CONTRIBUTOS PARA A ANÁLISE DO ARTICULADO DA PROPOSTA DE LEI DE EXECUÇÃO DO RGPD | ANDPO

Proposta de Lei n.º120/XIII

A "**Associação Nacional de DPOs e Outros Profissionais de Privacidade (ANDPO)**", vem apresentar os seus contributos relativamente à Proposta de Lei N.º 120/XIII, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Assim, este documento expressa a posição da Associação tendo em conta a conjuntura existente à data em que o documento foi entregue.

Quaisquer questões relacionadas com a presente proposta deverão ser dirigidas A/C do Presidente da ANDPO, geral@andpo.pt.

Preâmbulo

A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental de todo e qualquer cidadão europeu.

Tal está estabelecido no artigo 8.º, n.º 1, da **Carta dos Direitos Fundamentais da União Europeia** (*Carta*)[1] e consolidado no artigo 16.º, n.º 1, do **Tratado sobre o Funcionamento da União Europeia** *(TFUE)*[2], ambos juridicamente vinculativos para a UE após a entrada em vigor do Tratado de Lisboa[3] em 13 Dezembro de 2009, tendo sido assinado pelos Estados-membros da União Europeia no culminar da terceira Presidência portuguesa do Conselho da União Europeia, em Lisboa, em Dezembro de 2007.

O Regulamento Geral sobre a Protecção de Dados (**RGPD**)[4], publicado em **27 de Abril de 2016**, proporciona um quadro de cumprimento modernizado e assente na responsabilidade em matéria de protecção de dados na Europa.

Os Encarregados da Protecção de Dados, conhecidos na literatura europeia e internacional como *Data Protection Officers* (**DPO**) e cuja terminologia é adoptada neste documento, terão um papel central neste novo quadro normativo relativamente a um vasto número de entidades, em particular onde seja obrigatória a sua designação, facilitando o cumprimento das disposições do **RGPD**.

Será pois fundamental o papel do **DPO** no acompanhamento, aconselhamento, controlo e monitorização da conformidade com o **RGPD** para, em última análise, garantir o correcto respeito pelos direitos e liberdades fundamentais das pessoas alvo desses tratamentos de dados. Além de facilitar o cumprimento das disposições do **RGPD**, o **DPO** atua como ponto de contacto para assuntos no âmbito do tratamento de dados pessoais entre a "sua" entidade e as partes interessadas relevantes, designadamente, a(s) autoridade(s) de controlo, o(s) titular(es) de dados ou seus representantes, ou no âmbito da relação inter-departamental dentro da própria organização.

Tal como disposto no **RGPD**, é irrelevante a natureza e o papel das entidades intervenientes num tratamento de dados. Todos estão abrangidos e têm de ser cumpridas as obrigações do **RGPD**, quer sejam "Responsáveis pelo tratamento", quer sejam "Responsáveis conjuntos pelo tratamento" , quer sejam "Subcontratantes". Em concreto, toda e qualquer entidade onde decorram operações de tratamento de dados pessoais, sejam entidades públicas ou privadas, autoridades ou organismos com ou sem fins lucrativos, sejam pequenas, médias ou grandes empresas, têm de cumprir com as obrigações do **RGPD**, nomeadamente no que se refere à responsabilidade própria perante os titulares dos dados.

Tendo em conta as obrigações e responsabilidades inerentes à função de **DPO**, o presente contributo constitui uma declaração expressa sobre os valores, princípios e normas que devem orientar a conduta daqueles designados para exercer esta importante função. É, pois, relevante clarificar as questões relativas à integridade, exigência, competência, transparência e legalidade daqueles que venham a exercer a função de Encarregados da Protecção de Dados.

---

[1] *https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al33501*
[2] *https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT*
[3] *https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html*
[4] *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*

Finalmente, pretende-se com este documento contribuir para a definição e incorporação de elementos na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis, tal como prevê o considerando 8[5] do **RGPD**.

Por último, importa referir que já em 30 de Setembro de 2017 tivemos oportunidade de submeter o nosso contributo na "Consulta Pública para aprovação de Legislação Nacional relativa ao Regulamento Geral de Protecção de Dados (RGPD)" lançada pelo "Grupo de Trabalho com o objectivo de preparar a legislação portuguesa para a aplicação do Regulamento Geral de Protecção de Dados (RGDP) em Portugal", que pretendia recolher opiniões acerca de várias matérias respeitantes à adaptação do RGPD à legislação portuguesa.

[5] *Considerando (8) Caso o presente regulamento preveja especificações ou restrições das suas regras pelo direito de um Estado-Membro, estes podem incorporar elementos do presente regulamento no respectivo direito nacional, na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis para as pessoas a quem se aplicam.*

Análise à Proposta de Lei n.º 120/XIII

[Exposição de Motivos]

Os motivos plasmados na exposição introdutória da proposta de lei apresentam algumas imprecisões quanto ao **RGPD** para as quais aqui se entende dever alertar.

Sem que se pretenda desenvolver em extensão a totalidade das questões, existem dois temas sobre os quais julgamos ser imperativa a nossa pronúncia de forma a contribuirmos para a correcta interpretação e redacção do documento final.

Constitui um dado assente que o paradigma que esteve subjacente ao legislador europeu para a elaboração do **RGPD** está firmemente plasmado no seu artigo 1.º (Objecto e objectivos) [6] e profusamente explanado nos considerandos (1)[7], (2)[8], (4)[9], podendo resumir-se da seguinte forma:

- A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.
- Os princípios e as regras em matéria de protecção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à protecção dos dados pessoais
- É primordial respeitar todos os direitos fundamentais e observar as liberdade e os princípios reconhecidos na **Carta**, consagrados nos **Tratados**, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a protecção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à acção e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.
- O objectivo do **RGPD** é contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

Por outro lado, o âmbito de aplicação material do **RGPD**, encontra-se definido no seu artigo 2.º (âmbito de aplicação material) e profusamente explicitado nos considerandos (5)[10], (6)[11], (7)[12], podendo resumir-se da seguinte forma:

---

[6] ***Artigo 1.º*** *(Objecto e objectivos)*

1. O presente regulamento estabelece as regras relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à protecção dos dados pessoais.

3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a protecção das pessoas singulares no que respeita ao tratamento de dados pessoais.

[7] ***Considerando (1)*** *A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*

[8] ***Considerando (2)*** *Os princípios e as regras em matéria de protecção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à protecção dos dados pessoais. O presente regulamento tem como objectivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.*

[9] *Considerando (4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à protecção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a protecção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à acção e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.*

- As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas actividades o que provocou um aumento significativo dos fluxos de dados pessoais.
- O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia.
- Esta evolução exige um quadro de protecção de dados sólido e mais coerente na União pelo que deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.

Proposta de alteração da **[Exposição de Motivos]**

Do exposto acima pode-se concluir que, entre os principais objectivos do RGPD estão, por um lado, a defesa dos direitos e liberdades das pessoas singulares no que respeita à protecção dos seus dados pessoais e, por outro lado, a implementação de um quadro de protecção de dados sólido e mais coerente na União pelo que se propõe a correcta adequação do texto final.

[Encarregado de protecção de dados]

O PAPEL DO DPO

O **RGPD** define a figura do **DPO**, atribuindo-lhe um papel central neste novo quadro normativo relativamente a um vasto número de entidades, de forma a facilitar o cumprimento das suas disposições.

Assim, o **DPO** é de designação obrigatória[13] em todas as **Autoridades e Organismos Públicos** (independentemente do tipo de dados que tratam e exceptuando os tribunais no exercício da sua função jurisdicional), bem como em outras

[10] ***Considerando** (5) A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro.*

[11] ***Considerando** (6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de protecção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas actividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de protecção dos dados pessoais.*

[12] ***Considerando** (7) Esta evolução exige um quadro de protecção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.*

[13] *Artigo 37.º (Designação do encarregado da protecção de dados)*

1.O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala 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.

Organizações cuja actividade 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 exija especificamente a nomeação de um **DPO**, o Comité Europeu para a Protecção de Dados – **CEPD** *(anteriormente designado como "Grupo do Artigo 29.º para a protecção de dados", também conhecido por WP29)* é favorável à sua designação a título voluntário por parte de entidades que considerem, nalguns casos, ser conveniente designar[14].

Os **DPOs** não são pessoalmente responsáveis em caso de incumprimento do disposto no **RGPD**. O cumprimento das regras de protecção de dados é uma competência do responsável pelo tratamento ou do subcontratante. Para tal, 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 (art. 24.º, n.º 1).

A EXIGÊNCIA DA FUNÇÃO DE DPO - AS COMPETÊNCIAS E CONHECIMENTOS ESPECIALIZADOS

A relação entre a tecnologia e o Direito manifesta-se de modo especial nos temas da privacidade. No caso concreto da prossecução da função de **DPO**, toma especial relevo a verificação das competências que o capacitem para a análise, desenvolvimento e acompanhamento da implementação da conformidade das medidas no âmbito da protecção de dados pessoais, designadamente na interpretação, análise e validação do cumprimento da conformidade relativos aos:

- princípios e as licitudes relativos ao tratamento de dados pessoais (art.5.º e 6.º)
- condições aplicáveis ao consentimento (art.7.º)
- tratamentos de categorias especiais de dados pessoais e dos tratamentos de dados pessoais relacionados com condenações penais e infracções (arts.9.º e 10.º)
- exercício dos direitos dos titulares dos dados (arts.12.º a 25.º)
- obrigações e responsabilidades das entidades actuantes quer como responsável pelo tratamento quer como subcontratante de tratamentos de dados pessoais (arts.24.º a 31.º)
- implementação do conceito da proteção de dados desde a conceção e por defeito (art. 25.º)
- definição e realização de auditorias e/ou inspeções conduzidas em nome da entidade ou por esta mandatado, para validação e apoio à demonstração do cumprimento das suas obrigações (art. 28, n.º 3, alínea h))
- manutenção de um registo das atividades de tratamento sob a responsabilidade da entidade (art. 30.º)
- cooperação com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições (art. 31.º)
- segurança dos dados pessoais (arts.32.º a 34.º)
- medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares. (art. 32.º)
- framework de gestão de riscos de forma a cumprir com a aquisição de um nível de segurança adequado, devendo ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição,

[14] *WP243 - Guidelines on Data Protection Officers ('DPOs')*

perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (art. 32.º, n.º 2)

- notificação e comunicação de violação de dados pessoais, nomeadamente no acompanhamento das avaliações do risco para os direitos e liberdades das pessoas singulares resultantes dos incidentes, bem como dos processos de notificação às autoridades de controlo e/ou comunicação de violação de dados pessoais a titulares dos dados (art. 33.º e 34.º)
- avaliação de impacto sobre a protecção de dados (art. 35.º)
- Na capacidade de cumprimento das obrigações e responsabilidades do exercício de funções do encarregado da protecção de dados (art. 39.º)
- Apoio na sensibilização, acompanhamento e fiscalização das boas práticas técnico-organizacionais da entidade no que concerne à protecção de dados pessoais
- Etc....

Pelo exposto, importa pois definir o nível de especialização, as qualidades profissionais e a capacidade para o correcto desempenho destas funções.

Assim, o RGPD dispõem no seu art. 37.º, n.º5:

> *O encarregado da protecção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de protecção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.*

Assim, e no acompanhando a Opinião 243 do **CEDP**[15], somos da opinião que o **DPO** deve ter:

- um nível de competências ajustado à sensibilidade, complexidade e quantidade de dados tratados pelas entidades;
- competências no domínio do Direito e práticas nacionais e europeias em matéria de protecção de dados e um conhecimento profundo do RGPD;
- um bom conhecimento tecnológico ao nível de sistemas de informação, da segurança dos dados e das necessidades de protecção de dados;
- um conhecimento adequado ao nível da organização e gestão de entidades, das operações de tratamento típicas e das regras e procedimentos administrativos organizacionais;
- um elevado nível de ética e integridade profissional;
- capacidade de desempenhar um papel determinante na promoção de uma cultura de proteção de dados no seio da entidade.

Como tal, resulta ser fundamental que o **DPO** disponha de um conjunto alargado de competências no âmbito da protecção de dados, concretamente na área jurídica, na área técnica e na área organizacional, de forma a contribuir no cumprimento dos elementos essenciais do **RGPD**.

---

[15] Opinion 243 - Guidelines on Data Protection Officers ('DPOs' http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Por último, o **DPO** deverá ser escolhido de forma criteriosa, tendo devidamente em conta as questões de protecção de dados suscitadas no âmbito da entidade

Proposta de alteração do **[Artigo 9.º - Disposição geral]**

O encarregado de protecção de dados, designado com base nos requisitos previstos no n.º 5 do artigo 37.º do RGPD, carece de certificação profissional para o desempenho das funções a que se refere o artigo 39.º do RGPD.

Proposta de **[Artigo 9.º - A – Certificação Profissional]**

A certificação profissional referida no artigo 9.º será objecto de regulamentação por parte da autoridade de controlo nacional, a que se refere o artigo n. 3º.

PROPOSTA DE SUPRESSÃO DE ARTIGOS[16]

Proposta de supressão do **[Artigo 10.º - Dever de sigilo]**

[Suprimir]

Proposta de supressão do **[Artigo 11.º - Funções do encarregado de protecção de dados]**

[Suprimir]

INCOMPATIBILIDADES E CONFLITO DE INTERESSES

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

Assim, e acompanhando a Opinião 243 do **CEDP**[17], somos da opinião que embora os **DPOs** estejam autorizados a desempenhar outras tarefas, só podem ser incumbidos de outras funções e atribuições se estas não derem origem a conflitos de interesses.

Assim, secundamos a Opinião 243 do **CEDP**[18], relativamente aos cargos susceptíveis de gerar conflitos no seio da entidade:

> *"...regra geral, os cargos susceptíveis de gerar conflitos no seio da organização podem incluir não só os cargos de gestão superiores (por exemplo, director executivo, director de operações, director financeiro, director do*

[16] *Tal como referido no ponto 12.2 do Joint Practical Guide sobre como legislar de acordo com as regras da União Europeia, que refere que "such repetition is dangerous, since any departure from the original wording may give the impression that a different result was intended, and even give rise to a presumption to that effect."*

[17] Opinion 243 - Guidelines on Data Protection Officers ('DPOs' http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

[18] Opinion 243 - Guidelines on Data Protection Officers ('DPOs' http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

departamento médico, director de marketing, director dos recursos humanos ou director 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."

Por conseguinte, o **DPO** não pode exercer um cargo dentro da entidade que o leve a determinar as finalidades e os meios do tratamento de dados pessoais nem pode, *maxime*, efectuar o tratamento de dados pessoais! Este será o caso em que seja chamado a representar a entidade perante autoridades ou organismos públicos no âmbito de processos que envolvam questões de protecção de dados. Um exemplo prático deste conflito de interesses, secundado na referida opinião do **CEPD**, será o exercício de funções de contabilista externo ou o exercício de funções de atendimento de clientes ao balcão para a venda de determinados produtos ou serviços.

Proposta de **[Artigo 9.º - B – Conflitos de interesses]**
O encarregado de protecção de dados abrangido pelos requisitos previstos no n.º 6 do artigo 38.º, deverá comunicar à autoridade de controlo nacional, a que se refere o artigo n. 3º, a declaração de inexistência de conflito de interesses.

A ANÁLISE DO RISCO DAS ENTIDADES

Dependendo do âmbito de intervenção da entidade, serão várias as categorias de dados pessoais com que esta terá de lidar nas suas operações diárias: desde dados pessoais de funcionários/colaboradores, a dados pessoais de utentes, de clientes, de cidadãos, de munícipes, de ex-funcionários/colaboradores, de visitantes, etc...

Uma entidade típica, será potencialmente responsável e responsabilizável perante dezenas, centenas ou milhares de pessoas singulares (os titulares de dados) que, entre outras, deverão de ter obrigatoriamente as garantias[19] da existência de condições necessárias para o correcto e eficaz exercício dos seus direitos (direito a aceder, a consultar, a alterar, a apagar, a portar, etc..).

Na situação de uma autoridade ou um organismo público pretender designar um único **DPO** para assumir funções para várias dessas autoridades ou organismos, o art.37, n.º3 do **RGPD** autoriza a designação do **DPO** nesses termos, desde que seja tido em conta "a respectiva estrutura organizacional e dimensão":

1. *Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da protecção de dados para várias dessas autoridades ou organismos, tendo em conta a respectiva estrutura organizacional e dimensão.*

[19] Exemplos: garantias de segurança dos seus dados pessoais, garantias de tratamento lícito, garantias de protecção contra incidentes de violação de dados pessoais, etc.,

Assim sendo, e dado que o **DPO** é responsável por uma variedade de tarefas exigentes, a designação do mesmo **DPO** por vários serviços ou entidades é uma opção que só pode ser seguida se forem asseguradas as condições adequadas para o cumprimento eficiente dos seus deveres, não podendo daqui resultar prejudicada a garantia dos direitos dos cidadãos.

Neste sentido, considera-se desconforme com o RGPD a designação do mesmo **DPO** para exercer funções na totalidade dos serviços de num determinado Ministério. Pelo contrário, importará efectuar uma análise de risco à entidade em causa, atendendo à sua dimensão, volume de dados tratados, existência de tratamento de categorias especiais de dados para, em concreto, permitir a agregação das funções de DPO pela mesma pessoa. Esta agregação terá ainda de exigir uma prévia aferição dos eventuais incompatibilidades e conflitos de interesses que podem surgir, designadamente quando existam transferências de dados entre esses serviços – para não entrar nas questões relativas à classificação dos trabalhadores integrados em carreiras que venham a ser designados, e à respectiva independência. Exemplificando, no âmbito do "Ministério da Educação", parece altamente recomendável a designação obrigatória de um **DPO** para cada entidade "Faculdade", "Instituto Superior", "Agrupamento Escolar", bem como para as estruturas, pelo menos centrais, do próprio Ministério da Educação. Todavia, se existirem agrupamentos escolares de muito pequena dimensão, ou serviços centrais com muito reduzido tratamento de dados pessoais, poderá ser ponderada a agregação que, todavia, nunca deverá ser a regra.

SOBRE AS ENTIDADES CUJA DESIGNAÇÃO DO DPO É OBRIGATÓRIA

No que concerne à definição de algum tipo de linha-delimitadora relativamente à designação de **DPO**, a nossa análise tenta interpretar o articulado no **RGPD** com as opiniões emanadas do **CEPD**, mais especificamente, a já referida "*Opinion 243 - Guidelines on Data Protection Officers ('DPOs')*", adoptada em 5 abril 2017.

Assim, o **RGPD** define no seu art. 37.º, n.º1, os três factores de designação obrigatória de **DPOs**:

1. *O responsável pelo tratamento e o subcontratante designam um encarregado da protecção de dados sempre que:*
    a. *O tratamento for efectuado por uma autoridade ou um organismo público, exceptuando os tribunais no exercício da sua função jurisdicional;*
    b. *As actividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou*
    c. *As actividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infracções a que se refere o artigo 10.º.*

Assim, no que concerne à alínea a), entende-se que todas as autoridades públicas bem como todos os organismos públicos, devem designar **DPOs**.

Exemplos de autoridades e organismos públicos:

- Administração Central do Sistema de Saúde (ACSS), I.P
- Associação Nacional de Municípios Portugueses (ANMP)
- Autoridade Nacional de Protecção Civil (ANPC)

- Direcção-Geral de Energia e Geologia (DGEG)
- Infraestruturas de Portugal, S.A. (IP, S.A.).
- Gabinete de Estratégia e Planeamento (GEP/MTSSS)
- Agência Portuguesa do Ambiente
- Instituto Português do Mar e da Atmosfera (IPMA)
- Laboratório Nacional de Energia e Geologia (LNEG)
- Navegação Aérea de Portugal — NAV Portugal, E. P. E
- ADENE – Agência para a Energia
- AMTL - Autoridade Metropolitana de Transportes de Lisboa
- ANSR – Autoridade Nacional de Segurança Rodoviária
- APA – Agência Portuguesa do Ambiente
- CCDR Algarve – Comissão de Coordenação e Desenvolvimento Regional do Algarve
- CIG - Comissão para a Cidadania e a Igualdade de Género
- DGOTDU – Direcção Geral do Ordenamento do Território e Desenvolvimento Urbano
- DGC - Direcção Geral do Consumidor

Nesta âmbito, também é nosso entendimento que as entidades privadas que prosseguem fins públicos devem designar **DPOs.** Exemplos:

- Prestação de serviços públicos de transporte (Metro de Lisboa, Carris, CP, Metro do Porto, STCP, etc..)
- Prestação de serviços públicos de fornecimento de água (EPAL, Aguas do Porto, etc..)
- Prestação de serviços públicos de fornecimento de energia (EDP, GALP GAS, etc..)
- Prestação de serviços públicos de televisão e rádio (RTP, RDP, LUSA, etc..)
- Prestação de serviços públicos de regulação de profissões (Ordens Profissionais, etc..)
- Prestação de serviços públicos de saúde (Hospitais em regime de PPP)
- Prestação de serviços públicos de infraestruturas e mobilidade (Autoestradas PPP, etc..)

No que concerne à alínea b), e no seguimento da opinião do **CEPD**, as "actividades principais" devem ser consideradas como as operações principais que a organização efectua para atingir os seus objectivos de negócio. Estas também devem incluir todas as actividades em que o processamento de dados forma parte intrínseca da actividade da organização.

Por exemplo, o processamento de dados de saúde, como os registros de saúde de pacientes, deve ser considerado como uma das actividades principais de qualquer hospital e, portanto, estes devem designar **DPOs** obrigatoriamente. Uma empresa de segurança privada que opera sistemas de CCTV remoto em diversos locais de acesso ao público (ex: lojas, escritórios, etc...) tem de designar um **DPO** obrigatoriamente.

No que concerne à alínea b), e no alinhamento com a opinião do **CEPD**, o tratamento em "grande escala" deve ser analisado segundo os seguintes factores:

- O número de pessoas singulares em causa - quer como um número específico ou como uma proporção da população relevante (ex: 1000 ou mais pessoas singulares);
- O volume de dados e/ou o intervalo de categorias de dados diferentes que estão em tratamento

- A duração da actividade de tratamento de dados (ex: durante 3 ou mais anos)
- A cobertura geográfica da actividade de tratamento (ex: Região de Lisboa e Vale do Tejo)

Exemplos de tratamentos em grande escala:

- Tratamento de dados de pacientes no decurso da actividade normal de um hospital;
- Tratamento de dados de viagens de passageiros que utilizam o sistema de transporte público de uma cidade (por exemplo, rastreamento através de cartões de viagem);
- Tratamento de dados, em tempo real, da geo-localização de clientes de uma cadeia de *fast-food*, para fins estatísticos, por um subcontratante especializado na prestação desses serviços;
- Tratamento de dados de clientes no decurso da actividade normal de uma companhia de seguros ou de um banco;
- Tratamento de dados pessoais para publicidade comportamental direccionada por parte de um motor de pesquisa de internet;
- Tratamento de dados (conteúdo, tráfego, localização) por prestadores de serviços de telecomunicações ou de internet;
- Entidades prestadoras de serviços de "*website analytics*" e "*targeted advertising and marketing*";
- Entidades prestadoras de serviços de Segurança e Saúde do Trabalho.

No que concerne à alínea b), e no seguimento da opinião do **CEPD**, o "controlo regular e sistemático" pode ser analisado como o "controlo do comportamento dos titulares dos dados, ... pessoas (que) 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". Sendo este um exemplo existirão outras situações onde ocorre o controlo regular e sistemático de pessoas singulares.

O **CEPD** interpreta como "regular", um tratamento que se encaixe num ou mais dos seguintes items:

- Tratamento em curso ou ocorrendo em intervalos específicos num determinado período;
- Tratamento recorrente ou repetido em períodos de tempo fixo;
- Tratamentos de forma constante ou ocorrendo de forma periódica.

O **CEPD** interpreta como "sistemático" um tratamento que se encaixe num ou mais dos seguintes items:

- Tratamento que ocorre de forma regular;
- Tratamento pré-organizado, organizado ou metódico;
- Tratamento que ocorre como actividade incluída num plano geral de recolha de dados;
- Tratamento que ocorre como actividade incluída numa estratégia organizacional.

Assim, apresentam-se de seguida exemplos de tratamentos de controlo regular e sistemático de pessoas:

- Operação de uma rede de telecomunicações;
- Fornecimento de serviços de telecomunicações;
- Perfilagem de pessoas para actividades de marketing ou email personalizado;

- Perfilagem e avaliação de pessoas para fins de avaliação de risco (por exemplo, para fins de pontuação de crédito, estabelecimento de prémios de seguro, prevenção de fraude, detecção de branqueamento de capitais, etc..);
- Rastreamento de localização, por exemplo, por aplicações móveis;
- Tratamento de dados no âmbito de programas de fidelização ou publicidade comportamental;
- Tratamento de dados no âmbito da monitorização de dados de bem-estar, fitness e saúde através de dispositivos portáteis (wearables);
- Tratamento de dados de imagem e som por CCTV - circuito fechado de televisão;
- Tratamento de dados no âmbito da IoT – Internet of Things, ex: medidores inteligentes, carros inteligentes, domótica, etc.

Assim, no que concerne à alínea c), e no alinhamento com a opinião do **CEPD**, entende-se por tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º 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*, bem como os dados pessoais relacionados com condenações penais e infracções a que se refere o artigo 10º.

Assim, apresentam-se de seguida exemplos de tratamentos de categorias especiais de dados:

- Tratamento de dados no âmbito de programas de acção social escolar;
- Tratamento de dados no âmbito das actividades sindicais;
- Tratamento de dados biométricos para controlo de acesso a edifícios;
- Tratamento de dados de saúde no âmbito da Segurança e Saúde do Trabalho (SST);

Como tal, deverá ser previsto a definição dos "limites organizacionais" a partir do qual seja obrigatória a designação de um **DPO** por parte de determinada entidade. Esta questão carece de especial atenção no caso dos Municípios, devendo o diploma definir qual o órgão ou órgãos responsáveis pelo tratamento, a quem compete a designação do respectivo DPO, e, no caso das freguesias, eliminar a regra constante da Proposta nos termos da qual apenas algumas freguesias necessitam de proceder à designação de DPO. Importa atender que as freguesias possuem competências, designadamente na área social, que importam o tratamento de um volume significativo de categorias especiais de dados.

Proposta de **[Artigo 9.º - C – Regime de exclusividade]**

O encarregado de protecção de dados, designado com base nos requisitos previstos no n.º 1, do artigo 37.º do RGPD, exerce as suas funções em regime de exclusividade.

Proposta de alteração **[Artigo 12.º - Encarregados de protecção de dados em entidades públicas]**

1. Para efeitos do número anterior, entende-se por entidades públicas:

(...)

i) Entidades privadas que prosseguem fins públicos

j) Sector Empresarial do Estado, regional e local

2. [manter articulado]

3. [suprimir]

4. [manter articulado]

Proposta de alteração do **[Artigo 13.º - Encarregados de protecção de dados em entidades privadas]**[20]

1. Nos termos da alínea b) e alínea c) do n.º 1 do artigo 37.º do RGPD, é obrigatória a designação de encarregados de protecção de dados de acordo com o disposto nos números seguintes.

2. Para efeitos do número anterior, entende-se por "tratamento em grande escala", designadamente as seguintes situações:

- **a. Tratamentos de dados de operação de rede ou fornecimento de serviços de telecomunicações;**
- **b. Tratamento de dados (conteúdo, tráfego, localização) por prestadores de serviços de telecomunicações ou de internet;**
- **c. Tratamento de dados de clientes no decurso da actividade normal de uma companhia de seguros ou de um banco;**
- **d. Tratamento de dados, em tempo real, da geo-localização ou rastreamento de localização;**
- **e. Tratamento de dados no âmbito de programas de fidelização ou publicidade comportamental;**
- **f. Tratamento de dados de perfilagem e avaliação de pessoas para fins de avaliação de risco;**
- **g. Tratamento de dados de pacientes no decurso da actividade normal de um hospital;**
- **h. Tratamentos de dados de serviços de Segurança e Saúde do Trabalho;**
- **i. Tratamento de dados no âmbito da monitorização de dados de bem-estar, fitness e saúde através de dispositivos portáteis (wearables)**
- **j. Tratamento de dados de viagens de passageiros;**
- **k. Tratamentos de dados de serviços de "website analytics" e "targeted advertising and marketing";**
- **l. Tratamento de dados no âmbito da "IoT" (internet of things)**
- **m. Tratamento de dados de imagem e som por CCTV em vários locais de acesso ao público;**
- **n. Tratamento de dados com 1000 ou mais pessoas singulares em causa**
- **o. Tratamento de dados cuja duração da actividade de tratamento ocorra durante 3 ou mais anos;**
- **p. Tratamento de dados cuja cobertura geográfica da actividade de tratamento incluam mais do que uma Região Administrativa;**

3. Para efeitos do número 1, entende-se por "controlo regular", designadamente as seguintes situações:

- **a. Tratamento em curso ou ocorrendo em intervalos específicos num determinado período;**
- **b. Tratamento recorrente ou repetido em períodos de tempo fixo;**
- **c. Tratamentos de forma constante ou ocorrendo de forma periódica.**

4. Para efeitos do número 1, entende-se por "controlo sistemático", designadamente as seguintes situações:

- **a. Tratamento que ocorre de forma regular;**
- **b. Tratamento pré-organizado, organizado ou metódico;**
- **c. Tratamento que ocorre como actividade incluída num plano geral de recolha de dados;**
- **d. Tratamento que ocorre como actividade incluída numa estratégia organizacional.**

Com os nossos melhores cumprimentos,

Lisboa, 15 de Novembro de 2018

[20] *Idem*