GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS

16/PT
WP 243 rev.01

Orientações sobre os encarregados da proteção de dados (EPD)

Adotadas em 13 de dezembro de 2016

Com a última redação revista e adotada em 5 de abril de 2017

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

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Estado de Direito) da Comissão Europeia, Direção-Geral da Justiça e dos Consumidores, B-1049 Bruxelas, Bélgica, Gabinete n.º MO59 03/068.

Sítio: http://ec.europa.eu/justice/data-protection/index_en.htm

O GRUPO DE TRABALHO PARA A PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º da referida diretiva,

Tendo em conta o seu regulamento interno,

ADOTOU AS PRESENTES ORIENTAÇÕES:

Índice

1 Introdução

O Regulamento Geral sobre a Proteção de Dados (RGPD)[1], cuja entrada em vigor está prevista para 25 de maio de 2018, proporciona um quadro de cumprimento modernizado e assente na responsabilidade em matéria de proteção de dados na Europa. Os encarregados da proteção de dados (EPD) terão um papel central neste novo quadro normativo relativamente a um vasto número de organizações, facilitando o cumprimento das disposições do RGPD.

Nos termos do RGPD, determinados responsáveis pelo tratamento e subcontratantes devem obrigatoriamente designar um EPD[2]. É o caso de todas as autoridades e organismos públicos (independentemente do tipo de dados que tratam) e de outras organizações cuja atividade principal consista no controlo de pessoas de forma sistemática e em grande escala, ou que tratam de categorias especiais de dados pessoais em larga escala.

Mesmo quando o RGPD não exige especificamente a nomeação de um EPD, as organizações poderão, nalguns casos, considerar conveniente designar um EPD a título voluntário. O Grupo do Artigo 29.º para a Proteção de Dados (GT 29) é favorável a estas iniciativas voluntárias.

O conceito de EPD não é novo. A Diretiva 95/46/CE[3] não obrigava nenhuma organização a nomear um EPD, mas, ainda assim, a prática da nomeação de EPD desenvolveu-se em vários Estados-Membros ao longo dos anos.

Já antes da adoção do RGPD, o GT 29 defendia que a figura do EPD é um pilar da responsabilidade e que a nomeação de um EPD pode facilitar a conformidade e, além disso, propiciar uma vantagem competitiva às empresas[4]. Além de facilitar a conformidade através da implementação de instrumentos de responsabilização (p. ex., viabilizando avaliações de impacto sobre a proteção de dados e efetuando ou viabilizando auditorias), os EPD servem de intermediários entre as partes interessadas (p. ex., as autoridades de controlo, os titulares de dados e as unidades empresariais dentro de uma organização).

Os EPD não são pessoalmente responsáveis em caso de incumprimento do disposto no RGPD. O RGPD deixa bem explícito que compete ao responsável pelo tratamento ou ao subcontratante assegurar e poder comprovar que o tratamento é realizado em conformidade com as suas disposições

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016). O RGPD é relevante para efeitos do EEE e será aplicável depois de ser integrado no Acordo EEE.

[2] A nomeação de um EPD é igualmente obrigatória para as autoridades competentes, em conformidade com o artigo 32.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, pp. 89-131), e com a legislação nacional de execução. Embora as presentes orientações incidam nos EPD ao abrigo do RGPD, são igualmente pertinentes para os EPD ao abrigo da Diretiva (UE) 2016/680, no que diz respeito às suas disposições semelhantes.

[3] 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 (JO L 281 de 23.11.1995, p. 31).

[4] Ver: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

(art. 24.º, n.º 1). O cumprimento das regras de proteção de dados é uma competência do responsável pelo tratamento ou do subcontratante.

O papel do responsável pelo tratamento ou do subcontratante é igualmente fundamental no sentido de permitir a prossecução eficaz das atribuições do EPD. A nomeação de um EPD é um primeiro passo, mas os EPD devem igualmente dispor de autonomia e de recursos suficientes para desempenharem eficazmente as suas funções.

O RGPD reconhece o papel essencial do EPD enquanto participante no novo sistema de governação de dados e estabelece as condições aplicáveis à sua nomeação, posição e atribuições. O objetivo das presentes orientações é clarificar as disposições pertinentes no RGPD, a fim de ajudar os responsáveis pelo tratamento e os subcontratantes a cumprirem a legislação, bem como assistir os EPD na sua missão. As orientações preveem igualmente recomendações sobre boas práticas, assentes na experiência adquirida nalguns Estados-Membros da UE. O GT 29 controlará a aplicação das presentes orientações e poderá complementá-las com mais pormenores, se necessário.

2 Designação do EPD

2.1. Designação obrigatória

O artigo 37.º, n.º 1, do RGPD exige a designação de um EPD em três situações específicas[5]:

a) Sempre que o tratamento seja efetuado por uma autoridade ou um organismo público[6];
b) Sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
c) Sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados[7] ou[8] de dados pessoais relacionados com condenações penais e infrações[9].

Nas subsecções que se seguem, o GT 29 fornece linhas de orientação quanto aos critérios e à terminologia utilizada no artigo 37.º, n.º 1.

Excetuando os casos em que seja evidente que uma organização não é obrigada a designar um EPD, o GT 29 recomenda que os responsáveis pelo tratamento e os subcontratantes documentem a análise interna efetuada no sentido de determinar se deve ou não ser nomeado um EPD, com vista a poder comprovar que os fatores pertinentes foram devidamente tomados em consideração[10]. Esta análise faz parte da documentação no âmbito do princípio da responsabilidade. Pode ser solicitada pela autoridade

[5] Saliente-se que, nos termos do artigo 37.º, n.º 4, o direito da União ou dos Estados-Membros poderá igualmente exigir a designação de EPD noutras situações.
[6] Excetuando os tribunais no exercício da sua função jurisdicional. Ver artigo 32.º da Diretiva (UE) 2016/680.
[7] Nos termos do artigo 9.º, estas categorias abrangem os dados pessoais 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 genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
[8] O artigo 37.º, n.º 1, alínea c), utiliza a conjunção *«e»*. A secção 2.1.5 *infra* explica por que motivo é utilizada a conjunção *«ou»* em vez de *«e»*.
[9] Artigo 10.º.
[10] Ver artigo 24.º, n.º 1.

de controlo e deve ser atualizada sempre que necessário, por exemplo, caso os responsáveis pelo tratamento ou os subcontratantes iniciem novas atividades ou prestem novos serviços que poderão ser abrangidos pelo artigo 37.º, n.º 1.

Quando uma organização designa um EPD a título voluntário, os requisitos dos artigos 37.º a 39.º são aplicáveis à sua nomeação, posição e atribuições como se a designação fosse obrigatória.

Nada impede uma organização, que não seja obrigada por lei a designar um EPD e não pretenda designar um EPD a título voluntário, de recorrer, apesar disso, a pessoal ou consultores externos com funções ligadas à proteção dos dados pessoais. Neste caso, é importante assegurar que não há confusão quanto ao seu cargo, estatuto, posição e atribuições. Por conseguinte, deve ficar claro, em todas as comunicações no seio da empresa e com as autoridades de proteção de dados, os titulares de dados e o público em geral, que o cargo deste funcionário ou consultor não corresponde à função de encarregado da proteção de dados (EPD). [11]

O EPD, independentemente de ser designado de forma obrigatória ou voluntária, assume todas as operações de tratamento realizadas pelo responsável pelo tratamento ou pelo subcontratante.

2.1.1 «AUTORIDADE OU ORGANISMO PÚBLICO»

O RGPD não define o que constitui «*uma autoridade ou um organismo público*». O GT 29 considera que este conceito deve ser definido ao abrigo da legislação nacional. Por conseguinte, as autoridades e organismos públicos incluem as autoridades nacionais, regionais e locais, mas o seu conceito, nos termos das legislações nacionais aplicáveis, também engloba, por norma, um conjunto de outros organismos de direito público[12]. Nestes casos, a designação de um EPD é obrigatória.

O desempenho de funções de serviço público e o exercício da autoridade pública[13] podem incumbir não só a autoridades ou organismos públicos, mas também a outras pessoas singulares ou coletivas de direito público ou privado, em setores como os serviços de transportes públicos, o abastecimento de água e energia, as infraestruturas rodoviárias, a radiodifusão de serviço público, a habitação pública ou os órgãos disciplinares de profissões regulamentadas, consoante a legislação de cada Estado-Membro.

Nestes casos, a situação dos titulares de dados pode ser muito semelhante aos contextos em que os seus dados são tratados por uma autoridade ou um organismo público. Concretamente, os dados podem ser tratados para fins similares e as pessoas têm geralmente pouco ou nenhum poder de decisão quanto ao facto de os seus dados serem tratados e de que forma, podendo, por isso, necessitar da proteção adicional que a designação de um EPD pode proporcionar.

Apesar de não haver qualquer obrigação nestes casos, o GT 29 recomenda, à guisa de boa prática, que as organizações privadas que desempenham funções de serviço público ou exercem uma autoridade

---

[11] Tal é igualmente aplicável aos diretores responsáveis pela privacidade ou a outros responsáveis pela proteção da privacidade que já existem atualmente nalgumas empresas, os quais poderão nem sempre preencher os critérios do RGPD, por exemplo no que se refere aos recursos disponíveis ou às garantias de independência. Caso não satisfaçam estes critérios, não podem ser considerados nem intitulados EPD.

[12] Ver, por exemplo, a definição de «*organismo do setor público*» e de «*organismo de direito público*» no artigo 2.º, n.os 1 e 2, da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público (JO L 345 de 31.12.2003, p. 90).

[13] Artigo 6.º, n.º 1, alínea e).

pública designem um EPD. As atividades do EPD abrangem todas as operações de tratamento realizadas, incluindo as que não estão relacionadas com o exercício de atribuições públicas ou funções oficiais (p. ex., gestão de uma base de dados de trabalhadores).

2.1.2 «ATIVIDADES PRINCIPAIS»

O artigo 37.º, n.º 1, alíneas b) e c), do RGPD faz referência às «*atividades principais do responsável pelo tratamento ou do subcontratante*». O considerando 97 especifica que as atividades principais do responsável pelo tratamento dizem respeito às suas «*atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar*». As «atividades principais» podem entender-se como as operações essenciais necessárias para alcançar os objetivos do responsável pelo tratamento ou do subcontratante.

No entanto, a interpretação das «atividades principais» não deve excluir as atividades em que o tratamento de dados constitui uma parte indissociável das atividades do responsável pelo tratamento ou do subcontratante. Por exemplo, a atividade principal de um hospital é a prestação de cuidados de saúde. Contudo, um hospital não poderia prestar cuidados de saúde de forma segura e eficaz sem proceder ao tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes. Assim, o tratamento destes dados deve ser considerado uma das atividades principais de qualquer hospital, cabendo, portanto, aos hospitais nomear encarregados da proteção de dados.

Para dar outro exemplo, uma empresa de segurança privada exerce a vigilância de um conjunto de centros comerciais privados e de espaços públicos. A vigilância é a atividade principal da empresa, que, por sua vez, está indissociavelmente ligada ao tratamento de dados pessoais. Por conseguinte, esta empresa deve igualmente designar um EPD.

Por outro lado, todas as organizações exercem determinadas atividades, por exemplo, a remuneração dos seus trabalhadores ou atividades comuns de apoio informático. Trata-se de exemplos de funções de apoio necessárias para a atividade principal ou a área de negócio central da organização. Embora sejam necessárias ou essenciais, por norma estas atividades são consideradas funções acessórias e não a atividade principal.

2.1.3 «GRANDE ESCALA»

O artigo 37.º, n.º 1, alíneas b) e c), exige que o tratamento de dados pessoais seja realizado em grande escala para que a designação de um EPD se torne obrigatória. O RGPD não define em que consiste o tratamento de grande escala, embora o considerando 91 forneça algumas linhas de orientação[14].

Com efeito, não é possível quantificar um número preciso quanto ao volume de dados tratados ou ao número de pessoas em causa que seria aplicável em todas as situações. Porém, tal não impede que possa ser desenvolvida, com o passar do tempo, uma prática corrente para identificar de forma mais específica e/ou quantitativa o que constitui uma *«grande escala»* relativamente a determinados tipos de atividades de tratamento comuns. O GT 29 planeia igualmente vir a contribuir para este desenvolvimento, através da partilha e da disseminação de limiares exemplificativos aplicáveis à designação do EPD.

Em qualquer caso, o GT 29 recomenda que, em especial, os seguintes fatores sejam tomados em consideração para determinar se o tratamento é efetuado em grande escala:

- O número de titulares de dados afetados – como número concreto ou em percentagem da população em causa
- O volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento
- A duração, ou permanência, da atividade de tratamento de dados
- O âmbito geográfico da atividade de tratamento

[14] De acordo com o referido considerando, seriam nomeadamente incluídas as *«operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco»*. Por outro lado, este considerando dispõe expressamente que o *«tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado»*. Importa ter em conta que, apesar de o considerando dar exemplos relativos aos extremos da escala (tratamento por um médico por oposição ao tratamento de dados de um país inteiro ou à escala da Europa), existe uma extensa zona cinzenta entre estes dois extremos. Além disso, há que ter presente que este considerando se refere às avaliações do impacto sobre a proteção de dados, o que implica que alguns elementos possam ser específicos deste contexto e não ser necessariamente aplicáveis à nomeação dos EPD nas mesmas modalidades.

Contam-se como exemplos de tratamento de grande escala:

- o tratamento de dados de doentes no exercício normal das atividades de um hospital
- o tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem)
- o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços
- o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco
- o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca
- o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet

Como exemplos que não constituem tratamento de grande escala, incluem-se:

- o tratamento de dados de doentes pacientes por um médico
- o tratamento de dados pessoais relacionados com condenações penais e infrações por um advogado

2.1.4 «CONTROLO REGULAR E SISTEMÁTICO»

A noção de controlo regular e sistemático dos titulares dos dados não está definida no RGPD, mas o conceito de *«controlo do comportamento dos titulares de dados»* é mencionado no considerando 24[15] e inclui claramente todas as formas de seguimento e de definição de perfis na internet, designadamente para fins de publicidade comportamental.

No entanto, a noção de controlo não se cinge ao ambiente em linha e o seguimento em linha deve ser encarado como mero exemplo de controlo do comportamento dos titulares de dados[16].

Na interpretação do GT 29, «regular» significa, neste caso, uma ou mais das seguintes características:

- Contínuo ou que ocorre a intervalos específicos num determinado período
- Recorrente ou repetido em horários estipulados
- Constante ou periódico

Na interpretação do GT 29, «sistemático» significa, neste caso, uma ou mais das seguintes características:

[15] *«A fim de determinar se uma atividade de tratamento pode ser considerada "controlo do comportamento" de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de 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.»*

[16] Saliente-se que o considerando 24 incide especialmente na aplicação extraterritorial do RGPD. Além disso, existe também uma diferença entre *«controlo do seu comportamento»* [art. 3.º, n.º 2, alínea b)] e *«controlo regular e sistemático dos titulares dos dados»* [art. 37.º, n.º 1, alínea b)], que, desta forma, poderia ser entendida como um conceito diferente.

- Que ocorre de acordo com um sistema
- Predefinido, organizado ou metódico
- Realizado no âmbito de um plano geral de recolha de dados
- Efetuado no âmbito de uma estratégia

Exemplos de atividades que podem constituir um controlo regular e sistemático dos titulares de dados: exploração de uma rede de telecomunicações; prestação de serviços de telecomunicações; reorientação de mensagens de correio eletrónico; atividades de promoção comercial baseadas em dados; definição de perfis e pontuação para fins de avaliação dos riscos (p. ex., para efeitos de pontuação de crédito, fixação de prémios de seguro, prevenção de fraudes, deteção de casos de branqueamento de capitais); localização, por exemplo, através de aplicações móveis; programas de fidelização; publicidade comportamental; controlo de dados relativos ao bem-estar, à condição física e à saúde através de usáveis; televisão em circuito fechado; dispositivos conectados, por exemplo, contadores inteligentes, automóveis inteligentes, domótica, etc.

2.1.5 CATEGORIAS ESPECIAIS DE DADOS E DADOS PESSOAIS RELACIONADOS COM CONDENAÇÕES PENAIS E INFRAÇÕES

O artigo 37.º, n.º 1, alínea c), incide no tratamento de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º. Apesar de esta disposição utilizar a conjunção *«e»*, não há nenhuma razão estratégica para que os dois critérios tenham de ser aplicados simultaneamente. Por conseguinte, o texto deve ser interpretado como significando *«ou»*.

2.2. EPD do subcontratante

O artigo 37.º aplica-se tanto aos responsáveis pelo tratamento[17] como aos subcontratantes[18] no que respeita à designação de um EPD. Quem preencher os critérios de designação obrigatória, em certos casos apenas o responsável pelo tratamento ou apenas o subcontratante ou, noutros casos, tanto o responsável pelo tratamento como o subcontratante, tem de nomear um EPD (que deve passar a cooperar com cada uma das entidades).

É importante sublinhar que, mesmo que o responsável pelo tratamento preencha os critérios de designação obrigatória, o seu subcontratante não tem necessariamente de nomear um EPD. Contudo, tal pode constituir uma boa prática.

Por exemplo:

- Uma pequena empresa familiar que exerça atividades na distribuição de eletrodomésticos numa única localidade utiliza os serviços de um subcontratante cuja atividade principal consiste em prestar serviços analíticos e de assistência no sítio Web, com publicidade e *marketing* direcionados. As atividades da empresa familiar e os seus clientes não engendram

[17] O responsável pelo tratamento é definido no artigo 4.º, ponto 7, como a pessoa ou o organismo que determina as finalidades e os meios de tratamento.

[18] O subcontratante é definido pelo artigo 4.º, ponto 8, como a pessoa ou o organismo que trata os dados por conta do responsável pelo tratamento.

um tratamento de dados «em grande escala», atendendo ao número reduzido de clientes e ao âmbito relativamente limitado das atividades. No entanto, globalmente, as atividades do subcontratante, com muitos clientes, a exemplo desta pequena empresa, acarretam um tratamento de grande escala. O subcontratante deve, portanto, designar um EPD ao abrigo do artigo 37.º, n.º 1, alínea b). Por sua vez, a empresa familiar não é obrigada a designar individualmente um EPD.

- Uma empresa de média dimensão que fabrica ladrilhos subcontrata os seus serviços de medicina do trabalho a um subcontratante externo, o qual tem um grande número de clientes semelhantes. O subcontratante deve designar um EPD ao abrigo do artigo 37.º, n.º 1, alínea c), desde que o tratamento seja efetuado em grande escala. Contudo, o fabricante não está necessariamente sujeito à obrigação de designar um EPD.

O EPD designado por um subcontratante também supervisiona as atividades realizadas pela organização subcontratante quando atua na qualidade de responsável pelo tratamento dos dados por direito próprio (recursos humanos, informática, logística).

2.3. Designação de um único EPD para várias organizações

Em virtude do artigo 37.º, n.º 2, um grupo empresarial pode designar um único EPD, desde que este esteja *«facilmente acessível a partir de cada estabelecimento»*. A noção de acessibilidade refere-se às funções do EPD enquanto ponto de contacto em relação aos titulares dos dados[19], à autoridade de controlo[20], mas também, internamente, no seio da organização, tendo em conta que, no exercício de uma das suas funções, o EPD *«[i]nforma e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento»*[21].

A fim de assegurar que o EPD, seja interno seja externo, esteja acessível, é importante garantir a disponibilidade dos seus contactos, em conformidade com os requisitos do RGPD[22].

O EPD, com a ajuda de uma equipa, se necessário, deve estar em condições de comunicar eficientemente com os titulares dos dados[23] e de cooperar[24] com as autoridades de controlo em causa. Significa isto também que as comunicações devem ser efetuadas na língua ou nas línguas utilizadas pelas autoridades de controlo e pelos titulares de dados em causa. A disponibilidade de um EPD (quer

[19] Artigo 38.º, n.º 4: *«Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento.»*

[20] Artigo 39.º, n.º 1, alínea e): *«Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.»*

[21] Artigo 39.º, n.º 1, alínea a).

[22] Ver também a secção 2.6 *infra*.

[23] Artigo 12.º, n.º 1: *«O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.»*

[24] Artigo 39.º, n.º 1, alínea d): *«Coopera com a autoridade de controlo.»*

fisicamente nas mesmas instalações que os trabalhadores, quer através de uma linha direta ou de outros meios de comunicação seguros) é essencial para garantir que os titulares dos dados possam contactá-lo.

Nos termos do artigo 37.º, n.º 3, pode ser designado um único EPD para várias autoridades ou organismos públicos, tendo em conta a respetiva estrutura organizacional e dimensão. Aplicam-se os mesmos critérios aos recursos e à comunicação. Uma vez que o EPD tem a seu cargo um conjunto de funções, o responsável pelo tratamento ou o subcontratante deve assegurar que um único EPD, com a ajuda de uma equipa, se necessário, possa cumprir as suas funções de forma eficiente, apesar de ter sido nomeado para várias autoridades e organismos públicos.

2.4. Acessibilidade e localização do EPD

De acordo com a Secção 4 do RGPD, o EPD deve estar efetivamente acessível.

No sentido de assegurar que o EPD esteja acessível, o GT 29 recomenda que o EPD esteja localizado na União Europeia, independentemente de o responsável pelo tratamento ou o subcontratante estar ou não estabelecido na União Europeia.

No entanto, não se pode excluir que, nalgumas situações em que o responsável pelo tratamento ou o subcontratante não tenha estabelecimento dentro da União Europeia[25], o EPD possa exercer as suas atividades de forma mais eficaz se estiver situado fora da UE.

2.5. Competências e conhecimentos especializados do EPD

O artigo 37.º, n.º 5, dispõe que o EPD *«é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º»*. O considerando 97 prevê que o nível necessário de conhecimentos especializados deverá ser determinado em função das operações de tratamento de dados realizadas e da proteção exigida para os dados pessoais objeto de tratamento.

- **Nível de especialização**

O nível necessário de competências não é definido de forma rigorosa, mas deve coadunar-se com a sensibilidade, a complexidade e a quantidade de dados tratados por uma organização. Por exemplo, se a atividade de tratamento de dados for particularmente complexa, ou se estiver em causa uma grande quantidade de dados sensíveis, o EPD poderá necessitar de um nível de competências e de apoio mais elevado. Outra variação depende do facto de a organização transferir sistematicamente os dados pessoais para fora da União Europeia ou de estas transferências serem ocasionais. Neste sentido, o EPD deve ser escolhido de forma criteriosa, tendo devidamente em conta as questões de proteção de dados suscitadas no âmbito da organização.

- **Qualidades profissionais**

[25] Ver o artigo 3.º do RGPD relativo ao âmbito de aplicação territorial.

Embora o artigo 37.º, n.º 5, não explicite quais as qualidades profissionais que devem ser consideradas aquando da nomeação do EPD, como atributos pertinentes, os EPD devem ter competências no domínio das legislações e práticas nacionais e europeia em matéria de proteção de dados e um conhecimento profundo do RGPD. É igualmente conveniente que as autoridades de controlo promovam formações adequadas e regulares destinadas aos EPD.

Um conhecimento do setor empresarial e da organização do responsável pelo tratamento afigura-se útil. O EPD deve também apresentar um bom conhecimento das operações de tratamento efetuadas, bem como dos sistemas de informação, da segurança dos dados e das necessidades de proteção de dados do responsável pelo tratamento.

No caso das autoridades ou organismos públicos, o EPD deve igualmente ter um conhecimento sólido das regras e dos procedimentos administrativos da organização.

- **Capacidade para desempenhar as suas funções**

A capacidade para desempenhar as funções atribuídas ao EPD deve ser interpretada como um atributo respeitante não só às suas qualidades e conhecimentos pessoais, mas também à sua posição no seio da organização. As qualidades pessoais devem incluir, por exemplo, a integridade e um elevado nível de ética profissional; a principal preocupação do EPD deve consistir em permitir o cumprimento do RGPD. O EPD desempenha um papel determinante na promoção de uma cultura de proteção de dados no seio da organização e contribui para dar cumprimento aos elementos essenciais do RGPD, tais como os princípios do tratamento de dados[26], os direitos dos titulares de dados[27], a proteção de dados desde a conceção e por defeito[28], os registos das atividades de tratamento[29], a segurança do tratamento[30] e a notificação e comunicação de violações de dados[31].

- **EPD com base num contrato de prestação de serviços**

As funções do EPD podem igualmente ser exercidas com base num contrato de prestação de serviços celebrado com uma pessoa ou uma organização fora do âmbito da organização do responsável pelo tratamento/subcontratante. Neste último caso, é essencial que cada membro da organização que exerça as funções de EPD cumpra todos os requisitos aplicáveis da Secção 4 do RGPD (p. ex., é essencial que nenhum interveniente tenha um conflito de interesses). É igualmente importante que cada um destes membros esteja protegido pelas disposições do RGPD (p. ex., garantindo a impossibilidade de rescisão abusiva do contrato de prestação de serviços para atividades enquanto EPD, ou de destituição abusiva de qualquer membro da organização que executa as tarefas de EPD). Simultaneamente, as competências e os pontos fortes individuais podem ser combinados de modo que várias pessoas, trabalhando em equipa, possam servir os seus clientes de forma mais eficiente.

Por motivos de clareza jurídica e de boa organização, e no sentido de prevenir conflitos de interesses dos membros das equipas, recomenda-se uma clara repartição das tarefas no seio da equipa do EPD e a designação de uma única pessoa como contacto principal e pessoa «responsável» para cada cliente.

[26] Capítulo II.
[27] Capítulo III.
[28] Artigo 25.º.
[29] Artigo 30.º.
[30] Artigo 32.º.
[31] Artigos 33.º e 34.º.

De modo geral, seria igualmente pertinente especificar estes pontos no contrato de prestação de serviços.

2.6. Publicação e comunicação dos contactos do EPD

Nos termos do artigo 37.º, n.º 7, do RGPD, o responsável pelo tratamento ou o subcontratante tem de:

- publicar os contactos do EPD, e
- comunicar os contactos do EPD às autoridades de controlo competentes.

O objetivo destes requisitos é assegurar que os titulares de dados (tanto dentro como fora da organização) e as autoridades de controlo possam contactar fácil e diretamente o EPD, sem terem de contactar outra parte da organização. A confidencialidade é igualmente importante: por exemplo, os trabalhadores podem mostrar-se relutantes em apresentar queixas ao EPD caso a confidencialidade das suas comunicações não seja garantida.
O EPD está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros (art. 38.º, n.º 5).

Os contactos do EPD devem incluir informações que permitam aos titulares dos dados e às autoridades de controlo contactar facilmente o EPD (endereço postal, número de telefone e/ou endereço de correio eletrónico). Se necessário, para efeitos de comunicação com o público, podem igualmente ser disponibilizados outros meios de comunicação, por exemplo uma linha direta específica, ou um formulário específico de contacto do EPD, disponível no sítio Web da organização.

O artigo 37.º, n.º 7, não exige que os contactos publicados incluam o nome do EPD. Ainda que a publicação desta informação possa constituir uma boa prática, cabe ao responsável pelo tratamento ou subcontratante e ao EPD decidirem se tal é necessário ou útil nas circunstâncias concretas[32].

No entanto, a comunicação do nome do EPD à autoridade de controlo é essencial para que o EPD possa funcionar como ponto de contacto entre a organização e a autoridade de controlo [art. 39.º, n.º 1, alínea e)].

A título de boa prática, o GT 29 recomenda igualmente que a organização informe os seus trabalhadores do nome e contactos do EPD. Por exemplo, o nome e contactos do EPD podem ser publicados internamente na intranet da organização, nas listas telefónicas internas e em organogramas.

3 Posição do EPD

3.1. Envolvimento do EPD em todas as questões relativas à proteção dos dados pessoais

[32] Cumpre referir que o artigo 33.º, n.º 3, alínea b), que descreve as informações a fornecer à autoridade de controlo e aos titulares dos dados em caso de violação de dados pessoais exige expressamente, ao contrário do artigo 37.º, n.º 7, que seja igualmente comunicado o nome (e não apenas os contactos) do EPD.

Nos termos do artigo 38.º do RGPD, o responsável pelo tratamento e o subcontratante devem assegurar que o EPD seja *«envolvido, de forma adequada e em tempo útil, [em] todas as questões relacionadas com a proteção de dados pessoais»*.

É crucial que o EPD, ou a sua equipa, seja envolvido, desde a fase mais precoce, em todas as questões relacionadas com a proteção de dados. Em relação às avaliações de impacto sobre a proteção de dados, o RGPD prevê explicitamente o envolvimento do EPD desde o início e especifica que, ao efetuar essas avaliações de impacto, o responsável pelo tratamento deve solicitar o parecer do EPD[33]. Assegurar que o EPD seja informado e consultado durante a fase inicial permitirá facilitar o cumprimento do RGPD e promover uma abordagem de proteção da privacidade desde a conceção, pelo que deve constituir o procedimento normal da governação da organização. Além disso, é importante que o EPD seja encarado como interlocutor no seio da organização e que faça parte dos grupos de trabalho incumbidos de gerir as atividades de tratamento de dados nessa organização.

Por conseguinte, a organização deve assegurar, por exemplo, que:

- O EPD é convidado a participar regularmente nas reuniões dos quadros de gestão médios e superiores;
- A sua presença é recomendada sempre que sejam adotadas decisões com implicações na proteção de dados. Todas as informações pertinentes são transmitidas oportunamente ao EPD, para que este possa prestar um aconselhamento adequado;
- O parecer do EPD é sempre devidamente ponderado. Em caso de desacordo, o GT 29 recomenda, como boa prática, que sejam enunciados os motivos para não seguir o parecer do EPD;
- O EPD é imediatamente consultado após a ocorrência de uma violação de dados ou outro incidente.

Se for caso disso, o responsável pelo tratamento ou o subcontratante pode elaborar orientações ou programas em matéria de proteção de dados que definam em que momento o EPD deve ser consultado.

3.2. Recursos necessários

O artigo 38.º, n.º 2, do RGPD exige que a organização apoie o seu EPD, *«fornecendo-lhe os recursos necessários ao desempenho [das suas] funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento»*. Em especial, devem ser considerados os seguintes aspetos:

- Um apoio ativo às funções do EPD por parte dos quadros de gestão superiores (nomeadamente, ao nível do conselho de administração);
- Tempo suficiente para que os EPD exerçam as suas atribuições. Trata-se de um aspeto particularmente importante quando o EPD interno é nomeado a tempo parcial ou quando o EPD externo garante a proteção de dados em complemento de outras atribuições. O incumprimento deste requisito poderia gerar conflitos de prioridades que se sobreporiam ao

[33] Artigo 35.º, n.º 2.

exercício das atribuições do EPD. É crucial dedicar tempo suficiente às funções do EPD. Neste sentido, é aconselhável, como boa prática, definir uma percentagem de tempo para as funções do EPD, se as mesmas não forem desempenhadas a tempo inteiro. De igual modo, é aconselhável determinar o tempo necessário para o desempenho das funções e o nível adequado de prioridade das atribuições do EPD e que o EPD (ou a organização) elabore um plano de trabalho;

- Um apoio adequado em termos de recursos financeiros, infraestruturas (locais, instalações, equipamento) e pessoal, sempre que necessário;
- A comunicação oficial da nomeação do EPD a todo o pessoal, a fim de divulgar a sua existência e missão dentro da organização;
- O necessário acesso a outros serviços, como os recursos humanos e os serviços jurídicos, informáticos, de segurança, etc., para que os EPD possam receber apoio, contributos e informações essenciais por parte destes outros serviços;
- A formação contínua. Os EPD devem ter a possibilidade de se manter atualizados no que diz respeito aos desenvolvimentos no domínio da proteção de dados. O objetivo deve ser uma melhoria permanente do nível de competência dos EPD, que devem ser incentivados a participar em cursos de formação sobre proteção de dados e noutras iniciativas de desenvolvimento profissional, tais como conferências sobre privacidade, seminários, etc.;
- Consoante a dimensão e a estrutura da organização, pode ser necessário criar uma equipa do EPD (o EPD e o seu pessoal). Nestes casos, a estrutura interna da equipa e as funções e responsabilidades de cada um dos seus membros devem estar claramente definidas. De igual modo, se a função do EPD for exercida por um prestador de serviços externo, um conjunto de pessoas que trabalham para essa entidade poderá exercer de modo eficaz as funções de EPD enquanto equipa, sob a responsabilidade de um contacto principal designado para o cliente.

De modo geral, quanto mais complexas e/ou sensíveis forem as operações de tratamento, mais recursos devem ser concedidos ao EPD. A missão de proteção de dados deve ser eficaz e dotada de recursos suficientes para o tratamento de dados efetuado.

3.3. Instruções e desempenho das *«funções e atribuições com independência»*

O artigo 38.º, n.º 3, estabelece determinadas garantias básicas no sentido de ajudar a assegurar que os EPD tenham condições para executar as suas tarefas com suficiente grau de autonomia no seio da sua organização. Concretamente, os responsáveis pelo tratamento/subcontratantes devem assegurar que o EPD *«não recebe instruções relativamente ao exercício das suas funções»*. O considerando 97 refere, além disso, que os EPD, *«sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência»*.

Significa isto que os EPD, no exercício das suas funções ao abrigo do artigo 39.º, não devem receber instruções quanto à forma de tratar uma questão, por exemplo quanto ao resultado que deve ser obtido, à forma de investigar uma queixa ou à necessidade de consultar a autoridade de controlo. Além disso, não devem receber instruções no sentido de adotarem determinada perspetiva sobre uma questão relacionada com as normas de proteção de dados, por exemplo determinada interpretação da legislação.

A autonomia dos EPD não implica, contudo, que lhes sejam conferidos poderes decisórios que extravasem as suas funções em conformidade com o artigo 39.º.

O responsável pelo tratamento ou o subcontratante permanece responsável pelo cumprimento das normas de proteção de dados e deve poder comprovar esse cumprimento[34]. Se o responsável pelo tratamento ou o subcontratante tomar decisões incompatíveis com o RGPD e o parecer do EPD, deve ser dada a possibilidade ao EPD de transmitir de forma clara o seu parecer divergente ao mais alto nível da direção e a quem tomou as decisões. A este respeito, nos termos do artigo 38.º, n.º 3, o EPD *«informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante»*. Esta comunicação direta assegura que os quadros de gestão superiores (p. ex., o conselho de administração) têm conhecimento do parecer e das recomendações do EPD, no âmbito da missão do EPD de informar e aconselhar o responsável pelo tratamento ou o subcontratante. Outro exemplo de comunicação direta consiste na elaboração de um relatório anual de atividades do EPD, a apresentar ao mais alto nível da direção.

3.4. Destituição ou penalização pelo exercício das funções de EPD

Em conformidade com o artigo 38.º, n.º 3, o EPD *«não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções»*.

Este requisito reforça a autonomia dos EPD e ajuda a garantir que estes atuam de forma independente e beneficiam de proteção suficiente no desempenho das suas funções de proteção de dados.

As penalizações são proibidas ao abrigo do RGPD apenas se forem impostas em resultado do efetivo exercício das funções de EPD. Por exemplo, o EPD pode considerar que determinado tratamento é suscetível de gerar elevado risco e aconselhar o responsável pelo tratamento ou o subcontratante a realizar uma avaliação de impacto sobre a proteção de dados, mas dar-se o caso de o responsável pelo tratamento ou o subcontratante discordar da apreciação do EPD. Nesta situação, o EPD não pode ser destituído por ter emitido o seu parecer.

As penalizações poderiam assumir diversas formas e poderiam ser diretas ou indiretas. Poderiam ser aplicadas, por exemplo, através da inexistência ou demora na atribuição de promoções, do impedimento da progressão na carreira ou da recusa dos benefícios concedidos a outros trabalhadores. Não é necessário que estas penalizações sejam efetivamente aplicadas; uma simples ameaça é suficiente na medida em que seja utilizada para penalizar o EPD por motivos relacionados com as suas atividades de EPD.

Como regra normal de gestão, e à semelhança de qualquer outro funcionário ou contratante, nos termos e sob reserva da legislação nacional aplicável em matéria contratual ou laboral e penal, um EPD pode, no entanto, ser legitimamente destituído por outras razões que não o exercício das suas funções como EPD (p. ex., em caso de roubo, assédio físico, psicológico ou sexual ou outra falta grave).

Neste contexto, convém notar que o RGPD não especifica como e quando o EPD pode ser afastado ou substituído por outra pessoa. Todavia, quanto mais estável for o contrato do EPD e quanto mais garantias existirem contra a destituição abusiva, maior será a probabilidade de o EPD poder atuar de

[34] Artigo 5.º, n.º 2.

forma independente. Por conseguinte, o GT 29 mostra-se favorável a que as organizações envidem esforços neste sentido.

3.5. Conflitos de interesses

O artigo 38.º, n.º 6, permite aos EPD *«exercer outras funções e atribuições»*. Porém, exige que a organização assegure que *«essas funções e atribuições não resultam num conflito de interesses»*.

A ausência de conflitos de interesses está intimamente ligada ao requisito de independência dos EPD. Embora os EPD estejam autorizados a desempenhar outras tarefas, só podem ser incumbidos de outras funções e atribuições se estas não derem origem a conflitos de interesses. Por conseguinte, o EPD não pode, em especial, exercer um cargo dentro da organização que o leve a determinar as finalidades e os meios do tratamento de dados pessoais. Devido à estrutura organizacional específica de cada organização, este aspeto deve ser apreciado caso a caso.

Regra geral, os cargos suscetíveis de gerar conflitos no seio da organização podem incluir não só os cargos de gestão superiores (por exemplo, diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de *marketing*, diretor dos recursos humanos ou diretor informático), mas também outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento. Além disso, pode igualmente surgir um conflito de interesses se, por exemplo, um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados.

Consoante as atividades, a dimensão e a estrutura da organização, é aconselhável, como boa prática, que os responsáveis pelo tratamento ou os subcontratantes:

- identifiquem os cargos que se afigurariam incompatíveis com as funções de EPD;
- aprovem normas internas para o efeito, com o intuito de evitar conflitos de interesses;
- incluam uma explicação mais geral sobre os conflitos de interesses;
- declarem que os respetivos EPD não têm conflitos de interesses no que se refere às suas funções enquanto EPD, como forma de divulgação deste requisito;
- incluam salvaguardas no regulamento interno da organização e assegurem que o anúncio de vaga para o lugar de EPD ou o contrato de prestação de serviços seja suficientemente preciso e pormenorizado, com vista a evitar conflitos de interesses. Neste contexto, importa igualmente ter em conta que os conflitos de interesses podem assumir formas diferentes em função do vínculo laboral do EPD enquanto colaborador interno ou externo.

4 Funções do EPD

4.1. Controlo da conformidade com o RGPD

O artigo 39.º, n.º 1, alínea b), incumbe o EPD, entre outras funções, de controlar a conformidade com o RGPD. O considerando 97 especifica, por outro lado, que o EPD deve assistir *«o responsável pelo tratamento [...] ou o subcontratante [...] no controlo do cumprimento do presente regulamento a nível interno»*.

No âmbito destas atribuições de controlo da conformidade, os EPD podem, nomeadamente:

- recolher informações para identificar as atividades de tratamento;
- analisar e verificar a conformidade das atividades de tratamento;
- prestar informações e aconselhamento e formular recomendações ao responsável pelo tratamento ou ao subcontratante.

O controlo da conformidade não significa que a responsabilidade pessoal do EPD seja imputada em caso de incumprimento. O RGPD esclarece que compete ao responsável pelo tratamento, e não ao EPD, aplicar *«as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento»* (art. 24.º, n.º 1). O cumprimento das regras de proteção de dados é uma competência empresarial do responsável pelo tratamento de dados, e não do EPD.

4.2. Papel do EPD no âmbito da avaliação de impacto sobre a proteção de dados

Nos termos do artigo 35.º, n.º 1, cabe ao responsável pelo tratamento, e não ao EPD, proceder, quando necessário, a uma avaliação de impacto sobre a proteção de dados (AIPD). Todavia, o EPD pode desempenhar um papel muito importante e útil, prestando assistência ao responsável pelo tratamento. Aplicando o princípio da proteção de dados desde a conceção, o artigo 35.º, n.º 2, dispõe expressamente que, ao efetuar uma AIPD, o responsável pelo tratamento deve *«solicita[r] o parecer»* do EPD. Por sua vez, o artigo 39.º, n.º 1, alínea c), determina que o EPD deve *«[p]resta[r] aconselhamento, quando tal lhe for solicitado, no que respeita à [AIPD], e controla[r] a sua realização nos termos do artigo 35.º»*.

O GT 29 recomenda que o responsável pelo tratamento solicite o parecer do EPD sobre as seguintes questões, entre outras[35]:

- se deve ou não efetuar uma AIPD;
- qual a metodologia a seguir na realização de uma AIPD;
- se deve realizar a AIPD internamente ou externalizá-la;
- quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;
- se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com o RGPD.

[35] O artigo 39.º, n.º 1, menciona as funções do EPD e indica que o EPD tem, *«pelo menos»*, as seguintes funções. Por conseguinte, nada impede que o responsável pelo tratamento atribua ao EPD outras funções além das explicitamente referidas no artigo 39.º, n.º 1, ou especifique as tarefas de forma mais pormenorizada.

Se o responsável pelo tratamento discordar do parecer emitido pelo EPD, a documentação da AIPD deve justificar especificamente, por escrito, os motivos pelos quais o parecer não foi tido em conta[36].

O GT 29 recomenda, além disso, que o responsável pelo tratamento indique claramente, por exemplo, no contrato com o EPD, bem como nas informações prestadas aos trabalhadores e aos quadros de gestão (e a outras partes interessadas, se for caso disso), as tarefas específicas do EPD e o respetivo âmbito de aplicação, nomeadamente no que diz respeito à realização da AIPD.

4.3. Cooperação com a autoridade de controlo e função de ponto de contacto

Nos termos do artigo 39.º, n.º 1, alíneas d) e e), o EPD *«[c]oopera com a autoridade de controlo»* e serve de *«[p]onto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto»*.

Estas funções enquadram-se no papel de «facilitador» do EPD, referido na introdução das presentes orientações. O EPD serve de ponto de contacto no sentido de facilitar o acesso da autoridade de controlo aos documentos e informações necessários para o desempenho das funções elencadas no artigo 57.º, bem como para o exercício dos seus poderes de investigação, de correção, consultivos e de autorização, tal como referidos no artigo 58.º. Conforme mencionado acima, o EPD está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros (art. 38.º, n.º 5). Todavia, a obrigação de sigilo/confidencialidade não proíbe o EPD de contactar e solicitar o parecer da autoridade de controlo. O artigo 39.º, n.º 1, alínea e), prevê que o encarregado da proteção de dados pode, sendo caso disso, consultar a autoridade de controlo sobre qualquer outro assunto.

4.4. Abordagem baseada no risco

O artigo 39.º, n.º 2, exige que o EPD tenha *«em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento»*.

Este artigo alude a um princípio geral e assente no bom senso, que pode revelar-se pertinente em muitos aspetos do trabalho diário do EPD. Essencialmente, exige que os EPD estabeleçam prioridades nas suas atividades e centrem os seus esforços nas questões que apresentam maiores riscos em matéria de proteção de dados. Tal não implica que os EPD devam negligenciar o controlo da conformidade das operações de tratamento de dados que, em termos comparativos, acarretam um nível de risco mais reduzido, indiciando antes que devem centrar-se fundamentalmente nos domínios de maior risco.

Esta abordagem seletiva e pragmática deve apoiar os EPD na sua missão de prestar aconselhamento ao responsável pelo tratamento sobre: a metodologia a seguir na realização de uma AIPD; os domínios que devem ser objeto de auditorias internas ou externas sobre a proteção de dados; as ações de

[36] O artigo 24.º, n.º 1, dispõe o seguinte: *«Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar* ***e poder comprovar*** *que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades»*.

formação internas a disponibilizar ao pessoal ou aos quadros de gestão responsáveis pelas atividades de tratamento de dados; e as operações de tratamento às quais o responsável pelo tratamento deve consagrar uma parte mais significativa do seu tempo e recursos.

4.5. Papel do EPD na conservação do registo de atividades

Nos termos do artigo 30.º, n.os 1 e 2, é o responsável pelo tratamento dos dados ou o subcontratante, e não o EPD, que *«conserva um registo de todas as atividades de tratamento sob a sua responsabilidade»* ou *«conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento»*.

Na prática, os EPD criam, por norma, inventários e mantêm um registo das operações de tratamento com base nas informações que recebem dos vários departamentos na sua organização aos quais incumbe o tratamento de dados pessoais. Esta prática foi estabelecida ao abrigo de muitas disposições legislativas nacionais em vigor e em conformidade com as normas de proteção de dados aplicáveis às instituições e aos órgãos da UE[37].

O artigo 39.º, n.º 1, prevê uma lista das funções mínimas que devem incumbir ao EPD. Por conseguinte, nada impede que o responsável pelo tratamento ou o subcontratante atribua ao EPD a função de conservar o registo das atividades de tratamento sob a responsabilidade do responsável pelo tratamento ou do subcontratante. Esse registo deve ser considerado um dos instrumentos que permitem ao EPD desempenhar as suas funções de controlo da conformidade e de prestação de informação e aconselhamento ao responsável pelo tratamento ou ao subcontratante.

Em qualquer caso, o registo de conservação obrigatória por força do artigo 30.º deve igualmente ser encarado como instrumento que permite ao responsável pelo tratamento e à autoridade de controlo, a pedido destes, obter uma perspetiva geral de todas as atividades de tratamento de dados pessoais levadas a cabo por uma organização. Trata-se, portanto, de um requisito prévio da conformidade e, como tal, constitui uma medida de responsabilização eficaz.

[37] Artigo 24.º, n.º 1, alínea d), do Regulamento (CE) n.º 45/2001.

5 ANEXO — ORIENTAÇÕES SOBRE OS EPD: O QUE PRECISA DE SABER

O objetivo do presente anexo é proporcionar uma resposta, num formato simplificado e de fácil leitura, a algumas das principais dúvidas que as organizações poderão ter acerca dos novos requisitos aplicáveis à nomeação do EPD nos termos do Regulamento Geral sobre a Proteção de Dados (RGPD).

Designação do EPD

1 Quais são as organizações que devem nomear um EPD?

A designação de um EPD é obrigatória:

- se o tratamento for efetuado por autoridade ou organismo público (independentemente dos dados objeto de tratamento);
- se as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento que exijam controlo regular e sistemático dos titulares dos dados em grande escala;
- se as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações.

Saliente-se que o direito da União ou dos Estados-Membros poderá igualmente exigir a designação de EPD noutras situações. Por último, mesmo quando não é obrigatório designar um EPD, as organizações poderão, nalguns casos, considerar conveniente designar um EPD a título voluntário. O Grupo do Artigo 29.º para a Proteção de Dados (GT 29) é favorável a estas iniciativas voluntárias. Quando uma organização designa um EPD a título voluntário, são aplicáveis à sua nomeação, posição e atribuições os mesmos requisitos aplicáveis à designação obrigatória.

Fonte: artigo 37.º, n.º 1, do RGPD

2 Qual o significado de «atividades principais»?

As «atividades principais» podem entender-se como as operações essenciais para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, as quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante. Por exemplo, o tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes, deve ser considerado uma das atividades principais de qualquer hospital, pelo que os hospitais devem nomear EPD.

Por outro lado, todas as organizações exercem determinadas atividades de apoio, nomeadamente a remuneração dos seus trabalhadores ou atividades comuns de apoio informático. Trata-se de exemplos de funções de apoio necessárias para a atividade principal ou a área de negócio central da organização. Embora sejam necessárias ou essenciais, por norma estas atividades são consideradas funções acessórias e não a atividade principal.

Fonte: artigo 37.º, n.º 1, alíneas b) e c), do RGPD

3 Qual o significado de «grande escala»?

O RGPD não define o que constitui um tratamento de grande escala. O GT 29 recomenda que, em especial, os seguintes fatores sejam tomados em consideração para determinar se o tratamento é efetuado em grande escala:

- o número de titulares de dados afetados – como número concreto ou em percentagem da população em causa;
- o volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento;
- a duração, ou permanência, da atividade de tratamento de dados;
- o âmbito geográfico da atividade de tratamento.

Contam-se como exemplos de tratamento de grande escala:

- o tratamento de dados de doentes no exercício normal das atividades de um hospital
- o tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem)
- o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado nestas atividades;
- o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco
- o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca
- o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet

Como exemplos que não constituem tratamento de grande escala, incluem-se:

- o tratamento de dados de doentes pacientes por um médico
- o tratamento de dados pessoais relacionados com condenações penais e infrações por um advogado

Fonte: artigo 37.º, n.º 1, alíneas b) e c), do RGPD

4 Qual o significado de «controlo regular e sistemático»?

A noção de controlo regular e sistemático dos titulares dos dados não está definida no RGPD, mas inclui claramente todas as formas de seguimento e de definição de perfis na internet, designadamente para fins de publicidade comportamental. No entanto, a noção de controlo não se cinge ao ambiente em linha.

Exemplos de atividades que podem constituir um controlo regular e sistemático dos titulares de dados: exploração de uma rede de telecomunicações; prestação de serviços de telecomunicações; reorientação de mensagens de correio eletrónico; atividades de promoção comercial baseadas em dados; definição de perfis e pontuação para fins de avaliação dos riscos (p. ex., para efeitos de pontuação de crédito, fixação de prémios de seguro, prevenção de fraudes, deteção de casos de branqueamento de capitais); localização, por exemplo, através de aplicações móveis; programas de fidelização; publicidade comportamental; controlo de dados relativos ao bem-estar, à condição física e à saúde através de usáveis; televisão em circuito fechado; dispositivos conectados, por exemplo, contadores inteligentes, automóveis inteligentes, domótica, etc.

Na interpretação do GT 29, «regular» significa, neste caso, uma ou mais das seguintes características:

- contínuo ou que ocorre a intervalos específicos num determinado período,
- recorrente ou repetido em horários estipulados,
- constante ou periódico.

Na interpretação do GT 29, «sistemático» significa, neste caso, uma ou mais das seguintes características:

- que ocorre de acordo com um sistema,
- predefinido, organizado ou metódico,
- realizado no âmbito de um plano geral de recolha de dados,
- efetuado no âmbito de uma estratégia.

Fonte: artigo 37.º, n.º 1, alínea b), do RGPD

5 As organizações podem nomear conjuntamente um EPD? Em caso afirmativo, em que condições?

Sim. Um grupo empresarial pode designar um único EPD, desde que este esteja *«facilmente acessível a partir de cada estabelecimento»*. A noção de acessibilidade refere-se às funções do EPD enquanto ponto de contacto em relação aos titulares dos dados, à autoridade de controlo e também, internamente, no seio da organização. A fim de assegurar que o EPD, seja interno seja externo, esteja acessível, é importante garantir a disponibilidade dos seus contactos. O EPD, com a ajuda de uma equipa, se necessário, deve estar em condições de comunicar eficientemente com os titulares dos dados e de cooperar com as autoridades de controlo em causa. Significa isto que as comunicações devem ser efetuadas na língua ou nas línguas utilizadas pelas autoridades de controlo e pelos titulares de dados em causa. A disponibilidade de um EPD (quer fisicamente nas mesmas instalações que os trabalhadores, quer através de uma linha direta ou de outros meios de comunicação seguros) é essencial para garantir que os titulares dos dados possam contactá-lo.

Pode ser designado um único EPD para várias autoridades ou organismos públicos, tendo em conta a respetiva estrutura organizacional e dimensão. Aplicam-se os mesmos critérios aos recursos e à comunicação. Uma vez que o EPD tem a seu cargo um conjunto de funções, o responsável pelo tratamento ou o subcontratante deve assegurar que um único EPD, com a ajuda de uma equipa, se necessário, possa cumprir as suas funções de forma eficiente, apesar de ter sido nomeado para várias autoridades e organismos públicos.

Fonte: artigo 37.º, n.os 2 e 3, do RGPD

6 Onde deve estar localizado o EPD?

No sentido de assegurar que o EPD esteja acessível, o GT 29 recomenda que o EPD esteja localizado na União Europeia, independentemente de o responsável pelo tratamento ou o subcontratante estar ou não estabelecido na União Europeia. No entanto, não se pode excluir que, nalgumas situações em que o responsável pelo tratamento ou o subcontratante não tenha estabelecimento dentro da União Europeia, o EPD possa exercer as suas atividades de forma mais eficaz se estiver situado fora da UE.

7 É possível nomear um EPD externo?

Sim. O EPD pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante (EPD interno), ou exercer as suas funções com base num contrato de prestação de serviços. Por outras palavras, o EPD pode ser externo e, neste caso, exercer a sua função com base num contrato de prestação de serviços celebrado com uma pessoa ou uma organização.

Se a função do EPD for exercida por um prestador de serviços externo, um conjunto de pessoas que trabalham para essa entidade poderá exercer de modo eficaz as funções do EPD enquanto equipa, sob a responsabilidade de um contacto principal e «pessoa responsável» designado para o cliente. Neste caso, é essencial que cada membro da organização externa que exerça as funções de EPD cumpra todos os requisitos aplicáveis do RGPD.

Por motivos de clareza jurídica e de boa organização, e no sentido de prevenir conflitos de interesses dos membros das equipas, as presentes orientações recomendam que o contrato de prestação de serviços preveja uma clara repartição das tarefas no seio da equipa do EPD externo e a designação de uma única pessoa como contacto principal e pessoa «responsável» do cliente.

Fonte: artigo 37.º, n.º 6, do RGPD

8 Quais são as qualidades profissionais que o EPD deve ter?

O EPD deve ser designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio das normas e práticas de proteção de dados, bem como na sua capacidade para desempenhar as respetivas funções.

O nível necessário de conhecimentos especializados deverá ser determinado em função das operações de tratamento de dados realizadas e da proteção exigida para os dados pessoais objeto de tratamento. Por exemplo, se a atividade de tratamento de dados for particularmente complexa, ou se estiver em causa uma grande quantidade de dados sensíveis, o EPD poderá necessitar de um nível de competências e de apoio mais elevado.

As competências e conhecimentos especializados pertinentes incluem:

- competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD,
- conhecimento das operações de tratamento efetuadas,
- conhecimento das tecnologias da informação e da segurança dos dados,
- conhecimento do setor empresarial e da organização,
- capacidade para promover uma cultura de proteção de dados no seio da organização.

Fonte: artigo 37.º, n.º 5, do RGPD

9 Que recursos o responsável pelo tratamento ou o subcontratante deve conceder ao EPD?

O EPD deve dispor dos recursos necessários ao desempenho das suas funções.

Em função da natureza das operações de tratamento e das atividades e dimensão da organização, devem ser concedidos os seguintes recursos ao EPD:

- apoio ativo às funções do EPD por parte dos quadros de gestão superiores;
- tempo suficiente para que os EPD desempenhem as suas tarefas;
- apoio adequado em termos de recursos financeiros, infraestruturas (locais, instalações, equipamento) e pessoal, sempre que necessário;
- comunicação oficial da nomeação do EPD a todo o pessoal;
- acesso a outros serviços no seio da organização, para que os EPD possam receber apoio, contributos ou informações essenciais por parte destes outros serviços;
- formação contínua.

Fonte: artigo 38.º, n.º 2, do RGPD

10 Que salvaguardas são introduzidas para permitir que o EPD desempenhe as suas funções com independência? Qual o significado de «conflito de interesses»?

Existem várias salvaguardas para permitir ao EPD atuar de forma independente:

- os responsáveis pelo tratamento ou subcontratantes não transmitem instruções relativas ao exercício das funções do EPD
- o responsável pelo tratamento não pode destituir nem penalizar o EPD pelo exercício das suas funções
- não é possível o conflito de interesses com outras possíveis funções e atribuições

As outras funções e atribuições do EPD não podem resultar num conflito de interesses. Significa isto, antes de mais, que o EPD não pode exercer um cargo dentro da organização que o leve a determinar as finalidades e os meios do tratamento de dados pessoais. Devido à estrutura organizacional específica de cada organização, este aspeto deve ser apreciado caso a caso.

Regra geral, os cargos suscetíveis de gerar conflitos no seio da organização podem incluir não só os cargos de gestão superiores (por exemplo, diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático), mas também outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento. Além disso, pode igualmente surgir um conflito de interesses se, por exemplo, o EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante junto dos tribunais no âmbito de processos respeitantes a questões de proteção de dados.

Fonte: artigo 38.º, n.os 3 e 6, do RGPD

Funções do EPD

11 Qual o significado de «controlo da conformidade»?

No âmbito destas atribuições de controlo da conformidade, os EPD podem, nomeadamente:

- recolher informações para identificar as atividades de tratamento;
- analisar e verificar a conformidade das atividades de tratamento;
- prestar informações e aconselhamento e formular recomendações ao responsável pelo tratamento ou ao subcontratante.

Fonte: artigo 39.º, n.º 1, alínea b), do RGPD

12 O EPD é pessoalmente responsável pelo incumprimento dos requisitos de proteção de dados?

Não. Os EPD não são pessoalmente responsáveis pelo incumprimento dos requisitos de proteção de dados. Compete ao responsável pelo tratamento ou ao subcontratante assegurar e poder comprovar que o tratamento respeita o Regulamento aplicável. O cumprimento das normas de proteção de dados é da competência do responsável pelo tratamento ou do subcontratante.

13 Qual é o papel do EPD no que respeita às avaliações de impacto sobre a proteção de dados e aos registos das atividades de tratamento?

No que concerne à avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento ou o subcontratante deve solicitar o parecer do EPD sobre, nomeadamente, as seguintes questões:

- se deve ou não efetuar a AIPD;
- qual a metodologia a seguir na realização da AIPD;
- se deve realizar a AIPD internamente ou externalizá-la;
- quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;
- se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com os requisitos de proteção de dados

É ao responsável pelo tratamento dos dados ou ao subcontratante, e não ao EPD, que compete conservar registos das atividades de tratamento. Contudo, nada impede que o responsável pelo tratamento ou o subcontratante atribua ao EPD a função de conservar os registos das atividades de tratamento sob a responsabilidade do responsável pelo tratamento ou do subcontratante. Esses registos devem ser considerados um dos instrumentos que permitem ao EPD desempenhar as suas funções de

controlo da conformidade e de prestação de informações e aconselhamento ao responsável pelo tratamento ou ao subcontratante.

Fonte: artigo 39.º, n.º 1, alínea c), e artigo 30.º do RGPD

Feito em Bruxelas, em 13 de dezembro de 2016

Pelo Grupo de Trabalho,
A Presidente

Isabelle FALQUE-PIERROTIN

Com a última redação revista e adotada em 5 de abril de 2017

Pelo Grupo de Trabalho
A Presidente

Isabelle FALQUE-PIERROTIN