CONSELHO DA UNIÃO EUROPEIA

Bruxelas, 28 de fevereiro de 2014 (28.02) (OR.en)

6762/1/14 REV 1

Dossier interinstitucional: 2012/0011 (COD)

DATAPROTECT 30
JAI 102
MI 191
DRS 26
DAPIX 25
FREMP 28
COMIX 110
CODEC 503

NOTA

de:	Presidência
para:	Conselho
n.º doc. ant.:	17831/13 DATAPROTECT 201 JAI 1149 MI 1166 DRS 223 DAPIX 158 FREMP 209 COMIX 700 CODEC 2973 5879/14 DATAPROTECT 13 JAI 46 MI 91 DRS 14 DAPIX 7 FREMP 12 COMIX 68 CODEC 230 5881/14 DATAPROTECT 15 JAI 48 MI 93 DRS 16 DAPIX 9 FREMP 14 COMIX 70 CODEC 232 1/14 DATAPROTECT 4 JAI 22 MI 38 DRS 7 DAPIX 4 FREMP 4 COMIX 28 CODEC 91
Assunto:	Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados) [primeira leitura] Debate de orientação sobre certas questões

I. Introdução

1. O Conselho ocupa-se com a máxima prioridade do pacote de proteção de dados apresentado pela Comissão em 25 de janeiro de 2012. O pacote de proteção de dados é composto por duas propostas legislativas fundamentadas no artigo 16.º do TFUE. A primeira, respeitante a um regulamento geral de proteção de dados, visa substituir a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A segunda, respeitante a uma diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e demanda judicial de infrações penais ou para execução de sanções penais, e à livre circulação desses dados, visa substituir a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

2. O Conselho Europeu de 24-25 de outubro de 2013, dedicado à economia digital, inovação e serviços, concluiu que "a adoção atempada de um sólido quadro geral da UE em matéria de proteção de dados e da diretiva relativa à cibersegurança é essencial para a realização do mercado único digital até 2015".

3. Nos primeiros dois meses do seu mandato, a Presidência conduziu debates de fundo sobre certos aspetos importantes desta reforma, com base nos trabalhos anteriores das Presidências dinamarquesa, cipriota, irlandesa e lituana. A Presidência dedicou mais de 10 dias de reuniões exclusivamente ao pacote legislativo sobre a proteção de dados (regulamento e diretiva).

4. No debate informal dos Ministros da Justiça, realizado em Atenas em 23-24 de janeiro de 2014, os ministros mostraram-se globalmente satisfeitos com o conteúdo do projeto de regulamento no que toca às questões internacionais e incentivaram a que estes modelos fossem, se possível, reforçados com outros modelos alternativos. Num mundo tão globalizado como o de hoje, essas disposições são essenciais para assegurar a continuidade da elevada proteção proporcionada aos cidadãos da UE, quando estes são alvo de empresas sediadas fora da UE e os seus dados pessoais são transferidos para países terceiros ou organizações internacionais.

5. O regulamento geral de proteção de dados desenvolve o sistema e os princípios comprovados da Diretiva Proteção de Dados (Diretiva 95/46/CE). A Comissão pode decidir, no âmbito da comitologia e com a participação de representantes dos Estados-Membros e do Parlamento Europeu, se é adequado o nível de proteção garantido por países terceiros – incluindo certos territórios ou setores de tratamento – ou por uma organização internacional. Será consultado o Comité Europeu para a Proteção de Dados, que dará o seu parecer. Uma das decisões de adequação adotadas pela Comissão diz respeito a transferências de dados para fins comerciais entre a UE e os EUA (Decisão 250/2000/CE da Comissão), a chamada "decisão porto seguro". A Comissão apresentou em novembro passado uma comunicação sobre o restabelecimento da confiança nos fluxos de dados UE-EUA e mantém um diálogo intenso com os homólogos americanos sobre o regime de porto seguro, a fim de o reforçar até ao verão.

6. O projeto de regulamento prevê ainda que podem ser feitas transferências para países terceiros se o responsável pelo tratamento ou o subcontratante aplicarem as garantias adequadas, inclusive as regras vinculativas para empresas e as cláusulas contratuais. Foi também reforçado o papel dos códigos de conduta e mecanismos de certificação aprovados. Tais transferências deverão ser efetuadas em pé de igualdade com as que são baseadas em decisões de adequação. As transferências também podem ser baseadas em derrogações restritas, em determinadas situações.

7. Tendo em conta os resultados do Conselho de junho de 2013, o Grupo da Proteção de Dados e Intercâmbio de Informações aprofundou a análise de certos aspetos dos capítulos I a IV. Foram extensos os debates sobre o direito à portabilidade dos dados e a constituição de perfis, bem como sobre a pseudonimização e as obrigações do responsável pelo tratamento/subcontratante. Na sequência dos debates, a Presidência procurou adaptar a redação de determinados pontos dos capítulos I a IV.

8. A Presidência apensa (...) o texto sobre o âmbito territorial, o capítulo V (transferências internacionais) e certos pontos importantes dos capítulos I a IV, acima mencionados. O texto constante dos Anexos I e II resulta dos debates havidos sob as Presidências dinamarquesa, cipriota, irlandesa, lituana e grega.

9. Durante a Presidência grega, foram alcançados progressos importantes na negociação deste projeto de regulamento. Prosseguem os debates sobre o mecanismo de balcão único, com base nas indicações dadas pelos ministros nos Conselhos JAI de outubro e dezembro de 2013.

II. Âmbito territorial e princípios essenciais das transferências internacionais

10. Durante o debate informal de Atenas, em janeiro de 2014, os ministros mostraram-se globalmente satisfeitos com o conteúdo do projeto de regulamento no que toca às transferências internacionais e com o âmbito territorial do regulamento, tendo salientado a necessidade de assegurar que as regras da União sejam aplicáveis aos responsáveis pelo tratamento não estabelecidos na UE quando procedem ao tratamento de dados pessoais de residentes da União.

    Os ministros também sublinharam a natureza excecional da transmissão de dados pessoais para países terceiros ou organizações internacionais com base em derrogações (isto é, quando não é baseada em decisões de adequação/garantias adequadas, inclusive regras para as empresas ou cláusulas contratuais), bem como a necessidade de criar salvaguardas para garantir os direitos e liberdades fundamentais no domínio da proteção de dados, tal como consagrado no artigo 8.º da Carta da UE.

    No que respeita a eventuais novos modelos (alternativos) que possam de futuro ser considerados para as transferências internacionais, a Presidência entende que os mesmos se podem inscrever na lógica do sistema – multifacetado mas coerente – agora proposto, que assenta em transferências baseadas em decisões de adequação, garantias adequadas e derrogações, e que recebeu o apoio dos ministros durante os debates informais de Atenas. O presente compromisso tem em conta a evolução futura e oferece suficientes possibilidades de albergar novos modelos baseados em garantias adequadas, que assegurem a proteção dos indivíduos cujos dados sejam transmitidos para o estrangeiro.

III. Disposições fundamentais – Capítulos I a IV

Os quatro tópicos a discutir focam alguns dos mais importantes desenvolvimentos tecnológicos dos últimos anos. Em cada caso, é intuito da Presidência assegurar que o pleno potencial do regulamento proposto seja desenvolvido de forma a fortalecer a confiança no mercado único interno da UE em matéria digital.

Pseudonimização

11. A pseudonimização dos dados pessoais é uma operação vulgar no mundo digital e um dos mais importantes meios de realizar a proteção de dados no contexto de uma abordagem baseada em riscos. É por esse motivo que a pseudonimização deve ser incentivada, continuando tais dados a ser dados pessoais. Os debates a nível técnico conduziram à inclusão da pseudonimização no regulamento, a fim de limitar o impacto nos direitos individuais e aumentar a segurança dos dados. Isso permitirá alcançar o justo equilíbrio entre a proteção dos direitos e liberdades fundamentais das pessoas em questão e a necessidade de os setores público e privado tratarem grandes volumes de dados. Exemplo de pseudonimização será o caso em que os dados médicos de pacientes de cancro passam por um processo de apagamento de elementos diretamente identificadores como sejam os nomes, e atribuição aleatória de números de série a cada paciente, de forma a que a informação resultante possa ser utilizada para fins de investigação médica ou de saúde pública.

Portabilidade dos dados pessoais

12. O objetivo do direito à portabilidade dos dados é permitir que as pessoas transfiram os seus próprios dados pessoais de um prestador de serviços para outro, quando decidem optar por outro prestador (p. ex. transmitir os dados pessoais relacionados com a experiência de trabalho de uma rede social geral para uma rede específica de carreiras profissionais). Os debates revelaram que o direito à portabilidade dos dados é importante para dar às pessoas o controlo dos seus próprios dados, em especial na Internet, e para modernizar o atual enquadramento. A Presidência foi ao encontro das preocupações de certas delegações, retirando o setor público do âmbito de aplicação deste direito e ajustando esse âmbito de forma a evitar a sobrecarga dos responsáveis pelo tratamento de dados. O compromisso assegura a proteção de outras pessoas envolvidas e tem em conta a necessidade de neutralidade tecnológica.

Obrigações dos responsáveis pelo tratamento e dos subcontratantes

13. Hoje em dia os prestadores de serviços têm uma função muito mais importante na economia digital do que em 1995. A recente evolução tecnológica, nomeadamente a computação em nuvem, exige a melhoria e a clarificação das funções e obrigações dos responsáveis e dos subcontratantes (incluindo a subcontratação ulterior) no tratamento de dados. A Presidência procurou clarificar a relação entre os responsáveis pelo tratamento e os subcontratantes, em particular com a inclusão de uma referência a contratos facultativos "normalizados" entre responsáveis pelo tratamento e subcontratantes. Esta orientação obteve apoio durante os debates a nível técnico.

Decisão automatizada com base na constituição de perfis

13. O tratamento de dados pessoais é absolutamente essencial para uma economia assente no conhecimento. Na época digital, muitas atividades económicas têm por base a constituição e a utilização de certos perfis. É assim que a publicidade na Internet, em si própria um importante pilar económico da Internet, tem muitas vezes por base a constituição e a utilização de certos perfis para fins de comercialização. A criação e a utilização de perfis de consumidores também podem ser usadas para proteger os consumidores, por exemplo contra fraudes com cartões de crédito ou outros tipos de fraude em ambiente digital.

Todavia, o tratamento destinado a avaliar (isto é, analisar e prever) certos aspetos relacionados com o desempenho no trabalho, situação económica, saúde, preferências ou interesses pessoais, fiabilidade de comportamento, localização ou deslocações (constituição de perfis) pode implicar graves riscos para os direitos e liberdades das pessoas singulares. A Diretiva de 1995 já contém uma disposição (artigo 15.º) sobre o direito da pessoa a não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados, que tem em conta alguns dos aspetos acima mencionados. Tal decisão poderia abranger atividades como a recusa automática de pedidos de cartão de crédito em linha, sem intervenção humana. Esta disposição visa portanto evitar que as pessoas sejam sujeitas a decisões automatizadas, sem intervenção humana.

O presente compromisso não introduz um regime específico para reger a constituição de perfis enquanto tal. Antes sujeita essa constituição a regras gerais de tratamento de dados pessoais (motivação jurídica do tratamento, princípios de proteção de dados) com garantias específicas (por exemplo, a obrigação de fazer uma avaliação de impacto em certos casos (artigos 33.º e 34.º) ou disposições relativas a determinadas informações a prestar à pessoa em causa. O Comité Europeu para a Proteção de Dados terá a possibilidade de emitir diretrizes neste âmbito.

A Presidência tenciona assegurar que a pessoa singular fica protegida contra decisões tomadas apenas com base num tratamento automatizado, nomeadamente a constituição de perfis que produza efeitos na sua esfera jurídica ou que a afete de modo significativo.

O presente texto procura proibir a tomada de decisões com base num tratamento automatizado, nomeadamente (mas não só) mediante a constituição de perfis, mas não proíbe a criação e utilização de perfis enquanto tal.

Se necessário, devem ser permitidas as decisões automatizadas para a celebração e execução de contratos, com base no consentimento explícito do titular dos dados ou quando tal for explicitamente autorizado pelo direito da União ou pela legislação de um Estado-Membro, , nomeadamente para prevenção da fraude e evasão fiscal e para fins de monitorização.

A constituição de perfis e a decisão automatizada com base em categorias especiais de dados pessoais só devem ser permitidas em condições específicas.

IV. Perguntas

A Presidência está ciente de que o apoio a qualquer das questões é condicional, entendendo-se que nenhuma parte do regulamento pode ter aprovação final até que haja acordo sobre todo o texto do regulamento.

Tendo em conta as considerações que precedem, convida-se o Conselho a

A. *debater se, na sequência dos debates da reunião ministerial informal de Atenas, confirma o seu amplo apoio aos projetos de disposições relativos ao âmbito territorial do Regulamento (artigo 3.º, n.º 2) (ver Anexo I);*

B. *debater se, na sequência dos debates da reunião ministerial informal de Atenas, confirma o seu entendimento dos princípios essenciais do capítulo V (ver Anexo II), como base para o Grupo da Proteção de Dados e Intercâmbio de Informações concluir a discussão técnica deste capítulo*;

C. *confirmar se o Grupo da Proteção de Dados e Intercâmbio de Informações deve continuar os trabalhos com base nos resultados até agora alcançados e a terminar os trabalhos sobre:*
   1) *a pseudonimização como elemento da abordagem baseada em riscos (ver Anexo III),*
   2) *a portabilidade dos dados pessoais para o setor privado (ver Anexo IV),*
   3) *as obrigações dos responsáveis pelo tratamento e dos subcontratantes (ver Anexo V);*

D. *debater se o projeto de regulamento, tal como a Diretiva 95/46/CE, deve*
   a. *limitar-se a regular a tomada de decisão automatizada, nomeadamente (mas não só) baseada em perfis que produzem efeitos jurídicos ou afetam pessoas de modo significativo, ou*
   b. *ou deve prever também um regime específico para a criação e a utilização de perfis.*

ÂMBITO TERRITORIAL

19) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento de dados, ou de um subcontratante, situado na União deve ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado dentro ou fora da União. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal ou de uma filial com personalidade jurídica, não é fator determinante neste contexto.

20) A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que residam na União por um responsável pelo tratamento não estabelecido na União deve ser sujeito ao presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem ou não associadas a um pagamento**(...)**feito na União. A fim de determinar se o responsável pelo tratamento de dados oferece ou não bens ou serviços a esses titulares de dados na União, há que determinar igualmente em que medida é evidente a sua intenção de fazer negócios com titulares de dados residentes num ou mais Estados--Membros da União. O mero facto de estar disponível na União quer um sítio Internet do responsável pelo tratamento dos dados ou de um intermediário quer um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, e/ou a referência a clientes ou utilizadores residentes na União, que podem ser reveladores de que o responsável pelo tratamento dos dados tem a intenção de oferecer bens ou serviços a esses titulares de dados na União**(...)**.

21) O tratamento de dados de titulares residentes na União por um responsável que não esteja estabelecido no seu território deve também ser abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares na União. A fim de determinar se uma atividade de tratamento pode ser considerada "controlo do comportamento" de titulares de dados, deve ser apurado se essas pessoas são seguidas na Internet através de técnicas de tratamento de dados que consistem em aplicar um perfil a uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

22) Se o direito nacional de um Estado-Membro for aplicável por força do direito internacional público, o presente regulamento é aplicável igualmente aos responsáveis pelo tratamento dos dados não estabelecidos na União, por exemplo numa missão diplomática ou num posto consular de um Estado-Membro.

Artigo 3.º

Âmbito territorial

1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento de dados ou de um subcontratante situado no território da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares de dados residentes no território da União, efetuado por um responsável pelo tratamento não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
   a) a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
   b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União Europeia.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento não estabelecido na União, mas num lugar em que se aplique o direito nacional de um Estado-Membro por força do direito internacional público.

_____

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to **recipients in** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to **recipients in** another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

80) The Commission may **(…)** decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of participation in a suitable international data protection system established in third countries or a territory or a processing sector. **The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations.**

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. **The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.**

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. **They should relate in particular to compliance with the general principles relating to personal data processing, the availability of data subject's rights and effective legal remedies are available and the principles of data protection by design and by default.**

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for the protection of (…) reasons of public interest, for example in cases of international data exchange, either spontaneous or on request, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, or between competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. **In the absence of an adequacy decision or of appropriate safeguards, Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…).

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, **in particular on the level of protection in third countries or international organisations,** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

Article 4

Definitions

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(21) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

(…).

Article 41

Transfers with an adequacy decision

1. A transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…), data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…);
   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country, or to which an international organisation is subject, with responsibility for ensuring compliance with the data protection rules **including adequate sanctioning powers** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, **in particular** in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…).** The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

3a. *Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission* **in accordance with the examination procedure referred to in Article 87(2). (…)**

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3). **(…)**

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44. (…)The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards *in a legally binding instrument* with respect to the protection of personal data **or where the controller or the processor has obtained prior authorisation for the transfer by the supervisory authority in accordance with paragraph 5.**

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
   (a) binding corporate rules **referred to in** Article 43; or
   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority pursuant to paragraph 4; or

(e) an approved code of conduct pursuant to Article 38; or

(f) a certification mechanism pursuant to Article 39:

3. A transfer based on *binding corporate rules or standard data protection clauses* as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 (…), the controller or processor shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…).

5. Where, notwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor **(…)**shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).

5a. If the transfer referred to in paragraph 4 (…)is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority*.

Article 43

Transfers by way of binding corporate rules

1. The competent supervisory authority shall *approve binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they:
   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;
   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall **contain a description of** at least the following elements:
   (a) the structure and contact details of the group concerned and of each of its members;
   (b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
   (c) their legally binding nature, both internally and externally;
   (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35, including monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 41, of appropriate safeguards pursuant to Article 42, **or of binding corporate rules pursuant to Article 43** a transfer or a category of transfers of personal data to **a recipient or recipients in** a third country or an international organisation may take place only on condition that:
   (a) the data subject has consented to the proposed transfer, after having been informed **that** such transfers **may pose** *risks* due to the absence of an adequacy decision and appropriate safeguards; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and*, where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. (…)

4. Points (a), (b), (c) **and (h)** of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the national law of the Member State to which the controller is subject. **Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…).

6a. (…)

7. (…).

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;
   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;
   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission **and supervisory authorities** shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VII
SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 66

Tasks of the European Data Protection Board[f]

(referred only the provisions that relate to international transfers)

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

   (cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to **in Article 41**;

   (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

   (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67

Reports

1. (…).

2 The European Data Protection Board *shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

ANEXO III

PSEUDONIMIZAÇÃO

23) Os princípios da proteção de dados devem aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Para determinar se uma pessoa é identificável, importa considerar todos os meios com razoável probabilidade de serem utilizados, quer pelo responsável pelo tratamento quer por qualquer outra pessoa, para identificar direta ou indiretamente a referida pessoa. Para determinar se há uma razoável probabilidade de os meios serem utilizados para identificar a pessoa, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta tanto a tecnologia disponível à data do tratamento dos dados como o desenvolvimento tecnológico. Os princípios da proteção de dados não devem pois aplicar-se às informações anónimas, isto é, informações que não digam respeito a nenhuma pessoa singular identificada ou identificável nem a dados tornados de tal forma anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz por isso respeito ao tratamento das informações anónimas, inclusive para fins estatísticos ou de investigação. Os princípios de proteção de dados não devem por isso ser aplicáveis a pessoas falecidas, a menos que as informações sobre pessoas falecidas estejam relacionadas com uma pessoa singular identificada ou identificável.

Os dados pseudonimizados, que só poderão ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados como informações sobre uma pessoa singular identificável, tendo em conta todos os meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa a fim de identificar a pessoa. Os princípios da proteção de dados devem também aplicar-se nos casos em que uma pessoa pode ser identificada mediante a utilização de informações suplementares, tendo em conta todos os meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa a fim de identificar a pessoa.

39) Constitui um interesse legítimo do responsável pelo tratamento dos dados o tratamento de dados na medida estritamente necessária para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança. Pode estar neste caso o tratamento que vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a atentados de "recusa de serviço" e a danos causados aos sistemas de comunicações informáticas e eletrónicas. **O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Pode considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.**

45) Se os dados tratados pelo responsável pelo tratamento não lhe permitirem identificar uma pessoa singular, (...) esse responsável não deve ser obrigado a obter informações suplementares para identificar o titular dos dados com a única finalidade de respeitar uma disposição do presente regulamento. (…). Todavia, o responsável pelo tratamento dos dados não se deverá recusar a aceitar informações **suplementares** fornecidas pelo titular **a fim de** apoiar o exercício dos seus direitos.

Artigo 4.º

Definições

Para efeitos do presente regulamento, entende-se por:

[...]

3-B. **"Pseudonimização", o tratamento de dados pessoais tratados de forma a que já não possam ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, enquanto essas informações suplementares forem mantidas separadamente e sujeitas a medidas técnicas e organizativas para garantir essa impossibilidade de atribuição.**

Artigo 14.º-A

Informações a facultar quando os dados não forem recolhidos junto do titular

4. Os n.ºs 1 a 3 não se aplicam quando e na medida em que:

b) se comprove a impossibilidade de disponibilizar a informação, ou o esforço envolvido seja desproporcionado ou seja suscetível de tornar impossível ou dificultar seriamente a realização do tratamento; em tais casos, o responsável pelo tratamento dos dados toma as medidas adequadas para proteger os interesses legítimos do titular; ou

Artigo 23.º

Proteção de dados por conceção e por defeito

1. Atendendo à tecnologia disponível e aos custos da sua aplicação, e tendo em conta os riscos para os direitos e liberdades das pessoas causados pela natureza, âmbito ou finalidade do tratamento dos dados, o responsável pelo tratamento (…) aplica (…) medidas técnicas e organizacionais adequadas à atividade de tratamento de dados desenvolvida e aos seus objetivos, incluindo a **pseudonimização dos** dados **pessoais**, de forma a que o tratamento cumpra os requisitos do presente regulamento e (…) proteja os direitos e liberdades do (…) titular dos dados.

Artigo 30.º

Segurança do tratamento

1. Atendendo à tecnologia disponível e aos custos de aplicação, e tendo em conta a natureza, contexto, âmbito e finalidades do tratamento dos dados e os riscos para os direitos e liberdades dos titulares, o responsável pelo tratamento e o subcontratante aplicam medidas técnicas e organizativas adequadas, incluindo a **pseudonimização dos** dados **pessoais**, para assegurar um nível de segurança adequado a esses riscos.

Artigo 32.º

Comunicação de uma violação de dados pessoais ao titular dos dados

3. A comunicação (...) ao titular dos dados a que se refere o n.º 1 não é exigida se:

   a. o responsável pelo tratamento dos dados (...) tiver aplicado medidas tecnológicas de proteção adequadas e (...) essas medidas tiverem sido aplicadas aos dados afetados pela violação de dados pessoais, especialmente medidas que tornem os dados incompreensíveis para qualquer pessoa que não esteja autorizada a aceder a esses dados, tais como a cifragem (...); ou

Artigo 38.º

Códigos de conduta

1-A. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento dos dados ou de subcontratantes podem elaborar códigos de conduta, alterar ou aumentar esses códigos, a fim de especificar a aplicação de certas disposições do presente regulamento, tais como:

b-B) a **pseudonimização dos** dados **pessoais**;

ANEXO IV

PORTABILIDADE DOS DADOS PESSOAIS

51) As pessoas singulares devem ter o direito de acesso aos dados recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a licitude do tratamento. Nisso se inclui o seu direito de aceder aos dados pessoais sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações médicas e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deve ter o direito de conhecer e ser informado, em especial, das finalidades a que se destinam os dados tratados, se possível, da duração da sua conservação, da identidade dos destinatários, da lógica subjacente ao eventual tratamento automático dos dados e das suas possíveis consequências, pelo menos quando tiver por base a constituição de perfis. Este direito não deve prejudicar os direitos e as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o suporte lógico. Todavia, estas considerações não devem resultar na recusa total de prestação de informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informações relativas ao titular dos dados, pode solicitar que, antes de as informações serem fornecidas, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido. **Para reforçar melhor o direito de acesso dos titulares aos seus próprios dados, os titulares dos dados deverão ter o direito, sempre que os dados pessoais sejam objeto de tratamento automatizado num formato estruturado e de uso corrente, de obter uma cópia dos dados que lhes digam respeito, igualmente num formato eletrónico de uso corrente.**

55) Para reforçar melhor o controlo sobre os seus próprios dados **(...)**, quando os dados pessoais sejam objeto de tratamento automatizado, os titulares dos mesmos devem ser autorizados a retirar os dados pessoais que tenham fornecido, **num formato de uso corrente**, de um sistema de tratamento automatizado e a transmitir esses dados, (...) a outro **sistema de tratamento automatizado**.

Esse **direito** é aplicável se o titular dos dados os tiver fornecido a um sistema de tratamento automatizado com base no seu consentimento ou em cumprimento de um contrato.

Não é aplicável se o tratamento se basear noutro fundamento legal que não seja o consentimento ou um contrato. **Por natureza própria, este direito não deverá ser exercido em relação aos responsáveis pelo tratamento dos dados no exercício das suas funções públicas. Por conseguinte, não é aplicável especialmente quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de funções de interesse público ou para o exercício de funções públicas de que esteja investido o responsável.**

Quando um conjunto de dados pessoais disser respeito a mais de um titular, o direito de retirar os dados e de os transmitir a outro sistema de tratamento automatizado **não deverá prejudicar o requisito de legitimidade do tratamento de dados pessoais relacionados com outro titular, nos termos do presente regulamento**. **Esse direito também não deverá prejudicar o direito de um titular obter o apagamento dos dados pessoais nem as limitações a esse direito estabelecidas no presente regulamento e**, **especialmente, não** deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que esses dados sejam necessários para a execução desse contrato e enquanto o forem. **(…).**

Artigo 18.º

Direito à portabilidade dos dados

1. (…).

2. Se o titular tiver fornecido dados pessoais e o tratamento dos mesmos, (…) baseado no consentimento ou num contrato, for efetuado num sistema de tratamento automático [fornecido por um serviço da sociedade da informação], tem o direito de retirar esses dados num **formato de uso corrente** e de os transmitir para outro sistema de tratamento automático sem que o responsável a quem se retiram os dados pessoais o possa impedir, **sem prejuízo do artigo 17.º**.

2-A. O direito a que se refere o n.º 2 aplica-se sem prejuízo dos direitos de propriedade intelectual **em relação ao tratamento dos dados nos sistemas de tratamento automático**.

[2-B. O direito a que se refere o n.º 2 não é aplicável ao tratamento com base no artigo 6.º, n.º 1, alíneas c), d), e) f).]

[3. A Comissão pode (…) estabelecer normas técnicas, modalidades e procedimentos para a transmissão de dados pessoais, nos termos do n.º 2. Os atos de execução correspondentes são adotados em conformidade com o procedimento de exame referido no artigo 87.º, n.º 2.]

4. (…).

ANEXO V

OBRIGAÇÕES DOS RESPONSÁVEIS PELO TRATAMENTO E DOS SUBCONTRATANTES

63-A) Para assegurar o cumprimento do presente regulamento no que se refere ao tratamento a efetuar pelo subcontratante por conta do responsável pelo tratamento, quando confiar atividades de tratamento a um subcontratante, o responsável pelo tratamento deverá recorrer exclusivamente a subcontratantes que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do presente regulamento, nomeadamente no que se refere à segurança do tratamento. Essas garantias suficientes podem ser demonstradas pelo facto de o subcontratante cumprir um código de conduta ou um mecanismo de certificação. A realização de operações de tratamento de dados em subcontratação é regulada por um contrato ou por outro ato jurídico que vincule o subcontratante ao responsável pelo tratamento, em que é estabelecido o objeto e a duração do contrato, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e os riscos que podem correr os direitos e liberdades do titular dos dados. O responsável pelo tratamento dos dados e o subcontratante podem optar por utilizar um contrato individual ou cláusulas contratuais-tipo que são adotadas pela Comissão ou por uma autoridade de controlo em conformidade com o mecanismo de controlo da coerência e adotadas pela Comissão, ou que fazem parte de uma certificação concedida no âmbito do mecanismo de certificação. Se um subcontratante proceder ao tratamento de dados pessoais de forma diferente da que foi definida nas instruções do responsável pelo tratamento, o subcontratante é considerado responsável quanto a esse tratamento. Após a conclusão do tratamento por conta do responsável, o subcontratante deverá devolver ou apagar os dados pessoais, a menos que exista um requisito de conservação dos dados no direito da União ou na legislação do Estado-Membro a que o subcontratante está sujeito; nesse caso, o subcontratante deverá aplicar medidas adequadas para assegurar a segurança e confidencialidade dos dados pessoais e não deverá continuar a tratar ativamente esses dados pessoais.

Artigo 26.º

Subcontratante

1. (...) O responsável pelo tratamento de dados recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas (...) de forma a que o tratamento seja conforme com os requisitos do presente Regulamento (...).

1-A. A apresentação de garantias suficientes a que se referem os n.ºs 1 e 2 pode ser demonstrada pelo facto de o respeito **pelo subcontratante** cumprir um código de conduta nos termos do artigo 38.º ou um mecanismo de certificação nos termos do artigo 39.º.

2. A realização de operações de tratamento de dados em subcontratação é regulada por um contrato ou por outro ato jurídico que vincule o subcontratante ao responsável pelo tratamento, e em que é estabelecido o objeto e a duração do contrato, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e em que se prevê, designadamente, que o subcontratante deve:

a) tratar os dados pessoais apenas mediante instruções do responsável pelo tratamento (...), a menos que seja obrigado a fazê-lo pelo direito da União ou pela legislação do Estado-Membro a que está sujeito, devendo nesse caso notificar o responsável pelo tratamento, a menos que o direito da União ou a legislação do Estado-Membro a que o subcontratante está sujeito proíba tal notificação por motivos importantes de interesse público**;**

b) (…)

c) adotar todas (...) as medidas exigidas nos termos do artigo 30.º;

d) determinar as condições para o recrutamento de outro subcontratante (...), tais como um requisito de consentimento prévio específico do responsável pelo tratamento;

e) na medida do (...) possível, tendo em conta a natureza do tratamento, prestar assistência ao responsável pelo tratamento naresposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no Capítulo III;

f) determinar de que modo deve ser prestada assistência ao responsável pelo tratamento dos dados no cumprimento das obrigações previstas nos artigos 30.º a 34.º;

g) devolver ou apagar, consoante a escolha do responsável pelo tratamento, os dados pessoais depois de concluído o tratamento especificado no contrato ou outro ato jurídico, a menos que seja exigida a armazenagem dos dados ao abrigo do direito da União ou da legislação do Estado-Membro a que o subcontratante está sujeito; nesse caso, o subcontratante aplica medidas adequadas para assegurar a segurança e confidencialidade das dados pessoais;

h) disponibilizar ao responsável pelo tratamento dos dados (...) todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo.

2-A. Caso um subcontratante recorra a um subcontratante ulterior para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, o subcontratante ulterior apresenta garantias suficientes de execução de medidas técnicas e organizativas adequadas (...) de forma a que o tratamento seja conforme com os requisitos do presente regulamento.

2-A-A. Caso um subcontratante recorra a um subcontratante ulterior para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, com um contrato ou outro ato jurídico, são impostas ao subcontratante ulterior as mesmas obrigações que as estabelecidas no contrato ou outro ato jurídico entre o responsável pelo tratamento e o subcontratante a que se refere o n.º 2.

2-A-B. Sem prejuízo de um contrato individual entre o responsável pelo tratamento e o subcontratante, o contrato ou outro ato jurídico referidos nos n.ºs 2 e 2-A-A podem ser baseados, totalmente ou em parte, nas cláusulas contratuais-tipo referidas nos n.ºs 2-B e 2-C ou em cláusulas contratuais-tipo que fazem parte de uma certificação concedida ao responsável pelo tratamento dos dados ou ao subcontratante por força dos artigos 39.º e 39.º-A.

2-B. A Comissão pode estabelecer cláusulas contratuais-tipo para as matérias referidas no n.º 2 e de acordo com o procedimento de exame referido no artigo 87.º, n.º 2.

2-C. A autoridade de controlo pode estabelecer cláusulas contratuais-tipo para as matérias referidas no n.º 2 e de acordo com o procedimento de exame referido no artigo 57.º.

3. O contrato ou outro ato jurídico referidos nos n.ºs 2 e 2-A serão efetuados por escrito ou num formato eletrónico ou noutro formato não legível que possa ser convertido num formato legível.

4. (…)

5. (…)