CONTRIBUTOS PARA A ANÁLISE DO ARTICULADO

NO

PROJETO DE TEXTO DE SUBSTITUIÇÃO DA PROPOSTA DE LEI N.º 120/XIII/3.ª (GOV)

ASSEMBLEIA DA REPÚBLICA - COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS - GRUPO DE TRABALHO – REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

A "**Associação Nacional de DPOs e Outros Profissionais de Privacidade (ANDPO)**", vem apresentar os seus contributos relativamente PROJETO DE TEXTO DE SUBSTITUIÇÃO DA PROPOSTA DE LEI N.º 120/XIII/3.ª (GOV), 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 Protecção de Dados ou RGPD), relativo à protecção 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 encaminhadas através do email geral@andpo.pt

Preâmbulo

A ANDPO tem vindo a acompanhar os esforços desenvolvidos para a adaptação do RGPD à ordem jurídica nacional.

De facto, já em **30 de Setembro de 2017** tivemos a oportunidade de submeter o nosso contributo na "**Consulta Pública para aprovação de Legislação Nacional relativa ao Regulamento Geral de Protecção de Dados (RGPD)**"[1].

Posteriormente, em **15 de Novembro de 2018**, apresentamos os nossos contributos relativamente à **Proposta de Lei N.º 120/XIII**, expressando a nossa posição relativamente aquela proposta, tendo em conta a conjuntura existente à data em que o documento foi entregue.

Recentemente, tivemos o ensejo de **debater esta temática com os candidatos[2] ao Parlamento Europeu 2019/2024**. Para tal, lançamos o desafio a todas as 17 listas candidatas para a participação no evento "Privacidade e Protecção de Dados no desenvolvimento do projecto Europeu", que decorreu a **7 Maio de 2019**, no ISEG (Lisboa).

Agora, vimos novamente submeter o nosso contributo relativamente ao **Projecto de Texto de Substituição da Proposta de Lei N.º 120/XIII/3.ª (GOV)** disponibilizado nos últimos dias.

Fundamentos para a reapreciação sobre o perfil do ético e profissional do DPO:

- **Privacidade e a dignidade são direitos fundamentais dos cidadãos.**
  A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental de todo e qualquer cidadão europeu.
- **As práticas de gestão da privacidade adoptadas pelas entidades devem pautar-se pelo compromisso ético e pela auto-responsabilização para com os titulares dos dados.**
  Os dados pessoais pertencem aos cidadãos, não pertencem nem aos governos nem às corporações. Neste âmbito, é errado privilegiar um sector relativamente a outro sector, exemplo, privilegiar o sector público em determinado elemento relativamente ao sector privado (ex: aplicação de coimas).
- **A União Europeia deve continuar a ter um papel decisivo na promoção da Privacidade e da Protecção de Dados.**
  O RGPD[3] proporciona um moderno quadro regulatório com enfoque nos direitos dos cidadãos e na responsabilização das entidades em matéria de protecção de dados. Esta opção de políticas públicas deve prosseguir de forma a acompanhar as tremendas exigências que se nos coloca o evoluir dos tempos.
- **A conformidade com a privacidade é uma necessidade absoluta**.
  Embora a tecnologia contenha muitas promessas, é importante ter presente as suas ameaças face às contínuas disrupções tecnológicas
- **Existe um risco real de se criarem ditaduras digitais**
  Nestas, todo o poder concentra-se nas mãos de uma pequeníssima elite, de cientistas, empresas e governos (ver o caso *Cambridge Analytics*). É pois importante encetarmos esforços na regulação do uso

[1] Consulta lançada pelo "Grupo de Trabalho com o objectivo de preparar a legislação portuguesa para a aplicação do Regulamento Geral de Protecção de Dados (RGPD) em Portugal"
[2] Os representantes do PSD, do BE, da CDU, do CDSP-PP, da ALIANÇA e do LIVRE partilharam connosco as suas visões, ideias e projectos sobre esta temática.
[3] 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

da informação pelas tecnologias emergentes de *Social Individual Ratings* (China), *Big Data*, *Inteligência Artificial*, *Blockchain*, *IoT*, *Computação Quântica*, *Biotecnologia*, *Nanotecnologia*, etc..

- **É primordial melhorar a literacia digital no âmbito da cibersegurança e da privacidade**.

A exigência da função do Data Protection Officer

Os **DPOs** têm um papel central neste novo quadro normativo de protecção dos dados porquanto actuam como facilitadores e controladores do cumprimento das disposições do RGPD.

Será pois fundamental o papel do **DPO** para, em última análise, e em conformidade com o RGPD, garantir o correcto respeito pelos direitos e liberdades fundamentais dos titulares dos tratamentos de dados.

As competências especializadas da função de Data Protection Officer

Para a correcta prossecução da função de **DPO**, assume 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[4].

Assim, e acompanhando a Opinião 243 do **Comité Europeu da Proteção de Dados**[5], parece-nos que o **DPO** deve ter:

- **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 técnicas em matéria 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**;
- um perfil de competências ajustado à sensibilidade, complexidade e quantidade de dados tratados pelas entidades;
- 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 tecnológica e na área organizacional.

[4] *Ver ANEXO 1 – Competências especializadas necessárias ao DPO, de forma a lidar adequadamente com os requisitos do RGPD*
[5] *Opinion 243 - Guidelines on Data Protection Officers ('DPOs' http://ec.europa.eu/newsroom/document.cfm?doc_id=44100*

O que tem acontecido neste primeiro ano de aplicabilidade do RGPD :

- **Uma grande escassez de profissionais com competências especializadas no âmbito da protecção de dados[6].**

  Desta escassez resulta o florescimento de um mercado de oportunistas, sem capacidade de lidar adequadamente com o RGPD.
- **O recurso sistemático de designação de DPO num recurso interno da organização, sem competência nem apetência no âmbito da protecção de dados[7].**

  Tal é uma péssima opção pois resulta num risco para a defesa dos direitos e liberdades dos titulares dos dados.
- **Uma escassez de orientações por parte das Autoridades de Controlo (CNPD).**

  Persiste um clima de incerteza relativamente a variados aspectos práticos adequados no que concerne ao cumprimento do RGPD.
- **Uma quantidade assustadoramente crescente de incidentes de cibersegurança**.

  Estes têm dado origem a inúmeras situações de violações de dados pessoais.
- **Alertas de diversos autores contemporâneos para os riscos da falta de ética no tratamento de questões relacionadas com a privacidade**.[8][9][10][11]

  À data de hoje, já passamos a *fase orwelliana* da vigilância global e manipulação pública e histórica. Estamos a entrar na fase em que os algoritmos automaticamente decidem por nós. Tal coloca uma séria ameaça aos valores da liberdade e igualdade. Tal como os concebemos hoje.

Face ao exposto, propomos alterações no sentido de:

- **Recentrar o debate na promoção da privacidade e da dignidade como direitos fundamentais dos cidadãos.**

  Os requisitos (obrigações/penalizações) em matérias de protecção de dados devem ser igualmente exigidos a todas as entidades. Não concordamos com a não aplicabilidade *ad eternum* de coimas ao sector público.
- **Investir no correcto desempenho da função de DPO.**

---

[6] *Study: An estimated 500K organizations have registered DPOs across Europe, IAPP, Maio 2019, https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe*

[7] *Já houve quatro multas em Portugal por causa do RGPD; https://eco.sapo.pt/2019/05/17/ja-houve-quatro-multas-em-portugal-por-causa-do-rgpd-uma-foi-ao-hospital-do-barreiro-e-tres-a-empresas-privadas*

[8] *"21 Lições para o Século 21", Yuval Noah Harari; https://pt.wikipedia.org/wiki/21_Li%C3%A7%C3%B5es_para_o_S%C3%A9culo_21*

[9] *"Zucked – Waking Up to the Facebook Catastrophe", Roger McNamee, https://www.amazon.com/Zucked-Waking-Up-Facebook-Catastrophe/dp/0525561358*

[10] *"The Age of Surveillance Capitalism", Shoshana Zuboff, https://www.bertrand.pt/livro/the-age-of-surveillance-capitalism-professor-shoshana-zuboff/21901899*

[11] *"China social credit system: punishments and rewards explained", Alexandra Ma, https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4*

É importante, designadamente, regulamentar o nível de especialização necessário para o exercício da função, salvaguardar as regras na designação do mesmo DPO para várias entidades ou criar mecanismos de fiscalização do correcto exercício da função.

- **Quantificar o que são operações de tratamento em "*grande escala*".**
  Densificar o conceito abstracto de "grande escala" referido nas alíneas b) e c) do n.º 1 do art. 37º do RGPD.

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 dos designados para exercer esta função**.

Análise ao PROJETO DE TEXTO DE SUBSTITUIÇÃO DA PROPOSTA DE LEI N.º 120/XIII/3.ª (GOV)

[Encarregado de protecção de dados]

Proposta de alteração do **[Artigo 9.º - Disposição geral]**
[Alterar] **1. O encarregado de proteção de dados é designado com base nos requisitos previstos no n.º 5 do art. 37.º do RGPD, ~~não~~ carecendo de certificação profissional para o efeito.** **2. [Manter…]** **3. A certificação profissional referida no n.º 1 será objecto de regulamentação.** **4. Sem prejuízo do disposto no n.º 1, o cumprimento dos requisitos estabelecidos no artigo n.º 5 do art. 37º do RGPD pode também ser demonstrado através de mecanismos de certificação voluntária que terão particularmente em conta a obtenção de um diploma universitário que credencie conhecimentos especializados no domínio do direito, engenharia ou gestão de organizações.** **5. O encarregado de protecção de dados abrangido pelo previsto no n.º 6 do art. 38.º do RGPD, deverá emitir declaração abonatória dessa conformidade.** **6. O encarregado de proteção de dados deverá ser capaz de demonstrar o cumprimento dos requisitos previstos nos números anteriores, sempre que tal for solicitado pelas entidades fiscalizadoras, pelo responsável pelo tratamento ou pelo subcontratante.** **7. Os responsáveis pelo tratamento e os subcontratantes devem comunicar à Comissão Nacional de Proteção de Dados, no prazo de dez dias, as designações, nomeações e demissões do encarregado de protecção de dados.** **8. A Comissão Nacional de Proteção de Dados manterá uma lista pública actualizada de encarregados de proteção de dados, acessível por meios electrónicos.**

[Entidades públicas]

Proposta de alteração **[Artigo 12.º - Encarregados de protecção de dados em entidades públicas]**
[Acrescentar] **1. [Manter…]** **2. Para efeitos do número anterior, entende-se por entidades públicas:** **(…)** **i)As entidades privadas que prosseguem fins públicos** *(Nota: As Misericórdias, IPSS, Mutualistas, ONGs, etc.. pela sua natureza de actuação, têm na sua posse uma elevada quantidade de dados sensíveis de saúde, financeiros, sócio-culturais, etc. relativa a crianças e idosos.)* **3. [Manter…]** **4. Nos termos do n.º 3 do artigo 37.º do RGPD, pode ser designado o mesmo encarregado de proteção de dados para vários ministérios ou áreas governativas, secretarias regionais, autarquias locais ou outras pessoas coletivas públicas, salvaguardando a análise ponderada das respectivas estruturas e dimensões organizacionais, o volume de tratamentos, a existência de categorias especiais de dados pessoais tratados e os riscos para os direitos ou liberdades dos titulares de dados.** **5. [Manter…]** **6. [Manter…]**

[tratamento em grande escala]

Proposta de alteração do **[Artigo 13.º - Encarregados de proteção de dados em entidades privadas]**
[Acrescentar] **2. Entende-se por tratamento em grande escala, operações de tratamento que abranjam um número igual ou superior a 750 de titulares de dados** *(Nota: tal como quantificado na alínea d), n.º 3 do art. 12º da presente lei.)*

[Aplicabilidade das coimas às entidades públicas]

Proposta de alteração do **[n.3 do Art. 44.º - Âmbito de aplicação das contraordenações]**
[Alterar] **1- [Manter…]** **2- Nos termos do disposto no n.º 7 do artigo 83.º do RGPD, as entidades públicas, mediante pedido devidamente fundamentado, podem solicitar à Comissão Nacional de Proteção de Dados a dispensa temporária da aplicação de coimas por um período máximo de dois anos, durante o prazo de três anos a contar da entrada em vigor da presente lei.** *3-* **[Suprimir]** *(Nota: Redundância. Já está previsto no número anterior.)*

Proposta de supressão do **[Artigo 59.º - Aplicabilidade das coimas às entidades públicas]**
[Suprimir] *(Nota: Redundância. Já está previsto no artigo 44º.)*

Com os nossos melhores cumprimentos,

P'la Direcção da ANDPO

Henrique Necho

Reunião da Direcção da ANDPO de 21 Maio 2019

ANEXO 1 - Competências especializadas necessárias ao DPO, de forma a lidar adequadamente com os requisitos do RGPD

Competências Jurídicas necessárias para verificar a conformidade de, designadamente**:**

- Princípios e a 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)
- 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)
- Cooperação com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições (art. 31.º)
- 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)
- Na capacidade de cumprimento das obrigações e responsabilidades do exercício de funções do encarregado da protecção de dados (art. 39.º)

Competências Tecnológicas no âmbito das TIC, para verificar a conformidade de, designadamente:

- 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))
- 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)

Competências Organizacionais e de Gestão, para verificar a conformidade de, designadamente:

- exercício dos direitos dos titulares dos dados (arts.12.º a 25.º)
- implementação do conceito da proteção de dados desde a conceção e por defeito (art. 25.º)
- avaliação de impacto sobre a protecção de dados (art. 35.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, 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 (n.º 2 do art. 32.º)
- manutenção de um registo das atividades de tratamento sob a responsabilidade da entidade (art. 30.º)
- Apoio na sensibilização, acompanhamento e fiscalização das boas práticas técnico-organizacionais da entidade no que concerne à protecção de dados pessoais