RECOMENDAÇÕES

RECOMENDAÇÃO DA COMISSÃO

de 1 de Março de 2011

sobre orientações para a aplicação das regras de protecção de dados no Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS)

(2011/136/UE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

(1) O Regulamento (CE) n.º 2006/2004 do Parlamento Europeu e do Conselho, de 27 de Outubro de 2004, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor («regulamento relativo à cooperação no domínio da defesa do consumidor») [1] (em seguida designado «Regulamento CPC») pretende aumentar a cooperação em matéria de aplicação das leis de defesa do consumidor no mercado único, institui uma rede europeia de autoridades públicas de aplicação da lei (em seguida designada «rede CPC») e estabelece o quadro e as condições gerais que devem reger a cooperação entre os Estados-Membros, para proteger o interesse económico colectivo dos consumidores.

(2) A cooperação entre as autoridades públicas nacionais responsáveis pela aplicação da lei é vital para o eficaz funcionamento do mercado único e para que cada autoridade possa, no âmbito da rede CPC, pedir assistência às suas homólogas para investigar possíveis incumprimentos das leis da UE em matéria de defesa dos consumidores.

(3) O objectivo do Sistema de Cooperação no domínio da Defesa do Consumidor (em seguida designado «CPCS») é fazer com que as autoridades públicas de aplicação da lei possam trocar informação relativa a possíveis incumprimentos das leis de defesa do consumidor no âmbito de uma estrutura que dê garantias de segurança.

(4) O intercâmbio electrónico de informações entre os Estados-Membros deve respeitar as regras em matéria de protecção de dados pessoais estabelecidas na 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 [2] (em seguida designada «Directiva de Protecção de Dados», e no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [3] (em seguida designado «Regulamento de Protecção de Dados»).

(5) O artigo 8.º da Carta dos Direitos Fundamentais da União Europeia reconhece o direito à protecção dos dados. O CPCS deve garantir que as várias responsabilidades e obrigações partilhadas entre a Comissão e os Estados-Membros no que respeita às regras de protecção de dados sejam claras e que as pessoas em causa sejam informadas e tenham facilmente acesso a mecanismos que lhes permitam fazer valer os seus direitos.

(6) Convém estabelecer orientações para a aplicação das regras de protecção de dados no CPCS (em seguida designadas as «orientações»), para garantir o respeito pelas regras de protecção dos dados tratados pelo CPCS.

(7) Os funcionários responsáveis pela aplicação da lei devem contactar as respectivas autoridades nacionais de protecção de dados para serem enquadrados e aconselhados sobre a melhor maneira de aplicar as presentes orientações, em conformidade com a legislação nacional, e, se necessário, para garantir que o tratamento efectuado pelo CPCS é precedido por notificações e verificações realizadas a nível nacional.

(8) A participação nas acções de formação que serão organizadas pela Comissão para facilitar a aplicação destas orientações é veementemente encorajada.

(9) A informação facultada à Comissão sobre a aplicação das presentes orientações deve ser apresentada, o mais tardar, dois anos depois da adopção da presente recomendação. A Comissão fará uma avaliação posterior da situação em matéria de protecção de dados no CPCS e decidirá se são necessários instrumentos complementares, incluindo medidas regulamentares.

[1] JO L 364 de 9.12.2004, p. 1.
[2] JO L 281 de 23.11.1995, p. 31.
[3] JO L 8 de 12.1.2001, p. 1.

(10) Convém tomar medidas para facilitar a aplicação das orientações por parte dos intervenientes e utilizadores do CPCS. As autoridades nacionais de protecção de dados e a Autoridade Europeia para a Protecção de Dados (AEPD) devem seguir atentamente a evolução e a aplicação das salvaguardas em matéria de protecção de dados no âmbito do CPCS.

(11) As orientações complementam a Decisão 2007/76/CE [1] da Comissão e têm em consideração o parecer do Grupo de Trabalho sobre a protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, instituído ao abrigo do artigo 29.º [2] da Directiva de Protecção de Dados e o parecer da Autoridade Europeia para a Protecção de Dados [3] criada pelo artigo 41.º do Regulamento de Protecção de Dados (em seguida designada «AEPD»),

ADOPTOU A PRESENTE RECOMENDAÇÃO:

Os Estados-Membros devem seguir as orientações em anexo.

Feito em Bruxelas, em 1 de Março de 2011.

Pela Comissão
John DALLI
Membro da Comissão

[1] JO L 32 de 6.2.2007, p. 192.
[2] Parecer 6/2007 sobre questões relativas à protecção de dados relacionadas com o Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS) 01910/2007/EN – WP 130, adoptado em 21 de Setembro de 2007.
[3] Parecer da AEPD, Ref. 2010-0692.

ANEXO

Orientações para a aplicação das regras de protecção de dados no Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS)

1. INTRODUÇÃO

A cooperação entre as autoridades nacionais de defesa do consumidor é vital para o bom funcionamento do mercado interno, uma vez que a inobservância da legislação no âmbito de casos transfronteiriços abala a confiança dos consumidores nas ofertas transfronteiriças e, por conseguinte, a sua fé no mercado interno, além de causar uma distorção da concorrência.

O CPCS é uma ferramenta electrónica instituída pelo Regulamento CPC e constitui um mecanismo estruturado para o intercâmbio de informações entre as autoridades nacionais de defesa do consumidor que compõem a rede CPC. Permite às autoridades públicas pedir assistência às suas homólogas da rede CPC para investigar e remediar possíveis infracções às leis da UE em matéria de defesa do consumidor, bem como tomar medidas para pôr cobro a práticas ilegais de venda ou prestação de serviços cujos destinatários são os consumidores que vivem noutros países da UE. Os pedidos de informação e toda a comunicação entre as autoridades públicas competentes relativos à aplicação do Regulamento CPC são realizados através do CPCS.

O objectivo do Regulamento CPC é reforçar a aplicação das leis de defesa do consumidor no mercado interno, criando em toda a UE uma rede de autoridades públicas nacionais responsáveis pela aplicação da lei, e estabelecer as condições que regem a cooperação entre os Estados-Membros. O Regulamento CPC estabelece que tais intercâmbios de informação e pedidos de assistência mútua entre as referidas autoridades nacionais sejam efectuados por intermédio de uma base de dados determinada. O CPCS foi, pois, concebido para facilitar a cooperação administrativa e o intercâmbio de informação com vista a reforçar a aplicação das leis da UE em matéria de defesa do consumidor.

O âmbito de cooperação limita-se a infracções intracomunitárias aos actos jurídicos constantes do anexo do Regulamento CPC que protege os interesses económicos colectivos dos consumidores.

2. ÂMBITO E OBJECTIVO DAS PRESENTES ORIENTAÇÕES

As presentes orientações abordam uma questão fundamental, ou seja, assegurar o equilíbrio entre uma cooperação eficaz e eficiente das autoridades nacionais competentes e o respeito pelo direito fundamental à privacidade.

A Directiva de Protecção de Dados [1] define dados pessoais como qualquer informação relativa a uma pessoa singular identificada ou identificável; 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.

Uma vez que os funcionários nacionais responsáveis pela aplicação da lei (responsáveis pelos casos) que utilizam o CPCS nem sempre são peritos em protecção de dados e podem não estar suficientemente informados sobre os requisitos impostos pela sua própria legislação nacional na matéria, é conveniente fornecer-lhes orientações sobre o funcionamento do CPCS, de um ponto de vista prático, relativamente à protecção dos dados e às salvaguardas inerentes ao sistema, bem como relativamente aos riscos possíveis associados à sua utilização.

As orientações apresentam os aspectos mais importantes da protecção de dados no quadro do CPCS e facultam explicações fáceis para que todos os utilizadores do CPCS as possam entender. Contudo, não fazem uma análise exaustiva das implicações que a protecção de dados possa ter para o CPCS.

Recomenda-se que as autoridades responsáveis pela protecção de dados nos Estados-Membros sejam consultadas para garantir que as presentes orientações possam ser complementadas com as obrigações específicas estabelecidas na respectiva legislação nacional. Os utilizadores do CPCS podem obter assistência e apoio suplementares junto das referidas autoridades para assegurar o cumprimento dos requisitos na matéria. A lista das autoridades, bem como os respectivos contactos e sítios *web*, pode ser consultada em:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/#eu

Sublinha-se que o tratamento de dados pessoais deve ser feito no respeito dos princípios e condições específicos estabelecidos na Directiva de Protecção de Dados. No contexto do Regulamento CPC, os responsáveis pelos casos podem trocar dados por intermédio do CPCS, incluindo dados pessoais, se o objectivo do tratamento for o de pôr cobro às infracções às leis da UE em matéria de defesa dos consumidores, como consta do anexo ao mesmo regulamento. Contudo, antes de tratar tais dados, deve ser feita uma avaliação cuidadosa para determinar se o tratamento dos dados é indispensável para alcançar os objectivos do Regulamento CPC.

[1] Artigo 2.º, alínea a).

Assim, os responsáveis pelos casos que têm acesso ao CPCS devem realizar uma avaliação casuística antes de qualquer tratamento de dados [1]. O objectivo das presentes orientações é ajudar os responsáveis pelos casos a fazerem esta avaliação, dando-lhes a conhecer alguns princípios de protecção de dados que devem ser tidos em consideração.

O objectivo é ainda esclarecer algumas complexidades da estrutura do CPCS no que se refere a operações conjuntas de tratamento e de vigilância, definindo o papel da Comissão e das autoridades competentes dos Estados-Membros enquanto «responsáveis conjuntas» pelo tratamento dos dados que transitam pelo CPCS.

3. O CPCS – UMA FERRAMENTA ELECTRÓNICA PARA COOPERAR NA APLICAÇÃO

O CPCS é uma ferramenta electrónica projectada e mantida pela Comissão em cooperação com os Estados-Membros. É seu objectivo ajudar os Estados-Membros a aplicar, na prática, a legislação da UE em matéria de defesa do consumidor. É utilizada pela rede CPC, composta por autoridades públicas designadas pelos Estados-Membros e por países do EEE, para a cooperação e o intercâmbio de informação no domínio da aplicação das leis de defesa do consumidor, nos termos previstos no Regulamento CPC.

O artigo 10.º do Regulamento CPC dispõe que:

«A Comissão manterá uma base de dados electrónica na qual armazenará e tratará as informações que receber nos termos dos artigos 7.º, 8.º e 9.º Essa base de dados apenas será disponibilizada para consulta pelas autoridades competentes …».

O artigo 12.º, n.º 3, do Regulamento CPC acrescenta:

«Os pedidos de assistência e toda a comunicação de informações serão efectuados por escrito, utilizando um formulário-tipo, e transmitidos por via electrónica através da base de dados referida no artigo 10.º»

O CPCS facilita a cooperação e o intercâmbio de informações limitadas a infracções intracomunitárias às directivas e aos regulamentos constantes no anexo do Regulamento CPC, que abarca vários assuntos, nomeadamente práticas comerciais desleais, vendas à distância, crédito ao consumo, viagens organizadas, cláusulas contratuais abusivas, utilização a tempo parcial de bens imóveis, comércio electrónico e outros. O CPCS não pode ser utilizado para o intercâmbio de informações sobre questões legislativas não especificamente enumeradas nesse anexo.

Exemplos:

I. Um comerciante estabelecido na Bélgica impõe condições desleais nas transacções que realiza com consumidores residentes em França, em violação da directiva relativa às cláusulas abusivas nos contratos. A autoridade francesa responsável pela protecção dos consumidores pode, através do CPCS, solicitar à sua homóloga belga que adopte todas as medidas necessárias disponíveis na Bélgica para que o comerciante cesse imediatamente a infracção intracomunitária.

II. A autoridade dinamarquesa recebe queixas relativas a um sítio *web* que recorre a práticas comerciais fraudulentas e enganosas em detrimento dos consumidores. O sítio *web* está hospedado na Suécia. A autoridade para os consumidores dinamarquesa precisa de informação sobre o sítio *web*. Pode recorrer, por conseguinte, ao CPCS para solicitar informação à autoridade sueca sua homóloga, que é obrigada a fornecê-la.

A informação é introduzida pelos Estados-Membros, conservada no CPCS, acessível aos Estados-Membros a quem se destina e suprimida pela Comissão [2]. O CPCS é utilizado como um repositório e um meio de troca da informação através de um sistema de comunicação eficiente e seguro.

Em termos de dados pessoais, este tipo de base comporta sempre certos riscos para o direito fundamental à sua protecção: partilhar mais dados do que o estritamente necessário para efeitos de uma cooperação eficiente, reter dados que deveriam ter sido suprimidos e manter dados desactualizados ou incorrectos, bem como não garantir que os direitos das pessoas em causa e as obrigações dos responsáveis pelo tratamento são respeitados. Para enfrentar esses riscos é preciso informar e formar os utilizadores do CPCS em matéria de regras de protecção de dados, para que sejam capazes de assegurar o cumprimento da legislação aplicável em matéria de protecção de dados.

4. QUADRO LEGAL E DE SUPERVISÃO DA PROTECÇÃO DE DADOS

A União Europeia possui um quadro jurídico em matéria de protecção de dados desde 1995: a Directiva de Protecção de Dados [3] que rege o tratamento de dados pessoais pelos Estados-Membros e o Regulamento de Protecção de Dados [4] que rege o tratamento dos dados pessoais pelas instituições e organismos da União Europeia. A aplicação de legislação em matéria de protecção de dados depende actualmente da identidade do interveniente no CPCS ou do utilizador do sistema.

[1] Saliente-se que os princípios de protecção se aplicam tanto a dados conservados electronicamente como em papel.
[2] As regras específicas sobre supressão podem ser consultadas em: Decisão 2007/76/CE e «Rede de Cooperação no domínio da Defesa do Consumidor: regras de funcionamento».
[3] Directiva 95/46/CE.
[4] Regulamento (CE) n.º 45/2001.

As operações de tratamento empreendidas pela Comissão regem-se pelo Regulamento de Protecção de Dados e as empreendidas pelos funcionários das autoridades nacionais competentes regem-se pelas leis nacionais que transpõem a Directiva de Protecção de Dados.

Uma vez que ambas são intervenientes principais com papéis específicos a desempenhar no CPCS, a Comissão e as autoridades competentes designadas são também as responsáveis conjuntas pelo tratamento pelo que devem notificar e submeter as suas operações de tratamento ao controlo prévio das autoridades de supervisão competentes. As legislações nacionais de transposição da Directiva de Protecção de Dados, porém, podem prever derrogações aos requisitos de notificação e verificação prévias.

A harmonização da legislação em matéria de protecção de dados pretende assegurar um nível elevado de protecção e salvaguardar os direitos fundamentais das pessoas, sem impedir a livre circulação de dados pessoais entre os Estados-Membros. Dado que as medidas nacionais de execução podem comportar diferenças, para garantir o cumprimento das regras de protecção de dados, os utilizadores do CPCS são vivamente aconselhados a discutir as presentes orientações com as suas autoridades nacionais de protecção de dados, uma vez que as regras podem variar, por exemplo, quanto à informação a facultar às pessoas ou quanto à obrigação de notificar certas operações de tratamento às autoridades responsáveis pela protecção de dados.

Uma característica significativa do quadro jurídico da UE em matéria de protecção de dados é o facto de a supervisão ser desempenhada por autoridades independentes responsáveis pela protecção de dados. Os cidadãos têm o direito de apresentar queixas a estas autoridades e de resolver prontamente as suas preocupações de protecção de dados sem ter de recorrer aos tribunais. O tratamento de dados pessoais a nível nacional é supervisionado pelas autoridades nacionais responsáveis pela protecção de dados e o tratamento de dados pessoais realizado pelas instituições europeias é supervisionado pela Autoridade Europeia para a Protecção de Dados (AEPD) [1]. Consequentemente, a Comissão está sujeita à supervisão da AEPD e os outros utilizadores do CPCS à supervisão das autoridades nacionais de protecção de dados.

5. QUEM É QUEM NO CPCS? – A QUESTÃO DA RESPONSABILIDADE CONJUNTA PELO TRATAMENTO

O CPCS é um exemplo claro de tratamento conjunto cuja responsabilidade é também conjunta. Por exemplo, enquanto apenas as autoridades competentes nos Estados-Membros recolhem, registam, comunicam e trocam dados pessoais, a conservação e a eliminação desses dados nos seus servidores é da responsabilidade da Comissão. A Comissão não tem acesso a estes dados pessoais mas é considerada o gestor e o operador do sistema.

Consequentemente, a atribuição das diferentes tarefas e responsabilidades entre a Comissão e os Estados-Membros pode resumir-se do seguinte modo:

— cada autoridade competente é responsável pelas suas próprias actividades de tratamento de dados,

— a Comissão não é um utilizador, mas sim o operador do sistema, antes de mais responsável pela sua manutenção e segurança; contudo, a Comissão tem igualmente acesso aos alertas, à informação obtida em retorno e à informação sobre outros casos [2]. O objectivo do acesso da Comissão é acompanhar a aplicação do Regulamento CPC, bem como a legislação em matéria de defesa do consumidor referida no anexo do Regulamento CPC, e compilar informação estatística relacionada com o desempenho desses deveres. A Comissão, contudo, não tem acesso à informação contida em pedidos de assistência mútua nem de aplicação da legislação, que apenas são dirigidos às autoridades competentes dos Estados-Membros responsáveis pelo caso específico em questão. O Regulamento CPC prevê a possibilidade de a Comissão intervir junto das autoridades competentes para dirimir certos litígios [3] e ser convidada a participar em investigações coordenadas que envolvam mais do que dois Estados-Membros [4],

— os participantes no CPCS partilham responsabilidades no que diz respeito à legitimidade do tratamento, às disposições em matéria de notificação e direitos de acesso, oposição e rectificação,

— a Comissão e as autoridades competentes responsáveis pelo tratamento de dados são individualmente responsáveis pela garantia de que as regras seguidas pelas suas operações de tratamento de dados são compatíveis com as regras em matéria de protecção de dados.

6. INTERVENIENTES E UTILIZADORES DO CPCS

No CPCS existem perfis de acesso diferentes: o perfil de acesso à base de dados está limitado e atribuído a um só funcionário, nomeado pela autoridade competente (utilizador autenticado), e não é transferível. Os pedidos de acesso ao CPCS só podem ser concedidos aos funcionários notificados à Comissão pelas autoridades competentes dos Estados-Membros. Para entrar no sistema, é obrigatória uma inscrição/senha, que só pode ser obtida por um único serviço de ligação.

Só os utilizadores das autoridades competentes, as que solicitam e as que facultam assistência, têm pleno acesso à informação completa trocada no âmbito de um dado caso, incluindo todos os anexos do respectivo ficheiro no CPCS. Os serviços de ligação só podem ler informação fundamental sobre os casos se tal lhes for necessário para identificar a autoridade que deve receber o pedido. Não podem ler documentos confidenciais anexados a um pedido ou alerta.

[1] http://www.edps.europa.eu/EDPSWEB/edps/EDPS
[2] Artigos 8.º, 9.º e 15.º do Regulamento (CE) n.º 2006/2004.
[3] Artigo 8.º, n.º 5, do Regulamento (CE) n.º 2006/2004.
[4] Artigo 9.º do Regulamento (CE) n.º 2006/2004.

No caso de pedidos de aplicação da lei, a informação geral é partilhada entre os utilizadores de todas as autoridades competentes notificadas como responsáveis pelas infracções aos actos legais. Tal é feito através das notificações. Estas devem descrever sucintamente o caso vertente e evitar incluir dados pessoais. Podem ser feitas excepções como, por exemplo, o nome do comerciante ou fornecedor (se for uma pessoa singular).

A Comissão não tem acesso aos pedidos de informação e aplicação da lei nem a documentos confidenciais, mas recebe notificações e alertas.

7. PRINCÍPIOS RELATIVOS À PROTECÇÃO DE DADOS APLICÁVEIS AO INTERCÂMBIO DE INFORMAÇÕES

O tratamento de dados pessoais pelos utilizadores do CPCS nos Estados-Membros só pode realizar-se em condições conformes aos princípios estabelecidos na Directiva de Protecção de Dados. Compete ao responsável pelo tratamento dos dados assegurar que os princípios de protecção de dados são respeitados pelo tratamento a que estes são submetidos no CPCS.

Note-se que as regras em matéria de confidencialidade e protecção de dados se aplicam também ao CPCS. As regras de confidencialidade e o sigilo profissional podem aplicar-se aos dados em geral, mas as regras de protecção de dados estão limitadas aos dados pessoais.

É importante ter em conta que os utilizadores do CPCS nos Estados-Membros são responsáveis por muitas outras operações de tratamento e podem não ser especialistas da protecção de dados. As regras em matéria de protecção de dados no âmbito do CPCS não precisam de ser desnecessariamente complicadas nem representar uma sobrecarga administrativa excessiva. Também não têm de seguir obrigatoriamente um formato único. Relembramos que estas orientações são recomendações para o tratamento de dados pessoais e que nem todos os dados que são objecto de intercâmbio no CPCS são dados pessoais.

Antes de introduzir a informação no CPCS, os funcionários responsáveis pela aplicação da lei têm de verificar se os dados pessoais a comunicar são absolutamente necessários para uma cooperação eficiente e ter em atenção a entidade a quem estão a ser enviados. O responsável pela aplicação da lei tem de perguntar-se se o destinatário precisa de facto da informação para efeitos de alerta ou assistência mútua.

A lista de princípios que a seguir se apresenta visa ajudar os funcionários responsáveis pela aplicação da lei que têm acesso ao CPCS a fazer uma avaliação casuística para determinar se cada operação de tratamento de dados pessoais presentes no sistema cumpre os princípios de protecção de dados. Os funcionários responsáveis pela aplicação da lei deveriam igualmente ter em conta que as derrogações e restrições à aplicação dos princípios de protecção de dados constantes da lista seguinte podem existir a nível nacional, pelo que se aconselha a consulta das autoridades nacionais de protecção de dados [1].

Quais os princípios de protecção de dados a observar?

Os princípios gerais de protecção de dados a observar antes de empreender o tratamento de quaisquer dados pessoais foram retirados da Directiva de Protecção de Dados. Uma vez que a referida directiva foi transposta na legislação nacional, convém que os responsáveis pelos casos consultem as suas autoridades nacionais de protecção de dados sobre a aplicação dos princípios seguintes e que verifiquem se existem derrogações ou restrições à sua aplicação.

Princípio de transparência

De acordo com a Directiva de Protecção de Dados, a pessoa em causa tem direito a ser informada sobre o tratamento dos seus dados. O responsável pelo tratamento deve facultar o seu nome e endereço, a finalidade do tratamento, os destinatários dos dados e qualquer outra informação necessária para garantir à pessoa em causa um tratamento leal dos mesmos [2].

O tratamento de dados pessoais só poderá ser efectuado se [3]:

— a pessoa em causa tiver dado de forma inequívoca o seu consentimento,

— for necessário para a execução de um contrato ou formação do contrato,

— for necessário para cumprir uma obrigação legal,

— for necessário para a protecção de interesses vitais da pessoa em causa,

[1] Artigo 11.º, n.º 2, e artigo 13.º da Directiva 95/46/CE.
[2] Artigos 10.º e 11.º da Directiva 95/46/CE.
[3] Artigo 7.º da Directiva 95/46/CE.

— for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados,

— for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados.

Princípio da legitimidade e da equidade

Os dados pessoais não podem ser recolhidos ou tratados de maneira abusiva ou ilegal, nem devem ser utilizados para finalidades contrárias às estabelecidas no Regulamento CPC. Para que o tratamento seja legal, os responsáveis pelos casos devem assegurar-se de que há razões claras que justificam a necessidade do tratamento. O tratamento deve ser feito para finalidades determinadas, explícitas e legítimas, e os dados não serão posteriormente tratados de forma incompatível com essas finalidades ([1]). Tal só pode ser previsto no Regulamento CPC.

Para que o tratamento seja justo, as pessoas em causa devem ser informadas das finalidades do tratamento e da existência do direito de acesso, de rectificação e de oposição.

Princípio de proporcionalidade, exactidão e períodos de conservação dos dados

Os dados devem ser proporcionados, adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e/ou tratados posteriormente. Os dados devem ser exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para 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 dados pessoais não devem ser conservados mais tempo do que o necessário, numa forma que permita a identificação das pessoas em causa, à luz das finalidades para que foram recolhidos ou tratados. Devem ser criadas salvaguardas adequadas para os dados pessoais conservados durante períodos mais longos e destinados a uma utilização histórica, estatística ou científica.

Os responsáveis pelos casos devem considerar se a informação a processar é absolutamente necessária para alcançar os objectivos fixados.

Princípio de limitação da finalidade do tratamento

Os dados pessoais devem ser recolhidos para finalidades específicas, explícitas e legítimas e não devem ser tratados posteriormente de uma forma incompatível com essas finalidades, bem como ser levados ao conhecimento da pessoa em causa. Os responsáveis pelos casos só devem tratar dados pessoais quando existir um objectivo claro para isso, ou seja, fundamentos jurídicos no Regulamento CPC que justifiquem a transferência.

Direito de acesso

As pessoas em causa têm o direito, em conformidade com a Directiva de Protecção de Dados ([2]), de ser informadas de que os seus dados pessoais estão a ser tratados; das finalidades subjacentes ao tratamento; dos destinatários dos dados e de que têm direitos específicos, ou seja, o direito à informação e à rectificação. As pessoas em causa têm direito a aceder a todos os seus dados pessoais que sejam objecto de tratamento. As pessoas em causa têm igualmente o direito de pedir a rectificação, o apagamento ou o bloqueio de dados incompletos, inexactos ou cujo tratamento não respeite as regras de protecção de dados ([3]).

Dados sensíveis

É proibido o tratamento de dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual, a infracções e condenações penais. Contudo, a Directiva de Protecção de Dados ([4]) estabelece certas derrogações a esta regra, segundo as quais os dados sensíveis podem ser tratados, no respeito por certas condições ([5]). Convém que os utilizadores do CPCS adoptem uma atitude de prudência sempre que tiverem de tratar dados sensíveis ([6]). Os utilizadores do CPCS devem consultar a sua autoridade nacional de protecção de dados para saber se as derrogações se aplicam ao tratamento de dados sensíveis.

Derrogações

A prevenção, a investigação, a detecção e a repressão de infracções penais justificam as derrogações previstas na Directiva de Protecção de Dados. Os responsáveis pelos casos devem consultar a legislação nacional para avaliar se tais derrogações são possíveis e em que condições ([7]). A existirem, tais derrogações devem ser claramente indicadas nas declarações em matéria de política de privacidade de cada autoridade competente.

([1]) Artigo 6.º, n.º 1, alínea b), da Directiva 95/46/CE.
([2]) Artigos 10.º, 11.º e 12.º da Directiva 95/46/CE.
([3]) Artigo 12.º da Directiva 95/46/CE.
([4]) Artigo 8.º, n.º 2, da Directiva 95/46/CE.
([5]) Artigo 8.º da Directiva 95/46/CE.
([6]) Capítulo 4 do anexo da Decisão 2007/76/CE.
([7]) Parecer 6/2007 sobre questões relativas à protecção de dados relacionadas com o Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS) 01910/2007/EN – WP 130, adoptado em 21 de Setembro de 2007, pp 24-26.

Aplicação dos princípios de protecção de dados

A aplicação dos princípios de protecção de dados ao funcionamento do CPCS determina a elaboração das seguintes recomendações:

1. A utilização do CPCS deveria ser estritamente limitada aos objectivos previstos no Regulamento CPC. O artigo 13.º, n.º 1, do Regulamento CPC estabelece que «As informações comunicadas só podem ser utilizadas para garantir o cumprimento da legislação de defesa dos interesses dos consumidores». Estas leis estão enumeradas no anexo do referido regulamento.

2. Recomenda-se que os responsáveis pela aplicação da lei só utilizem a informação obtida a partir de um pedido de assistência mútua ou um alerta para as finalidades relacionadas com esse caso especificamente, no respeito total dos requisitos legais em matéria de protecção de dados, avaliando *ex ante* a necessidade do tratamento num contexto relacionado com o interesse público.

3. As transferências dos dados tratados pelos funcionários responsáveis pela aplicação da lei devem ser avaliadas de modo a determinar casuisticamente os seus destinatários.

4. Os utilizadores do CPCS devem seleccionar cuidadosamente as perguntas que constam dos pedidos de assistência mútua e não solicitar mais dados do que os necessários. Não se trata apenas de uma questão de respeito pelos princípios de qualidade dos dados, mas também de redução da sobrecarga administrativa.

5. A Directiva de Protecção de Dados [1] exige que os dados pessoais sejam exactos e, se necessário, actualizados. Recomenda-se que a autoridade competente que forneceu a informação contribua para garantir a exactidão dos dados conservados no CPCS. Foram acrescentadas mensagens no CPCS para recordar periodicamente aos responsáveis pelos casos que devem verificar se os dados pessoais são exactos e actualizados.

6. Uma maneira prática de informar as pessoas em causa dos seus direitos é a advertência sobre a política em matéria de privacidade divulgada na página *web*. Recomenda-se que cada autoridade competente inclua na respectiva página *web* uma advertência sobre a sua política nesta matéria. Esta advertência deve cumprir os requisitos de informação estabelecidos na Directiva de Protecção de Dados, incluir uma ligação à página *web* da Comissão sobre privacidade e facultar mais pormenores, incluindo os contactos da autoridade competente em questão, bem como informar sobre quaisquer restrições nacionais ao direito de acesso ou de informação. Os responsáveis pelo tratamento dos dados envolvidos são igualmente responsáveis pela publicação destas advertências.

7. A pessoa em causa pode solicitar o acesso, a rectificação e o apagamento dos seus dados pessoais em mais de uma fonte. Embora cada autoridade competente seja responsável, tal como o responsável pelo tratamento, pelas suas próprias operações de tratamento de dados, o objectivo deve ser dar uma resposta coordenada aos pedidos referentes a casos transfronteiriços. Recomenda-se que, em tais casos, as autoridades competentes informem as suas homólogas interessadas de que receberam um pedido.

   Se as autoridades competentes considerarem que a concessão de um pedido pode afectar procedimentos de investigação ou de aplicação da lei a cargo de outras autoridades competentes, devem sondar estas últimas antes de o conceder.

   A pessoa em causa pode igualmente apresentar o seu pedido à Comissão. A Comissão só pode aceder a um pedido de dados se a eles tiver acesso. Após a recepção de um pedido, a Comissão deve consultar a autoridade competente que forneceu a informação. Se não for levantada nenhuma objecção ou se a autoridade competente não puder responder num prazo razoável, a Comissão decide se pode conceder ou não o pedido com base no Regulamento de Protecção de Dados. A Comissão deve igualmente solicitar o parecer de autoridades competentes cujas actividades de investigação ou aplicação da lei possam ser comprometidas pela concessão do pedido. A Comissão deve examinar se a introdução de novas possibilidades técnicas no CPCS virá facilitar tais intercâmbios.

8. A decisão de aplicação do CPC, Decisão 2007/76/CE, prevê a criação, no CPCS, de campos para a identificação de directores de empresas. Os funcionários responsáveis pela aplicação da lei devem avaliar se a inclusão destes dados pessoais é necessária para resolver o caso. Deve ser feita uma avaliação casuística para determinar se a identificação de um director de uma empresa deve figurar no campo de dados criado para o efeito, antes de se introduzirem as informações no CPCS e antes de os pedidos de assistência mútua ou alerta serem enviados a outra autoridade competente.

9. A decisão de aplicação do CPC, Decisão 2007/76/CE, exige que a autoridade competente que introduz informações, pedidos de aplicação da legislação ou alertas indique se as informações têm de ser objecto de tratamento confidencial. Esta selecção é feita numa base casuística. De igual modo, quando fornece informações, a autoridade requerida tem de indicar se estas devem ser objecto de tratamento confidencial. O sistema CPCS inclui um parâmetro por defeito destinado a permitir aos seus utilizadores conceder o acesso a documentos, desactivando o ícone de confidencialidade.

[1] Artigo 6.º, n.º 1, alínea d), da Directiva 95/46/CE.

8. O CPCS E A PROTECÇÃO DE DADOS

Ambiente informático favorável à protecção de dados

O CPCS foi concebido tendo em conta os requisitos da legislação de protecção de dados:

— o CPCS usa o programa s-TESTA (serviços telemáticos transeuropeus seguros entre administrações). Constitui uma plataforma pan-europeia de comunicação fácil de gerir, fiável e segura para as administrações nacionais e europeia. A rede s-TESTA é baseada numa infra-estrutura dedicada, privada e completamente separada da Internet. O sistema inclui medidas de segurança adequadas para garantir a melhor protecção possível para a rede. A rede está sujeita a uma acreditação de segurança para poder transmitir informação classificada no nível «restrito à UE»,

— para tal, foram introduzidas algumas características técnicas: senhas seguras e personalizadas para os funcionários competentes das autoridades designadas, utilização de uma rede segura (s-TESTA), mensagens para lembrar aos responsáveis pelos casos que devem ter em mente as regras de protecção de dados ao tratar dados pessoais, criação de diferentes perfis de utilizadores que modulam o acesso à informação consoante o papel do utilizador (a autoridade competente, o gabinete de ligação ou a Comissão), possibilidade de limitar o acesso a documentos graças à sua classificação como confidenciais e mensagem de advertência na página de entrada do CPCS que aponta para as regras de protecção de dados,

— normas de execução ([1]) que abrangem aspectos essenciais para assegurar o cumprimento das regras de protecção de dados: regras de supressão claras (qual a informação; como e quando apagar dados); princípios que especificam os tipos de acesso à informação (só as autoridades competentes directamente envolvidas têm pleno acesso, podendo as restantes dispor de informação geral apenas),

— orientações de funcionamento ([2]) que definem os elementos a ter em conta no preenchimento dos diferentes campos e, mais especificamente, as presentes orientações ([3]),

— revisões anuais para assegurar que as autoridades competentes verificam a exactidão dos dados pessoais (está previsto um marcador mas ainda não foi introduzido) e o encerramento e/ou desactivação dos casos tratados, segundo as regras, para que não fiquem esquecidos. A Comissão organiza com os Estados-Membros uma revisão periódica dos casos em aberto durante um período substancialmente superior ao tempo necessário para a sua resolução,

— supressão automática das informações sobre os casos de assistência mútua cinco anos após o seu encerramento, em conformidade com o Regulamento CPC,

— o CPCS é uma ferramenta electrónica evolutiva cujo objectivo é proteger os dados pessoais. O sistema comporta ainda muitos outros elementos de salvaguarda já integrados na arquitectura anteriormente descrita. À medida das necessidades, a Comissão continuará a desenvolver outras melhorias.

Orientação adicional

Durante quanto tempo devem os casos ser tratados e quando devem ser encerrados e suprimidos?

Só a Comissão pode suprimir informação do CPCS ([4]) e, regra geral, fá-lo a pedido da autoridade competente. Ao fazer o pedido de supressão, a autoridade competente tem de especificar as suas razões. A única excepção aplica-se aos pedidos de aplicação da lei. Estes são suprimidos automaticamente pela Comissão cinco anos após o encerramento do caso pela autoridade requerente.

Foram estabelecidas regras com prazos determinados para garantir a supressão de dados desnecessários, inexactos, infundados e/ou conservados durante períodos máximos.

Por que está a retenção de dados fixada em cinco anos?

O objectivo de um período de retenção é facilitar a cooperação entre as autoridades públicas responsáveis pela aplicação das leis em matéria de defesa do consumidor no âmbito do tratamento das infracções intracomunitárias e contribuir para o bom funcionamento do mercado interno, para a qualidade e coerência de aplicação dessas leis, supervisionar a defesa dos interesses económicos dos consumidores e contribuir para aumentar o nível e a coerência dessa aplicação. Durante o período de retenção, os funcionários responsáveis da autoridade competente a quem o caso foi entregue podem ser autorizados a consultar o ficheiro respectivo para investigar possíveis padrões de infracção e contribuir, assim, para reforçar a eficiência da aplicação da lei.

([1]) Decisão 2007/76/CE.
([2]) Rede de Cooperação no domínio da Defesa do Consumidor: regras de funcionamento, adoptadas pelo comité CPC em 8 de Junho de 2010.
([3]) O conteúdo das presentes orientações será integrado em formações futuras sobre o CPCS.
([4]) Artigo 10.º do Regulamento (CE) n.º 2006/2004 e Capítulo 2 do anexo da decisão de execução do CPC, Decisão 2007/76/CE.

Que informação pode ser incluída no fórum de discussão?

O fórum de discussão é um anexo do CPCS e uma ferramenta de intercâmbio de informação no que diz respeito a assuntos como as novas competências de aplicação da lei e as melhores práticas. Regra geral, e embora não seja frequentemente utilizado pelos funcionários responsáveis pela aplicação da lei, o fórum de discussão não deve servir para o intercâmbio de dados relativos aos casos nem deve referir dados pessoais.

Que tipo de dados pode ser incluído nos resumos e documentos anexos?

A decisão de execução do CPC, Decisão 2007/76/CE, prevê o campo «documentos anexos», no caso de alertas e pedidos de informação e de aplicação da lei. Os resumos são feitos em campos onde deve ser apresentada uma descrição da infracção. Recomenda-se que não sejam aí incluídos dados pessoais, uma vez que o objectivo é apenas obter uma descrição geral da infracção. Os dados pessoais que constam dos documentos anexos mas não são estritamente necessários devem ser bloqueados ou removidos.

Que significa uma «suspeita razoável» de infracção?

O conceito de motivo razoável de suspeita é um conceito que deve ser interpretado em conformidade com a legislação nacional. Contudo, recomenda-se que as suspeitas de infracção só sejam incluídas no CPCS se houver provas presentes ou passadas que possam apoiá-las.

E as transferências para países terceiros?

O Regulamento CPC [1] estipula que as informações comunicadas nos termos das suas disposições podem igualmente ser comunicadas a uma autoridade de um país terceiro por um Estado-Membro que tenha um acordo de assistência bilateral, desde que o consentimento da autoridade competente que comunicou originalmente a informação tenha sido obtido e que as condições de protecção de dados estejam reunidas.

Recomenda-se que, se não existir um acordo internacional de assistência mútua [2] entre a União Europeia e um país terceiro, qualquer acordo de assistência bilateral com um país terceiro deve prever salvaguardas de protecção de dados adequadas e ser notificado às autoridades de supervisão relevantes em matéria de protecção de dados, de modo a que possam ser efectuadas verificações prévias, salvo se a Comissão considerar que o referido país terceiro garante um nível de protecção adequado aos dados pessoais transferidos da União, em conformidade com o artigo 25.º da Directiva de Protecção de Dados.

---

[1] Artigos 14.º, n.º 2, do Regulamento (CE) n.º 2006/2004.
[2] Artigo 18.º do Regulamento (CE) n.º 2006/2004.