto do Título VI do Tratado da União Europeia devem ser reconhecidas. Por um lado, não devem prejudicar a coerência com a política geral da União Europeia no domínio do respeito pela vida privada e da protecção de dados com base na Carta dos Direitos Fundamentais da União Europeia e na Directiva 95/46/CE. Os princípios fundamentais da protecção de dados são aplicáveis ao tratamento de dados no primeiro e terceiro pilares. Além disso, deve ser assegurada a coerência com outros instrumentos que prevêem obrigações específicas relativas às informações susceptíveis de serem relevantes para efeitos da prevenção e luta contra o crime. Deve ser dada atenção à evolução da situação em matéria de conservação dos dados tratados e

---

13 JO L 239 de 22.09.2000, p. 19.
14 JO C 316 de 27.11.1995, p. 2.
15 JO C 88 de 30.03.1999, p. 1.
16 JO L 63 de 06.03.2002, p. 1.
17 JO C 68 de 19.03.2005, p. 1.
18 JO C 316 de 27.11.1995, p. 34.
19 JO C 197 de 12.07.2000, pp. 1, 15.
20 COM(2005) 230 final.
21 COM(2005) 236 final, COM(2005) 237 final.

armazenados no quadro do fornecimento de serviços de comunicações electrónicas acessíveis ao público ou dos dados transmitidos em redes de telecomunicações públicas para efeitos de prevenção, investigação, detecção e repressão de delitos e infracções penais, incluindo o terrorismo. É conveniente fazer uma referência especial à relação estreita que existe entre a presente proposta de decisão-quadro e a proposta da Comissão de uma directiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no quadro do fornecimento de serviços de comunicações electrónicas acessíveis ao público, e que altera a Directiva 2002/58/CE[22].

2) CONSULTA DAS PARTES INTERESSADAS E AVALIAÇÃO DO IMPACTO

- **Consulta das partes interessadas**

Métodos de consulta, principais sectores visados e perfil geral dos inquiridos

Em 22 de Novembro de 2004 e 21 de Junho de 2005, a Comissão convidou e consultou peritos dos governos dos Estados-Membros, da Islândia, da Noruega e da Suíça e, em 11 de Janeiro de 2005, peritos das autoridades competentes em matéria de protecção de dados destes Estados. A AEPD, a Europol, a Eurojust e o Secretariado dos órgãos comuns de controlo da protecção de dados estavam também representados. As consultas tinham por principal objectivo identificar a necessidade de um instrumento jurídico sobre o tratamento e a protecção de dados pessoais no âmbito do terceiro pilar e, em caso afirmativo, qual devia ser o teor de um instrumento desse tipo. A Comissão perguntou às partes consultadas, nomeadamente com base num questionário e num documento de discussão, qual a sua posição relativamente à abordagem geral de um novo instrumento jurídico e a sua relação com os instrumentos existentes, a base jurídica, o eventual âmbito, os princípios relativos à qualidade dos dados, os critérios relativos à legitimidade do tratamento dos dados pelas autoridades policiais ou judiciárias, os dados pessoais de não suspeitos, os requisitos para a transmissão de dados pessoais a autoridades competentes de outros Estados-Membros e de países terceiros, os direitos da pessoa em causa, autoridades de controlo e um eventual órgão consultivo para a protecção dos dados no terceiro pilar.

O grupo de trabalho criado ao abrigo do artigo 29º da Directiva 95/46/CE foi periodicamente informado da evolução em curso. Em 12 de Abril e 21 de Junho de 2005, a Comissão assistiu a reuniões do grupo de trabalho "Polícia" da Conferência das Autoridades Europeias para a Protecção de Dados. Em 31 de Janeiro de 2005, a Comissão participou num "Seminário Público: protecção de dados e segurança dos cidadãos": que princípios para a União Europeia? realizada pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. A Comissão tomou em consideração os resultados da Conferência da Primavera das Autoridades Europeias para a Protecção de Dados, realizada em Cracóvia, em 25-26 de Abril de 2005, bem como a posição do Parlamento Europeu, tal como estabelecida, nomeadamente, na recomendação do Parlamento Europeu ao Conselho Europeu e ao Conselho relativa à troca de informações e à cooperação em matéria de infracções terroristas (2005/2046(INI)), adoptada em 7 de Junho de 2005.

Resumo das respostas e do modo como foram tomadas em consideração

Tanto o Parlamento Europeu como as Autoridades para a Protecção de Dados da União Europeia defendem veementemente a adopção de um instrumento jurídico sobre a protecção de dados pessoais no âmbito do terceiro pilar. Os representantes dos Governos dos

[22] COM (2005) 438 final DE 21.9.2005.

Estados-Membros e da Islândia, Noruega e Suíça, bem como da Europol e da Eurojust não manifestaram uma posição comum relativamente a esta questão. Contudo, a Comissão pôde concluir que não se verificava uma oposição significativa à ideia de um instrumento desse tipo. Parecia existir acordo quanto ao facto de a aplicação do princípio da disponibilidade dever ser acompanhada por regras de compensação adequadas no domínio da protecção de dados. Alguns Estados-Membros declararam que futuramente devia ser definida em primeiro lugar a forma de intercâmbio de dados e seguidamente as regras de protecção dos dados pessoais. Alguns preferiam que fosse incluído um conjunto de disposições específicas no acto relativo ao princípio da disponibilidade.

Tendo ponderado as diferentes posições, a Comissão considera que a aplicação do princípio da disponibilidade reforçará o desenvolvimento e alterará fundamentalmente a qualidade e a intensidade do intercâmbio de informações entre os Estados-Membros. Esse desenvolvimento afectará em grande medida os dados pessoais e o direito à protecção dos dados e deve ser compensado de forma adequada. Iniciativas recentes destinadas a proporcionar um acesso automatizado directo, com base num sistema de sim ou não, são susceptíveis de aumentar o risco de troca de dados ilegítimos, inexactos e desactualizados e devem ser tomadas em consideração. Estas iniciativas implicam que o controlador dos dados deixará de poder continuar a verificar *em cada caso individual* a legitimidade e a exactidão dos dados em causa. Consequentemente, tal deve ser acompanhado por obrigações rigorosas no sentido de garantir e verificar constantemente a qualidade dos dados a que é concedido acesso automatizado directo.

Uma vez que é dada especial atenção ao impacto da aplicação do princípio da disponibilidade, as disposições que se limitam a abordar os aspectos individuais da protecção de dados não são suficientes. Um instrumento jurídico relativo à protecção de dados pessoais no terceiro pilar pode, em princípio, contribuir para promover a cooperação policial e judiciária em matéria penal em termos de eficácia, bem como à sua legitimidade e respeito dos direitos fundamentais, em especial o direito à protecção dos dados pessoais.

Especialmente na perspectiva da aplicação do princípio da disponibilidade, um instrumento deste tipo é particularmente necessário e deve ser desenvolvido paralelamente à implementação deste princípio. A decisão-quadro deve acompanhar tanto quanto possível o espírito e a estrutura da Directiva 95/46/CE, tomando simultaneamente em consideração as necessidades específicas da cooperação policial e judiciária em matéria penal e o princípio da proporcionalidade. A Recomendação nº R(87) 15 do Conselho da Europa de 1987, que regulamenta a utilização dos dados pessoais no sector da polícia, foi tomada em consideração, a fim de transformar os seus principais princípios em disposições juridicamente vinculativas a nível da UE. Deviam ser estabelecidas regras claras para a protecção de dados pessoais que serão ou foram disponibilizados às autoridades competentes de outros Estados-Membros. Isto implica um sistema que garanta a qualidade do tratamento dos dados em causa. Um sistema desse tipo deve incluir disposições que estabeleçam direitos adequados da pessoa em causa e poderes das autoridades de controlo, uma vez que esses direitos e poderes são susceptíveis de contribuir para a qualidade dos dados em questão.

- **Avaliação do impacto**

Foram tomadas em linha de conta as seguintes opções: aplicabilidade da Directiva 95/46/CE; não adopção de uma proposta de disposições relativas à protecção de dados pessoais no terceiro pilar ou proposta a adoptar posteriormente; conjunto limitado de disposições específicas num acto jurídico relativo à troca de informações à luz do princípio da disponibilidade; decisão-quadro relativa à protecção de dados pessoais no terceiro pilar. No que diz respeito a esta última opção, foi analisado se um tal instrumento devia igualmente ser

aplicável à troca de informações através de sistemas de informação e por entidades estabelecidas a nível da UE.

As disposições gerais e fundamentais da Directiva 95/46/CE não são aplicáveis no âmbito do terceiro pilar, tal como estabelecido no nº 2 do seu artigo 3º. Mesmo a supressão deste artigo não podia implicar automaticamente a aplicabilidade da directiva à cooperação policial e judiciária em matéria penal. Em primeiro lugar, as especificidades desta cooperação não são plenamente tomadas em consideração na directiva e exigiriam uma maior precisão. Segundo, as exigências legislativas relativas aos actos abrangidos pelo Título VI do Tratado da União Europeia, que se destina a promover a cooperação policial e judiciária em matéria penal, devem ser respeitadas. A opção de não se adoptar uma proposta ou de tal proposta ser adoptada posteriormente no que se refere às disposições sobre o tratamento e protecção de dados pessoais no terceiro pilar deve ser excluída. Seria provável que esta opção implicasse a introdução de novas formas de trocas de informações na sequência da aplicação do princípio da disponibilidade sem garantia de uma rigorosa observância das condições essenciais no domínio da protecção de dados. Um conjunto limitado de disposições específicas num acto jurídico no que diz respeito à troca de informações à luz do princípio da disponibilidade não é suficiente tendo em conta o eventual impacto deste último. Uma decisão-quadro relativa à protecção de dados pessoais tratados no quadro da cooperação policial e judiciária em matéria penal constitui a única opção plenamente satisfatória. É pouco provável que os custos administrativos incorridos pelos Estados-Membros com esta opção – a existirem – sejam consideráveis.

A Comissão efectuou uma avaliação de impacto, que é mencionada no programa de trabalho e publicou um relatório sobre essa questão em http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) ELEMENTOS JURÍDICOS DA PROPOSTA

- **Síntese da acção proposta**

A decisão-quadro proposta inclui regras gerais sobre a licitude do tratamento de dados pessoais, disposições relativas a formas específicas de tratamento (transmissão e disponibilização de dados pessoais às autoridades competentes de outros Estados-Membros, tratamento posterior, em especial transmissão posterior, de dados recebidos de ou disponibilizados pelas autoridades competentes de outros Estados Membros), direitos da pessoa em causa, confidencialidade e segurança do tratamento, recursos judiciais, responsabilidade, sanções, autoridades de controlo e um grupo de trabalho sobre a protecção das pessoas no que diz respeito ao tratamento de dados pessoais para efeitos da prevenção, investigação, detecção e repressão de infracções penais. Deve ser dada especial atenção ao princípio de que os dados pessoais só serão transferidos para os países terceiros e organismos internacionais que garantam um nível adequado de protecção. A decisão-quadro prevê um mecanismo destinado a assegurar o respeito deste princípio em toda a UE.

- **Base jurídica**

Esta decisão-quadro deverá basear-se nos artigos 30º e 31º e no nº 2, alínea b), do artigo 34º do Tratado da União Europeia. Tendo especialmente em conta a aplicação do princípio da disponibilidade, são necessárias disposições adequadas no que diz respeito ao tratamento e protecção de dados pessoais, incluindo normas comuns para a transmissão destes dados a países terceiros e organismos internacionais, a fim de melhorar a cooperação policial e judiciária em matéria penal, em particular a luta contra o terrorismo e os crimes graves. Além

disso, os Estados-Membros só poderão confiar plenamente uns nos outros, se existirem normas comuns claras para a eventual transmissão posterior dos dados trocados a outras partes, em especial a países terceiros. As disposições propostas garantirão que a troca de informações entre as autoridades competentes não é prejudicada por níveis diferentes de protecção de dados nos Estados-Membros.

- **Princípios da subsidiariedade e da proporcionalidade**

A decisão-quadro contempla situações particularmente relevantes para a cooperação policial e judiciária em matéria penal entre os Estados-Membros, em especial no que se refere à troca de informações, a fim de garantir e promover medidas eficazes e lícitas para prevenir e lutar contra a criminalidade, particularmente os crimes graves e o terrorismo, em *todos* os Estados-Membros. As soluções nacionais, bilaterais ou multilaterais podem ser úteis para os Estados-Membros individualmente, mas não tomariam em consideração a necessidade de assegurar a segurança interna de toda a União. As necessidades em termos de informação por parte das autoridades responsáveis pela aplicação da lei são em grande medida determinadas pelo nível de integração entre países. A troca de informações para efeitos da aplicação da lei entre Estados-Membros deveria intensificar-se, devendo por conseguinte ser acompanhada por regras coerentes em matéria de tratamento e protecção de dados. Esta decisão-quadro respeita o princípio da subsidiariedade previsto no artigo 2º do Tratado da União Europeia e no artigo 5º do Tratado que institui a Comunidade Europeia, na medida em que tem por objectivo aproximar a legislação e regulamentação dos Estados-Membros, o que não pode ser realizado de forma adequada pelos Estados-Membros agindo unilateralmente e exige medidas concertadas no âmbito da União Europeia. Em conformidade com o princípio da proporcionalidade referido no último artigo, a presente decisão é limitada ao estritamente necessário para alcançar esse objectivo. A presente decisão refere-se apenas ao tratamento de dados pessoais que sejam relevantes para a cooperação policial e judiciária em matéria penal.

- **Escolha dos instrumentos**

Instrumento proposto: decisão-quadro. Este instrumento jurídico tem por objectivo a aproximação da legislação e regulamentação dos Estados-Membros, no que diz respeito à protecção dos dados pessoais tratados para efeitos de prevenir e lutar contra o crime.

4) INCIDÊNCIA ORÇAMENTAL

A execução da decisão-quadro proposta comporta apenas despesas administrativas reduzidas, a suportar pelo orçamento das Comunidades Europeias, para reuniões e serviços de secretariado do comité e do órgão consultivo a criar em conformidade com os artigos 16º e 31º.

2005/0202 (CNS)

Proposta de

DECISÃO-QUADRO DO CONSELHO

relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente os artigos 30º e 31º e a alínea b) do nº 2 do artigo 34º,

Tendo em conta a proposta da Comissão[23],

Tendo em conta o parecer do Parlamento Europeu [24],

Considerando o seguinte:

(1) A União Europeia estabeleceu o objectivo de manter e desenvolver um espaço de liberdade, de segurança e de justiça, deve ser proporcionado aos cidadãos um elevado nível de protecção, mediante a instituição de acções em comum entre os Estados-Membros nos domínios da cooperação policial e judiciária em matéria penal.

(2) As acções em comum no domínio da cooperação policial nos termos da alínea b) do nº 1 do artigo 30º do Tratado da União Europeia e a acção em comum no domínio da cooperação judiciária em matéria penal nos termos da alínea a) do nº 1 do artigo 31° do Tratado da União Europeia implicam a necessidade de tratar informações relevantes, devendo este tratamento estar sujeito às disposições adequadas em matéria de protecção de dados pessoais.

(3) A legislação abrangida pelo âmbito do Título VI do Tratado da União Europeia deve promover a cooperação policial e judiciária em matéria penal em termos de eficácia, bem como da sua legitimidade e respeito dos direitos fundamentais, em especial, o direito ao respeito pela vida privada e à protecção de dados pessoais. Normas comuns em matéria de tratamento e protecção de dados pessoais tratados para prevenir e lutar contra o crime podem contribuir para atingir os dois objectivos.

(4) O Programa da Haia relativo ao reforço da liberdade, da segurança e da justiça na União Europeia, adoptado pelo Conselho Europeu em 4 de Novembro de 2004, sublinhou a necessidade de uma abordagem inovadora do intercâmbio transfronteiras de informações sobre a aplicação da lei, com respeito escrupuloso pelas condições fundamentais no domínio da protecção de dados e convidou a Comissão a apresentar propostas relativamente a esta questão, o mais tardar até ao final de 2005. É o que reflecte o *Plano de Acção do Conselho e da Comissão de aplicação do Programa da Haia: reforço da liberdade, da segurança e da justiça na União Europeia*[25].

---

23 …

24 …

25 JO C 198 de 12.08.2005, p. 1.

(5) O intercâmbio de dados pessoais no quadro da cooperação policial e judiciária em matéria penal, nomeadamente à luz do princípio da disponibilidade de informação, tal como estabelecido no Programa da Haia, deve ser acompanhado por regras vinculativas claras, que reforcem a confiança mútua entre as autoridades competentes e que garantam a protecção das informações relevantes, de forma a excluir qualquer obstrução a esta cooperação entre os Estados-Membros, e respeitando plenamente os direitos fundamentais das pessoas. Os instrumentos em vigor a nível europeu não são suficientes. A Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas no que respeita ao tratamento dos dados pessoais e à livre circulação desses dados[26] não é aplicável ao tratamento de dados pessoais efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas no Título VI do Tratado da União Europeia e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado e as actividades do Estado no domínio do direito penal.

(6) Um instrumento jurídico relativo a normas comuns para a protecção de dados pessoais tratados para efeitos de prevenir e lutar contra o crime deve ser coerente com a política global da União Europeia no domínio do respeito pela vida privada e da protecção de dados. Sempre que possível, tendo em conta a necessidade de melhorar a eficiência das actividades legítimas das autoridades policiais, aduaneiras, judiciárias e outras autoridades competentes, deve por conseguinte seguir os princípios e definições existentes e comprovados, nomeadamente os estabelecidos na Directiva 95/46/CE do Parlamento Europeu e do Conselho ou relativos ao intercâmbio de informações pela Europol ou pela Eurojust, ou tratados através do Sistema de Informação Aduaneira ou outros instrumentos comparáveis.

(7) A aproximação das legislações dos Estados-Membros não deve implicar uma diminuição da protecção dos dados que asseguram, devendo, pelo contrário, ter por objectivo garantir um elevado nível de protecção na União.

(8) É necessário especificar os objectivos da protecção de dados no quadro das actividades policiais e judiciárias e estabelecer regras relativas à licitude do tratamento de dados pessoais, a fim de garantir que quaisquer informações eventualmente trocadas foram legitimamente tratadas e em conformidade com princípios fundamentais respeitantes à qualidade dos dados. Simultaneamente, as actividades legítimas das autoridades policiais, aduaneiras, judiciárias e outras autoridades competentes não podem ser prejudicadas.

(9) Garantir um elevado nível de protecção dos dados pessoais dos cidadãos europeus exige disposições comuns para determinar a licitude e a qualidade dos dados tratados pelas autoridades competentes noutros Estados-Membros.

(10) Afigura-se apropriado definir a nível europeu as condições em que as autoridades competentes dos Estados-Membros devem ser autorizadas a transmitir e disponibilizar dados pessoais às autoridades e aos particulares noutros Estados-Membros.

(11) O tratamento posterior de dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados, em especial, a transmissão ou disponibilização posterior de tais dados, deve ser sujeito a regras comuns a nível europeu.

---

[26] JO L 281 de 23.11.1995, p. 31.

(12) Quando são transferidos dados pessoais de um Estado-Membro da União Europeia para países terceiros ou organismos internacionais, estes dados devem, em princípio, beneficiar de um nível adequado de protecção.

(13) A presente decisão-quadro deve definir o procedimento de adopção das medidas necessárias para avaliar o nível de protecção dos dados num país terceiro ou num organismo internacional.

(14) A fim de garantir a protecção dos dados pessoais sem comprometer o objectivo das investigações penais, é necessário definir os direitos das pessoas em causa.

(15) Afigura-se apropriado estabelecer regras comuns em matéria de confidencialidade e de segurança do tratamento, de responsabilidade e de sanções por uso ilícito por parte das autoridades competentes, bem como de recursos judiciais à disposição da pessoa em causa. Além disso, é necessário que os Estados-Membros prevejam sanções penais para as infracções especialmente graves e intencionais às disposições em matéria de protecção de dados.

(16) A criação nos Estados-Membros de autoridades de controlo, que exerçam as suas funções com total independência, constitui um elemento essencial da protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária entre Estados-Membros.

(17) Essas autoridades devem ser dotadas dos meios necessários para a realização das suas funções, incluindo poderes de inquérito e de intervenção, especialmente em caso de reclamações, e poderes para intervir em processos judiciais. Essas autoridades devem ajudar a garantir a transparência do tratamento de dados efectuado no Estado-Membro sob cuja jurisdição se encontram. Contudo, os poderes destas autoridades não devem interferir nem com regras específicas fixadas para os processos penais nem com a independência do poder judiciário.

(18) Deve ser criado um grupo de trabalho sobre a protecção das pessoas no que diz respeito ao tratamento de dados pessoais para efeitos da prevenção, investigação, detecção e repressão de infracções penais, o qual deve gozar de total independência no desempenho das suas funções. Deve aconselhar a Comissão e os Estados-Membros e, em especial, contribuir para uma aplicação uniforme das regras nacionais adoptadas nos termos da presente decisão-quadro.

(19) O artigo 47º do Tratado da União Europeia prevê que nenhuma das suas disposições afecta os Tratados que instituem as Comunidades Europeias nem os Tratados e actos subsequentes que os alteraram ou completaram. Por conseguinte, a presente decisão-quadro não afecta a protecção de dados pessoais no âmbito do direito comunitário, em especial, tal como previsto na Directiva 95/46/CE do Parlamento Europeu e do Conselho, no Regulamento (CE) nº 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[27] e na Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações (Directiva relativa à privacidade e às comunicações electrónicas)[28].

---

[27] JO L 8 de 12.01.2001, p. 1.

[28] JO L 201 de 31.07.2001, p. 37.

(20) A presente decisão-quadro não prejudica as disposições específicas em matéria de protecção de dados previstas nos instrumentos jurídicos relevantes no que se refere ao tratamento e protecção de dados pessoais por parte da Europol, da Eurojust e do Sistema de Informação Aduaneira.

(21) As disposições relativas à protecção de dados pessoais constantes do Título IV da Convenção de 1990 de Aplicação do Acordo de Schengen, de 14 de Junho de 1985, relativa à supressão gradual dos controlos nas fronteiras comuns[29] (a seguir designada "Convenção de Schengen") e integradas no quadro da União Europeia por força do Protocolo anexo ao Tratado da União Europeia e ao Tratado que institui a Comunidade Europeia, devem ser substituídas pelas regras da presente decisão-quadro relativamente às questões abrangidas pelo âmbito do Tratado da União Europeia.

(22) Afigura-se apropriado que a presente decisão-quadro seja aplicável aos dados pessoais tratados no âmbito do Sistema de Informação Schengen de segunda geração e o respectivo intercâmbio de informações suplementares em conformidade com a Decisão JAI/2006/…, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração.

(23) A presente decisão-quadro não prejudica as regras relativas ao acesso ilícito a dados previstas na Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação[30].

(24) Afigura-se apropriado substituir o artigo 23º da Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia[31].

(25) Qualquer referência à Convenção do Conselho da Europa de 28 de Janeiro de 1981 relativa à protecção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais deve entender-se como uma referência à presente decisão-quadro.

(26) Dado que os objectivos da acção a realizar, nomeadamente a determinação de regras comuns para a protecção dos dados pessoais tratados no quadro da cooperação policial e judiciária em matéria penal, não podem ser concretizados de forma suficiente pelos Estados Membros agindo individualmente, e podem por conseguinte, devido às dimensões e aos efeitos da acção prevista, ser melhor realizados a nível da União Europeia, o Conselho pode adoptar medidas em conformidade com o princípio da proporcionalidade consagrado no artigo 5.º do Tratado CE e referido no artigo 2º do tratado da UE. Em conformidade com o princípio da proporcionalidade consagrado no artigo 5.º do Tratado CE, a presente decisão não excede o necessário para atingir aqueles objectivos.

(27) O Reino Unido participa na presente decisão-quadro, nos termos do artigo 5.° do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado UE e ao Tratado CE, e do n.º 2 do artigo 8.° da Decisão 2000/365/CE do Conselho, de 29 de Maio de 2000, sobre o pedido do Reino Unido da Grã-Bretanha e da Irlanda do Norte para participar em algumas das disposições do acervo de Schengen[32].

---

29 JO L 239 de 22.09.2000, p. 19.
30 JO L 69 de 16.03.2005, p. 67.
31 JO C 197 de 12.07.2000, p. 3.
32 JO L 131 de 01.06.2000, p. 43.

(28) A Irlanda participa na presente decisão-quadro, nos termos do artigo 5. ° do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado UE e ao Tratado CE, e do n.º 2 do artigo 6. ° da Decisão 2002/192/CE do Conselho, de 28 de Fevereiro de 2002, sobre o pedido da Irlanda para participar em algumas das disposições do acervo de Schengen.

(29) No que diz respeito à Islândia e à Noruega, a presente decisão-quadro constitui um desenvolvimento das disposições do acervo de Schengen na acepção do Acordo celebrado pelo Conselho da União Europeia com a República da Islândia e o Reino da Noruega relativo à associação dos dois Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen, que é abrangido pelo domínio referido no ponto H do artigo 1º da Decisão 1999/437/CE do Conselho, de 17 de Maio de 1999, relativa a determinadas regras de aplicação desse Acordo[33].

(30) No que diz respeito à Suíça, a presente decisão constitui um desenvolvimento das disposições do acervo de Schengen na acepção do Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen, que é abrangido pelo domínio referido no ponto H do artigo 1.º da Decisão 1999/437/CE do Conselho, de 17 de Maio de 1999, em articulação com o n.º 1 do artigo 4.º da Decisão 2004/849/CE do Conselho respeitante à assinatura, em nome da União Europeia, e à aplicação provisória de certas disposições do Acordo[34].

(31) A presente decisão-quadro constitui um acto baseado no acervo de Schengen ou de algum modo com ele relacionado, na acepção do nº 1 do artigo 3º do Acto de Adesão de 2003.

(32) A presente decisão-quadro respeita os direitos fundamentais e os princípios reconhecidos, em especial na Carta dos Direitos Fundamentais da União Europeia. A presente decisão-quadro procura garantir o pleno cumprimento dos direitos ao respeito pela vida privada e à protecção de dados pessoais constantes dos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia,

ADOPTOU A PRESENTE DECISÃO-QUADRO:

CAPÍTULO I
OBJECTO, DEFINIÇÕES E ÂMBITO DE APLICAÇÃO

Artigo 1º
Objecto

1. A presente decisão-quadro estabelece normas comuns para garantir a protecção das pessoas no que diz respeito ao tratamento de dados pessoais no quadro da cooperação policial e judiciária em matéria penal, prevista no Título VI do Tratado da União Europeia.

2. Os Estados-Membros devem garantir que a divulgação de dados pessoais às autoridades competentes de outros Estados-Membros não é restringida nem proibida por razões relacionadas com a protecção de dados pessoais, tal como previsto na presente decisão-quadro.

---

33 JO L 176 de 10.07.1999, p. 31.

34 JO L 368 de 15.12.2004, p. 26.

Artigo 2º
Definições

Para efeitos da presente decisão-quadro, entende-se por:

a)· «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

b)· «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

c)· «Ficheiro de dados pessoais» («ficheiro»), qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

d)· «Responsável pelo tratamento», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados pelo direito nacional ou por legislação adoptada em conformidade com o Título VI do Tratado da União Europeia, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou pela legislação adoptada em conformidade com o Título VI do Tratado da União Europeia;

e) «Subcontratante», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento;

f) «Terceiro», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade directa do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados;

g) «Destinatário», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados, independentemente de se tratar ou não de um terceiro;

h) «Consentimento da pessoa em causa», qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento.

i) "Organismos internacionais", instâncias ou organizações instituídas por acordos internacionais.

j) "Autoridades competentes", as autoridades policiais, aduaneiras, judiciárias e outras autoridades competentes dos Estados-Membros, na acepção do artigo 29º do Tratado da União Europeia.

Artigo 3º
Âmbito de aplicação

1. A presente decisão-quadro é aplicável ao tratamento de dados pessoais por meios total ou parcialmente automatizado, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados por uma autoridade competente para efeitos de prevenção, investigação, detecção e repressão de infracções penais.

2. A presente decisão-quadro não é aplicável ao tratamento de dados pessoais por parte:

   – do Serviço Europeu de Polícia (Europol);

   – da Unidade Europeia de Cooperação Judiciária (Eurojust);

   – do Sistema de Informação Aduaneira, tal como criado em conformidade com a Convenção estabelecida com base no artigo K.3 do Tratado da União Europeia, sobre a utilização da informática no domínio aduaneiro, e respectivas alterações.

CAPÍTULO II
CONDIÇÕES GERAIS DE LICITUDE DO TRATAMENTO DE DADOS PESSOAIS

Artigo 4º
Princípios relativos à qualidade dos dados

1. Os Estados-Membros devem estabelecer que os dados pessoais serão:

   a) Objecto de um tratamento leal e lícito;

   b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas;

   c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;

   d) Exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou rectificados. Os Estados-Membros podem prever um tratamento dos dados com diversos graus de exactidão e de fiabilidade, devendo nesse caso prever que os dados sejam distinguidos em função do seu grau de exactidão e de fiabilidade e, nomeadamente, que os dados baseados nos factos sejam distinguidos dos dados baseados em opiniões ou apreciações pessoais;

   e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-Membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.

2. Incumbe ao responsável pelo tratamento assegurar a observância do disposto no nº 1.

3. Os Estados-Membros devem estabelecer uma distinção clara entre dados pessoais relativos a

   – uma pessoa que é suspeita de ter cometido ou participado numa infracção penal,

   – uma pessoa que foi condenada por uma infracção penal,

   – uma pessoa relativamente à qual existam motivos fundados para crer que cometerá uma infracção penal,

   – uma pessoa que pode ser chamada a testemunhar em investigações penais ou nos processos penais subsequentes,

   – uma pessoa que foi vítima de uma infracção penal ou relativamente à qual certos factos levam a crer que podia ser vítima de uma infracção penal,

   – uma pessoa que pode fornecer informações sobre infracções penais,

   – um contacto ou associado de uma das pessoas mencionadas anteriormente, e

   – uma pessoa que não é abrangida por nenhuma das categorias anteriormente referidas.

4. Os Estados-Membros devem estabelecer que o tratamento de dados pessoais só será necessário se:

   – existirem boas razões para crer, à luz dos factos estabelecidos, que os dados pessoais em causa possibilitariam, facilitariam ou acelerariam a prevenção, a investigação, a detecção e a repressão de infracções penais, e

   – não existirem outros meios que afectem menos a pessoa em causa, e

   – o tratamento dos dados não for desproporcionado em relação à infracção em questão.

Artigo 5º
Princípios relativos à legitimidade do tratamento dos dados

Os Estados-Membros estabelecerão que o tratamento dos dados pessoais só pode ser efectuado pelas autoridades competentes por força de uma lei que estabeleça que esse tratamento é necessário para o cumprimento da missão legítima da autoridade em causa e para efeitos de prevenção, investigação, detecção e repressão de infracções penais.

Artigo 6º
Tratamento de categorias específicas de dados

1. Os Estados-Membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

2. O nº 1 não é aplicável quando:

   – o tratamento estiver previsto por lei e for absolutamente necessário para o cumprimento da missão legítima da autoridade em causa para efeitos de prevenção, investigação, detecção e repressão de infracções penais, ou se a pessoa em questão der expressamente o seu consentimento a o tratamento, e

– os Estados-Membros previrem as garantias específicas adequadas, por exemplo, o acesso aos dados em causa apenas por parte do pessoal responsável pelo cumprimento da missão legítima que justifica o tratamento.

Artigo 7º
Prazos para a conservação de dados pessoais

1. Os Estados-Membros estabelecerão que os dados pessoais só serão conservados durante o período estritamente necessário para os efeitos para que foram recolhidos, salvo disposição em contrário da legislação nacional. Os dados pessoais das pessoas a que se refere o nº 3, último travessão, do artigo 4º só serão conservados durante o período estritamente necessário para os efeitos para que foram recolhidos.

2. Os Estados-Membros estabelecerão as medidas processuais e técnicas adequadas, que garantam o cumprimento dos prazos de conservação dos dados pessoais. O respeito desses prazos de conservação será periodicamente controlado.

CAPÍTULO III – Formas específicas de tratamento

SECÇÃO I – TRANSMISSÃO E DISPONIBILIZAÇÃO DE DADOS PESSOAIS ÀS AUTORIDADES COMPETENTES DE OUTROS ESTADOS-MEMBROS

Artigo 8º
Transmissão e disponibilização de dados pessoais às autoridades competentes de outros Estados-Membros

Os Estados-Membros estabelecerão que os dados pessoais só serão transmitidos ou disponibilizados às autoridades competentes de outros Estados-Membros se forem necessários para o cumprimento de uma missão legítima da autoridade transmissora ou receptora e para efeitos de prevenção, investigação, detecção e repressão de infracções penais.

Artigo 9º
Verificação da qualidade dos dados transmitidos ou disponibilizados

1. Os Estados-Membros estabelecerão que a qualidade dos dados pessoais é verificada o mais tardar antes de serem transmitidos ou disponibilizados. Na medida do possível, em todas as transmissões de dados, as decisões judiciais e as decisões de arquivamento do processo devem ser indicadas e os dados baseados em opiniões ou apreciações pessoais devem ser verificados na fonte antes de serem transmitidos e indicado o seu grau de exactidão ou fiabilidade.

2. Os Estados-Membros estabelecerão que a qualidade dos dados pessoais disponibilizados por acesso automatizado directo às autoridades competentes de outro Estado-Membro é periodicamente verificada, a fim de garantir um acesso a dados exactos e actualizados.

3. Os Estados-Membros estabelecerão que os dados pessoais que deixaram de ser exactos ou actualizados não serão transmitidos nem disponibilizados.

4. Os Estados-Membros estabelecerão que uma autoridade competente, que transmitiu ou disponibilizou dados pessoais a uma autoridade competente de outro Estado-Membro, informará esta última imediatamente se verificar, por sua própria iniciativa ou a pedido da pessoa em causa, que os dados em questão não deviam ter

sido transmitidos ou disponibilizados ou que foram transmitidos ou disponibilizados dados inexactos ou obsoletos.

5. Os Estados-Membros estabelecerão que uma autoridade competente, que foi informada em conformidade com o artigo 4º, suprimirá ou rectificará os dados em causa. Além disso, essa autoridade rectificará os dados em causa, se detectar que estes são inexactos. Se essa autoridade tiver motivos razoáveis para crer que os dados pessoais recebidos são inexactos ou devem ser suprimidos, informará sem demora a autoridade competente que transmitiu ou disponibilizou os dados em causa.

6. Os Estados-Membros estabelecerão, sem prejuízo das regras de processo penal nacional, que os dados pessoais sejam "anotados" a pedido da pessoa em causa, se a sua exactidão for contestada pela pessoa em causa e se a sua exactidão ou inexactidão não puder ser apurada. Essa "anotação" só será suprimida com a autorização da pessoa em causa ou com base numa decisão do tribunal competente ou da autoridade de controlo competente.

7. Os Estados-Membros estabelecerão que os dados pessoais recebidos da autoridade de um outro Estado-Membro serão suprimidos:

   – se estes dados não devessem ter sido transmitidos, disponibilizados ou recebidos,

   – decorrido um prazo estabelecido na legislação do outro Estado-Membro, se a autoridade que transmitiu ou disponibilizou os dados em causa tiver informado a autoridade receptora desse prazo no momento da transmissão ou disponibilização dos dados, salvo se os dados pessoais ainda forem necessários para uma acção judicial,

   – se estes dados não são ou já não são necessários para os efeitos para os quais foram transmitidos ou disponibilizados.

8. Se os dados pessoais foram transmitidos sem pedido, a autoridade receptora verificará sem demora se estes dados são necessários para os efeitos para os quais foram transmitidos.

9. Os dados pessoais não serão suprimidos mas bloqueados, em conformidade com a legislação nacional, se existirem motivos razoáveis para crer que a sua supressão pode afectar interesses da pessoa em causa dignos de protecção. Os dados bloqueados só serão utilizados ou transmitidos para a finalidade que justificou a sua não supressão.

Artigo 10º
Registo e documentação

1. Os Estados-Membros estabelecerão que cada transmissão e recepção automatizada de dados pessoais, em especial através de acesso automatizado directo, seja registada, a fim de garantir a posterior verificação dos motivos da transmissão, os dados transmitidos, o dia e a hora da transmissão, as autoridades implicadas e, no que diz respeito à autoridade receptora em causa, as pessoas que receberam os dados e as pessoas na origem da recepção.

2. Os Estados-Membros estabelecerão que cada transmissão e recepção automatizada de dados pessoais seja documentada, a fim de garantir a posterior verificação dos motivos da transmissão, os dados transmitidos, o dia e a hora da transmissão, as

autoridades implicadas e, no que diz respeito à autoridade receptora em causa, as pessoas que receberam os dados e as pessoas na origem da recepção.

3. A autoridade que registou ou documentou tais informações comunicará o facto sem demora à autoridade de controlo competente a pedido desta última. As informações só serão utilizadas para efeitos do controlo da protecção de dados e para garantir o tratamento adequado dos dados, bem como a respectiva integridade e segurança.

SECÇÃO II – TRATAMENTO POSTERIOR, NOMEADAMENTE TRANSMISSÃO E TRANSFERÊNCIA POSTERIORES, DE DADOS RECEBIDOS DAS AUTORIDADES COMPETENTES DE OUTROS ESTADOS-MEMBROS OU POR ELAS DISPONIBILIZADOS

Artigo 11º
Tratamento posterior de dados pessoais recebidos das autoridades competentes de outro Estado-Membro ou por elas disponibilizados

1. Os Estados-Membros estabelecerão que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados só serão objecto de um tratamento posterior em conformidade com o a presente decisão-quadro, em especial os artigos 4º, 5º e 6º,

   a) Para a finalidade específica para a qual foram transmitidos ou disponibilizados, ou

   b) Se necessário, para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou para efeitos de prevenção de ameaças à segurança pública ou a uma pessoa, salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações.

2. Os dados pessoais em questão apenas serão objecto de tratamento posterior para os efeitos referidos na alínea b) do nº 1 mediante autorização prévia da autoridade que transmitiu ou disponibilizou os dados pessoais.

3. A alínea b) do nº 1 não é aplicável se um acto legislativo específico adoptado ao abrigo do Título VI do Tratado da União Europeia estabelecer expressamente que os dados pessoais recebidos da autoridade competente de outro Estado-membro ou por ela disponibilizados só serão objecto de um tratamento posterior para as finalidades para as quais foram transmitidos ou disponibilizados

Artigo 12º
Transmissão a outras autoridades competentes

Os Estados-Membros estabelecerão que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados só serão transmitidos ou disponibilizados posteriormente a outras autoridades competentes de um Estado-Membro apenas se estiverem reunidas cumulativamente as seguintes condições:

a) A transmissão ou a disponibilização constitui uma obrigação legal ou é autorizada por lei;

b) A transmissão ou a disponibilização é necessária para o cumprimento da missão legítima da autoridade que recebeu os dados em causa ou da autoridade à qual serão posteriormente transmitidos;

c) A transmissão ou a disponibilização é necessária para a finalidade específica para a qual foram transmitidos ou disponibilizados os dados ou para efeitos da prevenção, investigação, detecção e repressão de infracções penais ou para efeitos de prevenção de ameaças à segurança pública ou a uma pessoa, salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações;

d) A autoridade competente do Estado-Membro que transmitiu ou disponibilizou os dados em causa à autoridade competente que tenciona transmiti-los ou disponibilizá-los posteriormente deu autorização prévia para a sua transmissão ou disponibilização posterior.

Artigo 13º
Transmissão a outras autoridades que não as autoridades competentes

Os Estados-Membros estabelecerão que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados apenas serão transmitidos posteriormente a outras autoridades, que não as autoridades competentes, de um Estado-Membro em casos especiais e se estiverem reunidas cumulativamente as seguintes condições:

a) A transmissão constitui uma obrigação legal ou é autorizada por lei e

b) a transmissão é

necessária para a finalidade específica para a qual os dados em causa foram transmitidos ou disponibilizados ou para efeitos da prevenção, investigação, detecção e repressão de infracções penais ou para efeitos de prevenção de ameaças à segurança pública ou a uma pessoa, salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações,

ou

necessária, uma vez que os dados em causa são indispensáveis para a autoridade à qual os dados serão transmitidos posteriormente, a fim de lhe permitir cumprir a sua missão legítima e desde que o objectivo da recolha ou do tratamento a realizar por essa autoridade não seja incompatível com o tratamento previsto inicialmente e que as obrigações legais da autoridade competente que tenciona transmitir os dados a tal não se oponham,

ou

seja indubitavelmente do interesse da pessoa em causa e esta tenha autorizado ou as circunstâncias permitam presumir claramente essa autorização.

c) A autoridade competente do Estado-Membro que transmitiu ou disponibilizou os dados em causa à autoridade competente que tenciona transmiti-los posteriormente deu autorização prévia para a sua transmissão posterior.

Artigo 14º
Transmissão a particulares

Os Estados-Membros estabelecerão, sem prejuízo das regras de processo penal nacionais que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por esta

disponibilizados, só serão transmitidos posteriormente a particulares num Estado-Membro em casos específicos e se estiverem reunidas cumulativamente as seguintes condições:

a) A transmissão constitui uma obrigação legal ou é autorizada por lei, e

b) A transmissão é necessária para a finalidade para a qual os dados em causa foram transmitidos ou disponibilizados ou para efeitos da prevenção, investigação, detecção e repressão de infracções penais ou para efeitos de prevenção de ameaças à segurança pública ou a uma pessoa, salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações, e

c) A autoridade competente do Estado-Membro que transmitiu ou disponibilizou os dados em causa à autoridade competente, que tenciona transmiti-los posteriormente, deu autorização prévia para a sua transmissão posterior a particulares.

Artigo 15º

Transferência para as autoridades competentes de países terceiros ou organismos internacionais

1. Os Estados-Membros estabelecerão que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados não são transferidos posteriormente para autoridades competentes de países terceiros ou para organismos internacionais, salvo se tal transferência estiver em conformidade com a presente decisão-quadro e, em especial, se estiverem reunidas cumulativamente as seguintes condições:

   a) A transferência constitui uma obrigação legal ou é autorizada por lei;

   b) A transferência é necessária para a finalidade para a qual os dados em causa foram transmitidos ou disponibilizados ou para efeitos da prevenção, investigação, detecção e repressão de infracções penais ou para efeitos de prevenção de ameaças à segurança pública ou a uma pessoa, salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações;

   c) A autoridade competente de outro Estado-Membro que transmitiu ou disponibilizou os dados em causa à autoridade competente que tenciona transferi-los posteriormente deu autorização prévia para a sua transferência posterior;

   d) Um nível adequado de protecção dos dados é garantido no país terceiro ou pelo organismo internacional para o qual serão transferidos os dados em causa.

2. Os Estados-Membros garantirão que o carácter adequado do nível de protecção oferecido por um país terceiro ou um organismo internacional será apreciado no contexto de todas as circunstâncias que rodeiam cada transferência ou categoria de transferências. Esta apreciação será efectuada, em especial, com base numa análise dos seguintes elementos: o tipo de dados, as finalidades e a duração do tratamento para o qual os dados serão transferidos, o país de origem e o país de destino final, as disposições legais gerais e sectoriais em vigor no país terceiro ou no organismo em questão, as regras profissionais e de segurança aí aplicadas, bem como a aplicação de garantias suficientes pelo destinatário da transferência.

3. Os Estados-Membros e a Comissão informar-se-ão mutuamente dos casos em que consideram que um país terceiro ou um organismo internacional não assegura um nível de protecção adequado na acepção do nº 2.

4. Quando se verificar, em conformidade com o procedimento previsto no artigo 16º, que um país terceiro ou um organismo internacional não garante um nível adequado de protecção na acepção do nº 2, os Estados-Membros tomarão as medidas necessárias para impedir qualquer transferência de dados pessoais para o país terceiro ou para o organismo internacional em questão.

5. Em conformidade com o procedimento previsto no artigo 16º, pode declarar-se que um país terceiro ou um organismo internacional assegura um nível de protecção adequado na acepção do nº 2, em virtude da sua legislação nacional ou dos compromissos internacionais que subscreveu, com vista à protecção do direito ao respeito pela vida privada e das liberdades e direitos individuais de base.·

6. A título excepcional, os dados pessoais recebidos da autoridade competente de outro Estado-membro podem ser transferidos posteriormente para autoridades competentes de países terceiros ou para organismos internacionais que não asseguram um nível adequado de protecção ou no âmbito das quais este nível de protecção não está assegurado em caso de absoluta necessidade, a fim de salvaguardar os interesses essenciais de um Estado-Membro ou para a prevenção de um perigo grave iminente que ameaça a segurança pública ou uma ou várias pessoas em especial.

Artigo 16º
Comité

1. Quanto é feita referência ao presente artigo, a Comissão será assistida por um comité composto por representantes dos Estados-Membros e presidido pelo representante da Comissão.

2. O comité adoptará o seu regulamento interno, sob proposta do presidente, com base no regulamento interno tipo publicado no Jornal Oficial da União Europeia.

3. O representante da Comissão apresenta ao comité um projecto das medidas a tomar. O comité emitirá o seu parecer sobre esse projecto, num prazo que o presidente pode fixar em função da urgência da questão. O parecer é emitido pela maioria prevista no nº 2 do artigo 205º do Tratado que institui a Comunidade Europeia, para a adopção das decisões que o Conselho é chamado a tomar sob proposta da Comissão. Nas votações no comité, os votos dos representantes dos Estados-Membros estão sujeitos à ponderação definida no artigo atrás referido. O presidente não participa na votação.

4. A Comissão adopta as medidas previstas desde que sejam conformes ao parecer do comité. Se as medidas projectadas não forem conformes com o parecer do comité, ou na falta de parecer, a Comissão apresentará imediatamente ao Conselho uma proposta relativa às medidas a tomar e informará o Parlamento Europeu.

5. O Conselho pode deliberar por maioria qualificada sobre a proposta, no prazo de dois meses a contar da data em que o assunto lhe tenha sido submetido.

   Se, dentro daquele período, o Conselho indicou por maioria qualificada que se opõe à proposta, a Comissão reconsiderá-la-á, podendo apresentar ao Conselho uma proposta alterada, apresentar de novo a sua proposta ou apresentar uma proposta legislativa. Se, no termo desse prazo, o Conselho não tiver aprovado o acto de execução proposto nem se tiver pronunciado contra a proposta de medidas de execução, o acto de execução proposto será aprovado pela Comissão.

Artigo 17º
Derrogações aos artigos 12º, 13º, 14º e 15º

Os artigos 12º, 13º, 14º e 15º não serão aplicáveis se um acto legislativo específico adoptado ao abrigo do Título VI do Tratado da União Europeia estabelecer expressamente que os dados pessoais recebidos da autoridade competente de outro Estado-Membro ou por ela disponibilizados não serão transmitidos posteriormente ou só serão transmitidos posteriormente em condições mais específicas.

Artigo 18º
Informações a pedido da autoridade competente

Os Estados-Membros estabelecerão que a autoridade competente da qual ou através da qual foram recebidos os dados pessoais ou que os disponibilizou, seja informada a seu pedido do tratamento posterior desses dados e dos resultados obtidos.

CAPÍTULO IV
DIREITOS DA PESSOA EM CAUSA

Artigo 19º
Direito à informação em caso de recolha de dados junto da pessoa em causa e com o seu conhecimento

1. Os Estados-Membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito e com o seu conhecimento, pelo menos as seguintes informações a título gratuito, salvo se a pessoa já dispuser delas:

   a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante;

   b) Finalidades do tratamento a que os dados se destinam;

   c) Outras informações, tais como:

   – a base jurídica do tratamento,

   – os destinatários ou categorias de destinatários dos dados,

   – o carácter obrigatório ou facultativo da resposta ou de outras formas de cooperação, bem como as eventuais consequências da falta de resposta ou de cooperação,

   – a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar,

   desde que tais informações sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos.

2. O fornecimento das informações previstas no nº 1 só será recusado ou limitado se tal se revelar necessário

   a) Para permitir que o responsável pelo tratamento cumpra as suas funções legais de forma adequada;

   b) Para evitar prejudicar investigações, inquéritos ou processos em curso ou o cumprimento pelas autoridades competentes das suas funções legais;

   c) Para proteger a segurança e a ordem públicas num Estado-Membro;

   d) Para proteger os direitos e liberdades de terceiros,

   salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações.

3. Se a informação a que se refere o nº 1 for recusada ou limitada, o responsável pelo tratamento informará a pessoa em causa de que pode recorrer para a autoridade de controlo competente, sem prejuízo de um eventual recurso judicial e sem prejuízo de uma acção penal nos termos do direito nacional.

4. Os motivos que justificam uma recusa ou restrição nos termos do nº 2 não serão comunicados à pessoa em causa se esse facto comprometer a finalidade da recusa. Nesse caso, o responsável pelo tratamento informará a pessoa em causa de que pode recorrer para a autoridade de controlo competente, sem prejuízo de um eventual

recurso judicial e sem prejuízo de uma acção penal nos termos do direito nacional. Se a pessoa em causa apresentar um recurso junto da autoridade de controlo, esta última examina o recurso. A autoridade de controlo, ao investigar o recurso, só lhe comunicará se os dados foram tratados correctamente e, em caso negativo, se foram introduzidas as eventuais correcções necessárias.

Artigo 20º

Direito de informação em caso de dados não recolhidos junto da pessoa em causa ou obtidos sem o seu conhecimento

1. Se os dados não tiverem sido recolhidos junto da pessoa em causa ou tiverem sido obtidos sem o seu conhecimento ou sem esta saber da recolha de dados a seu respeito, os Estados-Membros estabelecerão que o responsável pelo tratamento, ou o seu representante, deve fornecer à pessoa em causa, no momento em que os dados forem registados ou, se estiver prevista a comunicação de dados a terceiros, num prazo razoável após a primeira divulgação dos dados, pelo menos as seguintes informações a título gratuito, salvo se este já dispuser delas ou se o fornecimento dessas informações for comprovadamente impossível ou implicar um esforço desproporcionado:

   a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante;

   b) Finalidades do tratamento;

   c) Outras informações, tais como:

   – a base jurídica do tratamento;

   – as categorias de dados envolvidos,

   – os destinatários ou categorias de destinatários dos dados,

   – a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar,

   desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos.

2. As informações previstas no nº 1 não serão fornecidas se tal for necessário

   a) Para permitir que o responsável pelo tratamento cumpra as suas funções legais de forma adequada;

   b) Para evitar prejudicar investigações, inquéritos ou processos em curso ou o cumprimento pelas autoridades competentes das suas funções legais;

   c) Para proteger a segurança e a ordem públicas num Estado-Membro;

   d) Para proteger os direitos e liberdades de terceiros,

   salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações.

Artigo 21º

Direito de acesso, rectificação, apagamento ou bloqueio

1. Os Estados-Membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento:

a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos:

– a confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide, a base jurídica do tratamento e os destinatários ou categorias de destinatários a quem foram comunicados os dados,

– a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados,

b) Consoante o caso, a rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente decisão-quadro, nomeadamente devido ao carácter incompleto ou inexacto desses dados;

c) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea b), salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado.

2. Qualquer acto a que a pessoa em causa tenha direito, em conformidade com o nº 1, será recusado se tal se revelar necessário

a) Para permitir que o responsável pelo tratamento cumpre as suas funções legais de forma adequada;

b) Para evitar prejudicar investigações, inquéritos ou processos em curso ou o cumprimento pelas autoridades competentes das suas funções legais;

c) Para proteger a segurança e a ordem públicas num Estado-Membro;

d) Para proteger os direitos e liberdades de terceiros,

salvo quando a necessidade de proteger os interesses ou os direitos fundamentais da pessoa em causa ultrapassa tais considerações.

3. Uma recusa ou restrição dos direitos a que se refere o nº 1 será estabelecida por escrito. Se a informação a que se refere o nº 1 for recusada ou limitada, o responsável pelo tratamento informará a pessoa em causa de que pode recorrer para a autoridade de controlo competente, sem prejuízo de um eventual recurso judicial e sem prejuízo de uma acção penal nos termos do direito nacional.

4. Os motivos que justificam uma recusa nos termos do nº 2 não serão comunicados à pessoa em causa se esse facto comprometer a finalidade da recusa. Nesse caso, o responsável pelo tratamento informará a pessoa em causa de que pode recorrer para a autoridade de controlo competente, sem prejuízo de um eventual recurso judicial e sem prejuízo de uma acção penal nos termos do direito nacional. Se a pessoa em causa apresentar um recurso junto da autoridade de controlo, esta última examina o recurso. A autoridade de controlo, ao investigar o recurso, só lhe comunicará se os dados foram tratados correctamente e, em caso negativo, se foram introduzidas as eventuais correcções necessárias.

Artigo 22º
Informações a terceiros na sequência de uma rectificação, de um bloqueio ou de um apagamento

Os Estados-Membros estabelecerão que serão tomadas as medidas técnicas adequadas, a fim de garantir que, nos casos em que o responsável pelo tratamento rectifica, bloqueia ou apaga dados pessoais na sequência de um pedido, é automaticamente estabelecida uma lista de fornecedores e de destinatários destes dados. O responsável pelo tratamento garante que os nomes incluídos na lista serão informados das alterações introduzidas nos dados pessoais.

CAPÍTULO V
Confidencialidade e segurança do tratamento

Artigo 23º
Confidencialidade

Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais. Todas as pessoas chamadas a trabalhar com uma autoridade competente de um Estado-Membro ou no âmbito dessa autoridade estão vinculadas por regras estritas em matéria de confidencialidade.

Artigo 24º
Segurança

1. Os Estados-Membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por uma rede ou a sua disponibilização através da concessão de acesso directo automatizado, e contra qualquer outra forma de tratamento ilícito, tomando em consideração, em especial, os riscos apresentados pelo tratamento e a natureza dos dados a proteger.

   Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger. As medidas apenas serão consideradas necessárias se os esforços envolvidos não forem desproporcionados face ao objectivo a atingir em termos de protecção.

2. No que diz respeito ao tratamento automatizado de dados, cada Estado-Membro aplicará medidas destinadas a:

   a) Impedir o acesso de qualquer pessoa não autorizada às instalações utilizadas para o tratamento de dados pessoais (controlo da entrada nas instalações);

   b) Impedir que os suportes de dados possam ser lidos, copiados, alterados ou retirados por uma pessoa não autorizada (controlo dos suportes de dados);

   c) Impedir a introdução não autorizada de dados no ficheiro, bem como qualquer tomada de conhecimento, alteração ou apagamento não autorizados de dados pessoais inseridos no ficheiro (controlo do arquivo de dados);

d) Impedir que os sistemas de tratamento informatizado de dados sejam utilizados por pessoas não autorizadas por meio de equipamento de transmissão de dados (controlo da utilização);

e) garantir que as pessoas autorizadas a utilizar o sistema de tratamento de dados apenas tenham acesso aos dados abrangidos pela sua autorização de acesso (controlo do acesso aos dados);

f) garantir que é possível verificar e estabelecer a que instâncias os dados pessoais foram ou podem ser transmitidos ou disponibilizados utilizando equipamento de comunicação de dados (controlo da transmissão);

g) Garantir que possa verificar-se a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado de dados, quando e por quem (controlo da introdução);

h) Impedir que os dados pessoais possam ser lidos, copiados, alterados ou suprimidos por uma pessoa não autorizada durante transferências de dados pessoais ou durante o transporte de suportes de dados (controlo do transporte);

i) Assegurar que os sistemas utilizados possam ser imediatamente reparados em caso de avaria (recuperação do equipamento);

j) Assegurar que o sistema funcione em perfeitas condições, que os erros de funcionamento sejam imediatamente assinalados (fiabilidade) e que os dados arquivados não sejam falseados por quaisquer erros de funcionamento do sistema (autenticidade).

3. Os Estados-Membros estabelecerão que o responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar e deverá zelar pelo cumprimento dessas medidas.

4. A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que:

– o subcontratante apenas actuará mediante instruções do responsável pelo tratamento,

– as obrigações referidas nos nºs 1 e 2, tal como definidas pela legislação do Estado-Membro onde o subcontratante está estabelecido, incumbem igualmente a este último.

5. Para efeitos de conservação de provas, os elementos do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no nº 1, deverão ficar consignados por escrito ou sob forma equivalente.

Artigo 25º
Registo

1. Os Estados-Membros estabelecerão que cada responsável pelo tratamento mantém um registo dos tratamentos ou conjuntos de tratamentos destinados a prosseguir uma mesma finalidade ou finalidades associadas. As informações a incluir no registo compreenderão:

a) O nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante;

b) A ou as finalidades do tratamento;

c) Uma descrição da ou das categorias de pessoas em causa e dos dados ou categorias de dados que lhes respeitem;

d) O fundamento jurídico do tratamento a que os dados se destinam;

e) Os destinatários ou categorias de destinatários a quem os dados poderão ser comunicados;

f) As transferências de dados previstas para países terceiros;

g) Uma descrição geral que permita efectuar uma avaliação prévia da adequação das medidas tomadas para garantir a segurança do tratamento nos termos do artigo 24º.

2. Os Estados-Membros especificarão as condições e os procedimentos de notificação à autoridade de controlo das informações referidas no nº 1.

Artigo 26º
Controlo prévio

1. Os Estados-Membros especificarão os tratamentos que possam representar riscos específicos para os direitos e liberdades das pessoas em causa e zelarão por que sejam controlados antes da sua aplicação.

2. Esse controlo prévio será efectuado pela autoridade de controlo após recepção de uma notificação do responsável pelo tratamento ou pelo encarregado da protecção de dados que, em caso de dúvida, deverá consultar a autoridade de controlo.

3. Os Estados-Membros poderão igualmente efectuar este controlo durante os trabalhos de preparação de uma medida do parlamento nacional ou de uma medida baseada nessa medida legislativa, a qual defina a natureza do tratamento e estabeleça as garantias adequadas.

CAPÍTULO VI
RECURSOS JUDICIAIS E RESPONSABILIDADE

Artigo 27º
Recursos

Sem prejuízo de quaisquer garantias graciosas, nomeadamente por parte da autoridade de controlo referida no artigo 30º, previamente a um recurso contencioso, os Estados-Membros estabelecerão que qualquer pessoa poderá recorrer judicialmente em caso de violação dos direitos garantidos pela legislação nacional aplicável nos termos da presente decisão-quadro ao tratamento em questão.

Artigo 28º
Responsabilidade

1. Os Estados-Membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente decisão-quadro tem o direito

de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano não lhe é imputável.

2. Todavia, uma autoridade competente que recebeu dados pessoais da autoridade competente de outro Estado-Membro é responsável perante a parte lesada por danos causados devido ao uso de dados inexactos ou não actualizados. Não pode eximir-se da sua responsabilidade pelo facto de ter recebido de outra autoridade informações inexactas ou não actualizadas. Se for concedida uma indemnização pela autoridade receptora devido à sua utilização de dados inexactos transmitidos ou disponibilizados pela autoridade competente de outro Estado-Membro, esta última reembolsará integralmente a autoridade receptora do montante pago a título de indemnização.

Artigo 29º
Sanções

1. Os Estados-Membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente decisão-quadro e determinarão, nomeadamente, sanções eficazes, proporcionadas e dissuasivas a aplicar em caso de violação das disposições adoptadas nos termos da presente decisão-quadro.

2. Os Estados-Membros determinarão sanções penais eficazes, proporcionadas e dissuasivas para infracções cometidas intencionalmente de carácter grave a disposições adoptadas nos termos da presente decisão-quadro, nomeadamente as disposições destinadas a garantir a confidencialidade e a segurança do tratamento.

CAPÍTULO VII
AUTORIDADE DE CONTROLO E GRUPO DE PROTECÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Artigo 30º
Autoridade de controlo

1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-Membros nos termos da presente decisão-quadro. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas.

2. Cada Estado-Membro estabelecerá que as autoridades de controlo serão consultadas aquando da elaboração de medidas regulamentares ou administrativas relativas à protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais para efeitos da prevenção, investigação, detecção e repressão de infracções penais.

3. Cada autoridade de controlo disporá, nomeadamente:

   – de poderes de inquérito, tais como o poder de aceder aos dados objecto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controlo,

   – de poderes efectivos de intervenção, tais como, por exemplo, o de emitir pareceres previamente à realização de tratamentos, em conformidade com o artigo 26º, e

garantir a publicação adequada desses pareceres, o de ordenar o bloqueio, o apagamento ou a destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentos nacionais ou para outras instituições políticas,

– do poder de intervir em processos judiciais no caso de violação das disposições nacionais adoptadas nos termos da presente decisão-quadro ou de levar essas infracções ao conhecimento das autoridades judiciais.

As decisões da autoridade de controlo que lesem interesses são passíveis de recurso jurisdicional.

4. Qualquer pessoa pode apresentar à autoridade de controlo um pedido para protecção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais. A pessoa em causa será informada do seguimento dado ao seu pedido.

5. Cada autoridade de controlo elaborará periodicamente um relatório sobre a sua actividade. O relatório será tornado público.

6. Cada autoridade de controlo é competente, independentemente do direito nacional aplicável ao tratamento em causa, para o exercício no território do seu Estado-Membro dos poderes que lhe foram atribuídos em conformidade com o nº 3. Cada autoridade de controlo pode ser solicitada a exercer os seus poderes por uma autoridade de outro Estado-membro.

7. As autoridades de controlo cooperarão entre si, bem como com as autoridades de controlo criadas ao abrigo do Título VI do Tratado da União Europeia e com a Autoridade Europeia para a Protecção de Dados, na medida do necessário ao desempenho das suas funções, em especial através do intercâmbio de quaisquer informações úteis.

8. Os Estados-Membros determinarão que os membros e agentes das autoridades de controlo fiquem sujeitos, mesmo após a cessação das suas actividades, à obrigação de segredo profissional em relação às informações confidenciais a que tenham acesso.

9. Os poderes da autoridade de controlo não afectam a independência do poder judicial e a decisão tomada por esta autoridade não prejudica a execução das tarefas legítimas do poder judicial no âmbito dos processos penais.

Artigo 31º

Grupo de protecção das pessoas no que respeita ao tratamento de dados pessoais para efeitos de prevenção, investigação, detecção e repressão de infracções penais

1. É criado um Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, detecção e repressão de infracções penais, a seguir designado «o grupo». Tem carácter consultivo e é independente.

2. O grupo é composto por um representante da autoridade ou autoridades de controlo designadas por cada Estado-Membro, por um representante da Autoridade Europeia para a Protecção de Dados, bem como por um representante da Comissão.

Cada membro do grupo será designado pela instituição, autoridade ou autoridades que representa. Sempre que um Estado-membro tiver designado várias autoridades de controlo, estas nomearão um representante comum.

Os presidentes das autoridades comuns de controlo criadas ao abrigo do Título VI do Tratado da União Europeia têm o direito de participar ou de se fazer representar em reuniões do grupo. A ou as autoridades de controlo designadas pela Islândia, Noruega e Suíça terão o direito de se fazer representar em reuniões do grupo de trabalho, na medida em que se trate de questões relativas ao acervo de Schengen.

3. O grupo tomará as suas decisões por maioria simples dos representantes das autoridades de controlo dos Estados-Membros.

4. O grupo elegerá o seu presidente. O mandato do presidente tem uma duração de dois anos e é renovável.

5. O secretariado do grupo será assegurado pela Comissão.

6. O grupo elaborará o seu regulamento interno.

7. O grupo analisará as questões inscritas na ordem de trabalhos pelo seu presidente, quer por iniciativa deste, quer a pedido de um representante das autoridades de controlo, quer ainda a pedido da Comissão, da Autoridade Europeia para a protecção de dados ou dos presidentes das autoridades comuns de controlo.

Artigo 32º
Atribuições

1. O grupo tem por atribuições:

   a) Analisar quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da presente decisão-quadro, com vista a contribuir para a sua aplicação uniforme;

   b) Dar parecer sobre o nível de protecção nos Estados-Membros e em países terceiros e organismos internacionais, nomeadamente a fim de garantir que os dados pessoais são transferidos em conformidade com o disposto no artigo 15º para países terceiros ou organismos internacionais que assegurem um nível adequado de protecção dos dados;

   c) Aconselhar a Comissão e os Estados-Membros sobre quaisquer projectos de alteração da presente decisão-quadro ou sobre quaisquer projectos de medidas adicionais ou específicas a tomar para proteger os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, detecção e repressão de infracções penais, bem como sobre quaisquer outros projectos de medidas com incidência sobre esses direitos e liberdades.

2. Se o grupo verificar que surgem divergências susceptíveis de prejudicar a equivalência da protecção das pessoas no que diz respeito ao tratamento de dados pessoais na União Europeia entre a legislação ou a prática dos Estados-Membros, informará desse facto o Conselho e a Comissão.

3. O grupo pode, por sua própria iniciativa ou por iniciativa da Comissão ou do Conselho, formular recomendações sobre quaisquer questões relativas à protecção das pessoas no que diz respeito ao tratamento de dados pessoais na União Europeia para efeitos da prevenção, investigação, detecção e repressão de infracções penais.

4. Os pareceres e recomendações do grupo serão transmitidos ao Conselho, à Comissão e ao Parlamento Europeu, bem como ao comité referido no artigo 16º.

5. A Comissão informará o grupo, com base nas informações fornecidas pelos Estados-Membros, do seguimento dado aos seus pareceres e recomendações. Para o efeito, elaborará um relatório que será igualmente enviado ao Parlamento Europeu e ao Conselho. O relatório será tornado público. Os Estados-Membros informarão o grupo de quaisquer medidas que tomem nos termos do nº 1.

6. O grupo elaborará um relatório anual sobre a situação da protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, detecção e repressão de infracções penais na União Europeia e nos países terceiros, que será comunicado à Comissão, ao Parlamento Europeu e ao Conselho. O relatório será tornado público.

CAPÍTULO VIII
Disposições finais

Artigo 33º
Alteração da Convenção de Schengen

Para efeitos das questões abrangidas pelo âmbito do Tratado da UE, a presente decisão-quadro substitui os artigos 126º a 130º da Convenção de Aplicação do Acordo de Schengen.

Artigo 34º
Relação com outros instrumentos relativos ao tratamento e protecção de dados pessoais

1. A presente decisão-quadro substitui o artigo 23º da Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia.

2. Qualquer referência à Convenção nº 108 do Conselho da Europa, de 28 de Janeiro de 1981, relativa à protecção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais deve entender-se como uma referência à presente decisão-quadro.

Artigo 35º
Execução

1. Os Estados-Membros tomarão as medidas necessárias para dar cumprimento à presente decisão-quadro até 31 de Dezembro de 2006.

2. Até à mesma data, os Estados-Membros transmitirão ao Secretariado-Geral do Conselho e à Comissão o texto das disposições que transpõem para o direito nacional as obrigações que lhes incumbem por força da presente decisão-quadro, bem como as informações relativas à designação da autoridade ou das autoridades de controlo a que se refere o artigo 29º. Com base nestas informações e num relatório escrito da Comissão, o Conselho examinará, antes de 31 de Dezembro de 2007, em que medida os Estados-Membros tomaram as medidas necessárias para se conformarem com a presente decisão-quadro.

Artigo 36º
Entrada em vigor

A presente decisão-quadro entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas,

Pelo Conselho
O Presidente

ANEXO

FICHA FINANCEIRA LEGISLATIVA

Domínio(s) político (s): Justiça e Assuntos Internos

Actividade(s): 1806 – Criar um verdadeiro espaço de liberdade, de segurança e de justiça em matéria penal e civil.

DESIGNAÇÃO DA ACÇÃO: PROPOSTA DE DECISÃO-QUADRO DO CONSELHO RELATIVA À PROTECÇÃO DOS DADOS PESSOAIS TRATADOS NO ÂMBITO DA COOPERAÇÃO POLICIAL E JUDICIÁRIA EM MATÉRIA PENAL

1. RUBRICA (S) ORÇAMENTAL(IS) + DESIGNAÇÃO(ÕES)

ND

2. DADOS QUANTIFICADOS GLOBAIS

2.1. Dotação total da acção (parte B): milhões de euros em dotações de autorização

ND

2.2. Período de aplicação:

início de 2006

2.3. Estimativa das despesas globais plurianuais:

a) Calendário das dotações de autorização/dotações de pagamento (intervenção financeira) (*ver ponto 6.1.1*)

Milhões de euros (*três casas decimais*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Total
Autorizações							
Pagamentos							

b) Assistência técnica e administrativa (ATA) e despesas de apoio (DDA) (*ver ponto 6.1.2*)

Autorizações							
Pagamentos							

Subtotal a+b							
Autorizações							
Pagamentos							

c) Incidência financeira global dos recursos humanos e outras despesas de funcionamento *(ver pontos 7.2 e 7.3)*

Dotações de autorização/Dotações de pagamento	0,389	0,389	0,389	0,389	0,389	0,389	2,334

TOTAL a+b+c							
Autorizações							
Pagamentos							

2.4. Compatibilidade com a programação financeira e as perspectivas financeiras

ND

2.5. Repercussões financeiras a nível das receitas

Proposta sem implicações financeiras

3. CARACTERÍSTICAS ORÇAMENTAIS

Natureza da despesa		**Nova**	**Contribuição EFTA**	**Participação dos países candidatos**	**Rubrica das PF**
Não obrig.	DND	ND	ND	ND	ND

4. BASE JURÍDICA

Artigos 30º, 31º e nº 2, alínea b), do artigo 34º TUE

5. DESCRIÇÃO E FUNDAMENTAÇÃO

5.1. Necessidade de intervenção comunitária

5.1.1. Objectivos visados

A proposta de decisão-quadro estabelece normas comuns relativas à protecção de dados pessoais tratados pelas autoridades competentes no contexto de actividades previstas no Título VI do Tratado da União Europeia (cooperação policial e judiciária em matéria penal). Autoridades de controlo públicas e independentes controlam a aplicação das disposições nacionais adoptadas por força da presente decisão-quadro nos Estados-Membros. É criado um Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais a nível da UE para efeitos de prevenção, investigação, detecção e repressão de infracções penais, a seguir designado «o grupo». O grupo é composto por um representante da autoridade ou autoridades de controlo designadas por cada Estado-Membro, por um representante da Autoridade Europeia para a Protecção de Dados, bem como por um representante da Comissão. O grupo analisará quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da decisão-quadro, com vista a contribuir para a sua aplicação uniforme; emitirá pareceres sobre o nível de protecção de dados pessoais nos Estados-Membros e em países terceiros e aconselhará a Comissão e os Estados-Membros sobre qualquer projecto de alteração da decisão-quadro, bem

como de quaisquer medidas adicionais ou específicas a tomar para salvaguardar os direitos fundamentais.

Além disso, nos termos do disposto no artigo 16º da decisão-quadro um comité, composto por representantes dos Estados-Membros e presidido por um representante da Comissão, assistirá a Comissão, a fim de avaliar, quando necessário, o nível de protecção dos dados num país terceiro.

5.1.2. Disposições adoptadas decorrentes da avaliação ex ante

Foram consultados representantes dos governos e das autoridades de controlo independentes dos Estados-Membros, bem como da Islândia, da Noruega e da Suíça, a Autoridade Europeia para a Protecção de Dados, a Europol e a Eurojust. Tomando especialmente em consideração diferentes pontos de vista, a Comissão propõe a criação do grupo referido. A fim de proceder a uma estimativa dos eventuais custos resultantes desta medida, a Comissão verificou os custos (despesas de deslocação, apoio administrativo para a preparação e organização de reuniões) actualmente suportados pelo grupo de trabalho criado nos termos do artigo 29º da Directiva 95/46/CE.

5.2. Acção prevista e modalidades de intervenção orçamental

É provável que o grupo se reúna periodicamente em princípio cinco vezes por ano. O comité referido no artigo 16º reunir-se-á, se e sempre que necessário, provavelmente também cinco vezes por ano. Será reembolsado um participante por Estado-Membro e por Estado Schengen (Islândia, Noruega). Poder-se-á obter certas orientações a partir dos grupos criados em conformidade com os artigo 29º e 31º da Directiva 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.

5.3. Modalidades de execução

Todas as reuniões devem ser organizadas e presididas pela Comissão. A Comissão deve fornecer serviços de secretariado para o grupo e para o comité referidos, bem como preparar e organizar as suas reuniões.

6. FINANCIAL IMPACT

6.1. Incidência financeira total na parte B - (relativamente à totalidade do período de programação)

6.1.1. Intervenção financeira

ND

6.1.2. Assistência técnica e administrativa (ATA), despesas de apoio (DDA) e despesas TI (dotações de autorização)

ND

6.2. Cálculo dos custos por medida prevista na parte B (relativamente à totalidade do período de programação)

ND

7. INCIDÊNCIA NOS EFECTIVOS E DESPESAS ADMINISTRATIVAS

O impacto sobre os efectivos e as despesas administrativas será coberto pelos recursos atribuídos à DG chefe de fila no contexto do procedimento anual de afectação de recursos.

A atribuição de postos depende igualmente da atribuição de funções e de recursos no quadro das Perspectivas Financeiras 2007-2013.

7.1. Incidência nos recursos humanos

Tipos de lugares		Efectivos a afectar à gestão da acção mediante a utilização dos recursos existentes e/ou adicionais		Total	Descrição das tarefas decorrentes da acção
		Número de lugares permanentes	Número de lugares temporários		
Funcionários ou agentes temporários	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Fornecimento de apoio administrativo Preparação das reuniões do grupo e do comité
Outros recursos humanos					
Total					

7.2. Incidência financeira global dos recursos humanos

Tipo de recursos humanos	Montante (€)	Método de cálculo *
Funcionários Pessoal provisório	Ano 1: 189 000	1 X 108 000 0,5 X 108 000 0,25 X 108 000 = 189 000
Outros recursos humanos (indicar a rubrica orçamental)		
Total	189 000	

Os montantes correspondem às despesas totais de 12 meses.

7.3. Outras despesas administrativas decorrentes da acção

Rubrica orçamental (n° e designação)	Montante (€)	Modo de cálculo:

Dotação global (título A7) A0701 - Deslocações em serviço A07030 - Reuniões A07031 - Comités obrigatórios A07032 Comités não-obrigatórios A07040 Conferências A0705 - Estudos e consultas Outras despesas (especificar)	200 000	10 reuniões* 27 * 740€
Sistemas de informação (A-5001/A-4300)		
Outras despesas - Parte A (especificar)		
Total	200 000	

Os montantes correspondem às despesas totais de 12 meses.

Especificar o tipo de comité, bem como o grupo a que pertence.

I.	Total anual (7,2 + 7,3)	€389 000
II.	Duração da acção	
III.	Custo total da acção (I x II)	

8. ACOMPANHAMENTO E AVALIAÇÃO

8.1. Sistema de acompanhamento

O grupo e o comité adoptam o seu regulamento interno, incluindo as regras de confidencialidade. O Parlamento Europeu será informado em modalidades análogas às previstas no artigo 7º da Decisão 99/468/CE do Conselho, de 28 de Fevereiro de 1999, que fixa as regras de exercício das competências de execução atribuídas à Comissão (JO L 184 de 17.7.1999, p. 23).

8.2. Modalidades e periodicidade da avaliação prevista

ND

9. MEDIDAS ANTIFRAUDE

ND

XXX