MACEDO VITORINO

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O IMPACTO DO RGPD NA ADMINISTRAÇÃO PÚBLICA

MACEDO VITORINO

ÍNDICE

INTRODUÇÃO

O Regulamento Geral de Proteção de Dados (RGPD) impõe novos desafios à Administração pública em matéria de proteção de dados, alguns deles, todavia, ainda por adotar três anos volvidos da sua aplicação.

A atual situação pode dever-se à possibilidade de uma «moratória» de três anos quanto a coimas prevista na lei de execução do RGPD, e que será objeto de revisão no próximo ano.

Certo é que, com ou sem dispensa de coima, a Administração pública tem de se consciencializar de que precisa de implementar cabalmente o RGPD porque os cidadãos têm direito à proteção dos seus dados pessoais e porque, mais tarde ou mais cedo, haverá sanções para evitar a violação do RGPD.

No início havia, aliás, a falsa ilusão de que a Comissão Nacional de Proteção de Dados (CNPD) não aplicaria de forma implacável o RGPD, ilusão que foi alimentada pelas notícias de falta de verbas desta autoridade.

Frustrando estas expetativas, a CNPD abriu, em 14 de outubro de 2018, um processo de averiguação à EMEL e à Câmara Municipal de Lisboa, na sequência do envio dos SMS pela EMEL com alertas sobre o furacão Leslie.

Uns dias mais tarde, a CNDP aplicaria uma coima de 400 mil euros ao Centro Hospitalar do Barreiro Montijo, EPE por acesso indevido a dados clínicos de doentes por profissionais não médicos.

O presente estudo visa analisar o impacto da aplicação do RGPD na Administração pública e as novas responsabilidades que decorrem para os serviços, organismos e entidades públicas, bem como as medidas-chaves a adotar na implementação do RGPD pelo sector público.

ALTERAÇÃO DOS PROCEDIMENTOS INTERNOS

A Administração pública deve adequar as suas políticas de privacidade e rever procedimentos internos para dar resposta aos reforçados direitos dos cidadãos

O RGPD veio alterar a forma como a Administração pública deve recolher, utilizar, comunicar, armazenar os dados pessoais dos seus utentes, clientes, fornecedores, funcionários, etc., e a interação da Administração pública com os cidadãos em geral, incluindo no âmbito dos pedidos de acesso a documentos administrativos que contenham dados pessoais.

É justificado o tratamento pela Administração pública quando for necessário ao exercício de funções de interesse público ou ao exercício de poderes de autoridade pública. Nestes casos, não será necessário um prévio consentimento ou a existência de um contrato para justificar o tratamento de dados pessoais.

O consentimento, que o RGPD impõe que seja livre, específico, informado e explícito, não será, aliás, válido para justificar o tratamento de dados pela Administração pública, quando sejam exercidos poderes de autoridade, dada a relação de desequilíbrio. Nos demais casos, e desde que cumpridos os referidos requisitos, o consentimento é válido.

Para conseguir dar uma resposta cabal e célere aos pedidos dos cidadãos, em particular de exercício dos direitos de informação, acesso, portabilidade e apagamento dos seus dados, a Administração pública deve adequar as políticas de privacidade, rever a informação transmitida aos cidadãos sobre a forma como protege os seus dados pessoais e criar procedimentos adequados por forma a satisfazer os diferentes pedidos. (e.g. criar uma linha de contacto e um registo de pedidos dos titulares).

O novo direito à portabilidade exige que a Administração pública seja capaz de, a pedido de um cidadão, transmitir os dados que lhe digam respeito e num formato interoperável ao próprio titular ou a um terceiro. Já o direito ao apagamento, exige que a Administração pública venha a ser dotada de meios para eliminar, a pedido de um cidadão, os dados pessoais.

Estes dois direitos não são, porém, absolutos; estão sujeitos a exceções. A portabilidade apenas tem lugar quando o tratamento for feito por meios automatizados e se baseie em consentimento (improvável, em vários casos) ou na execução de um contrato. A Administração pública poderá, por sua vez, recusar um pedido de apagamento de dados, quando estejam em causa, entre outros, motivos de interesse público no domínio da saúde pública ou de arquivo de interesse público

MÉTODOS DE INVENTARIAÇÃO E SUBCONTRATAÇÃO

A Administração pública e os seus subcontratados devem manter um registo das atividades de tratamento por forma a conseguir comprovar que cumprem o RGPD.

A Administração pública deve conseguir demonstrar que cumpre o RGPD.

Cada entidade pública com mais de 250 trabalhadores fica obrigada a manter um registo das atividades de tratamento. Esse registo não é mais do que um levantamento dos dados pessoais, finalidades de tratamento, categorias de titulares de dados e seus destinatários, prazos de conservação, etc.. Essa informação deverá ser consolidada num único documento (e.g. em folha Excel) e poderá ter de ser disponibilizada à CNPD.

O registo é sempre obrigatório se o tratamento implicar um risco para os direitos e liberdades dos cidadãos e não for ocasional ou disser respeito a categorias especiais de dados, e.g., dados de saúde e dados biométricos. O registo é aplicável às entidades subcontratadas pela Administração pública. Pense-se, por exemplo, em empresas de *outsourcing* de gestão de plataformas informáticas ou empresas que fornecem soluções tecnológicas à Administração pública.

Quando a Administração pública recorra a entidades subcontratadas deve assegurar um conjunto de requisitos no âmbito da relação contratual, para além daqueles que já decorrem das normas de contratação pública. A subcontratação tem de ser regulada por acordo escrito, podendo fazer parte do clausulado do próprio contrato (ou outro, que defina o objeto da relação) ou constar de um documento autónomo, por exemplo, um anexo ou acordo separado. O acordo de subcontratação tem de prever uma clara repartição de responsabilidades, do qual conste, entre outros aspetos:

- Que o subcontratado apenas atuará mediante instruções da entidade pública e que o seu pessoal fica sujeito a uma obrigação de confidencialidade;
- Que o subcontratado adotará as medidas técnicas e organizativas adequadas ao tratamento dos dados e que colaborará com a entidade pública na resposta aos pedidos de exercício de direitos dos cidadãos; e
- Que o subcontratado não poderá recorrer a subcontratados ulteriores sem o prévio consentimento escrito da entidade pública.

ADEQUAÇÃO DOS SISTEMAS DE GESTÃO E DE SEGURANÇA

A Administração pública deve rever os sistemas de gestão de tratamento e de segurança da informação por forma a prevenir acessos ou divulgações não autorizadas de dados.

O RGPD impõe a aplicação de «medidas técnicas e organizativas adequadas» à segurança da informação. Em caso de novos projetos, essas medidas devem ser aplicadas não apenas no momento do tratamento– «privacidade por defeito» –, mas desde a conceção do tratamento – «privacidade desde a conceção». Por exemplo, se a Administração pública pretender lançar uma nova plataforma para prestação de um serviço público, que envolva a recolha de dados dos cidadãos, os sistemas de gestão e de segurança da informação deverão ser pensados desde a conceção do serviço e acautelando os riscos associados.

Em matéria de arquitetura de segurança das redes e sistemas de informação, a resolução do Conselho de Ministros n.º 41/2018 de 28 de março prevê um conjunto de requisitos técnicos obrigatórios e recomendações, a adotar pela Administração direta e indireta do Estado.

Nos casos em que as operações de tratamento possam implicar um «elevado risco» para os cidadãos, será necessário realizar uma avaliação de risco, com parecer do DPO – «avaliação de impacto de proteção de dados» (AIPD). Embora o conceito de «elevado risco» ainda careça de ser concretizado, o RGPD dá alguns exemplos em que uma AIPD é obrigatória: definição de perfis, tratamento de categorias especiais de dados em grande escala, tratamento de um elevado volume de dados, dados recolhidos através de videovigilância ou geolocalização.

Se dessa avaliação resultar um elevado risco para os cidadãos, e não forem definidas medidas específicas para atenuar o risco, deverá ser feita uma consulta prévia (antes do tratamento) à CNPD. A CNPD tornará pública uma lista dos tipos de operações sujeitas a AIPD.

Em caso de violação de dados (e.g. quebra de segurança da qual resulte a destruição, perda, alteração, divulgação ou acesso não autorizado aos dados), as entidades públicas devem estar aptas a identificar a violação e, em caso de risco (e.g. se não forem adotadas medidas de proteção, como a cifragem), notificar a CNPD em 72 horas após o seu conhecimento, bem como informar os cidadãos, se o risco for elevado, com a maior brevidade possível.

DESIGNAÇÃO E FUNÇÕES DO ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

As autoridades e organismos públicos estão obrigados a designar um DPO, que terá por principal função auxiliar na implementação das novas regras.

Independentemente da atividade, número de trabalhadores, dimensão, as entidades públicas estão, em regra, obrigadas a designar um DPO, com exceção dos tribunais.

No âmbito da proposta de lei de execução do RGPD, colocava-se a questão de saber se todas as empresas do setor empresarial do Estado (SEE) estariam incluídas no conceito de «autoridade pública» do RGPD e ficavam, por essa via, obrigadas a designar um DPO.

A lei de execução do RGPD veio sanar essa dúvida, vinculando todas as empresas do SEE, mesmo quando não sigam uma forma jurídico-pública à designação de um DPO,

Designar a pessoa com o perfil mais adequado às funções de DPO, poderá não se revelar tarefa fácil e sobretudo num curto período de tempo.

O DPO, que deverá ter conhecimentos especializados no domínio do direito e das práticas de proteção de dados, terá como primeira missão colaborar na implementação do RGPD e controlar internamente o cumprimento das novas regras. Deve, por isso, ser envolvido, em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais e ter os recursos necessários ao desempenho, com independência, das suas funções. O DPO deve reportar diretamente à administração.

Dependendo da estrutura organizacional e dimensão da entidade pública, não é de excluir a hipótese de poder ser designado um único DPO para vários organismos públicos, desde que seja designado, pelo menos um, por área governativa, secretaria regional, município, freguesia e pessoa coletiva pública.

O RGPD tão-pouco exclui a hipótese de o DPO ser um colaborador interno ou que esta função possa ser assegurada por uma entidade externa, inclusivamente por uma equipa, desde que um dos seus elementos fique identificado como sendo o ponto de contacto junto da CNPD.

A designação do DPO é de comunicação obrigatória à CNPD e deve ser publicitada no sítio de Internet da entidade pública.

RESPONSABILIDADE E SANÇÕES PARA A ADMINISTRAÇÃO PÚBLICA?

O RGPD aumenta significativamente o valor das coimas, que podem chegar aos 20 milhões de euros ou 4% do volume de negócios anual a nível mundial se superior.

O RGPD deixa uma «porta aberta» a que a Administração pública possa ficar dispensada da aplicação de coimas, ao conferir aos Estados-membros a possibilidade de preverem normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos.

A lei de execução do RGPD veio prever a possibilidade de as entidades públicas, mediante pedido devidamente fundamentado, poderem solicitar à CNPD a dispensa da aplicação de coimas durante os primeiros três anos. Medida que se se encontra sujeito a posterior reavaliação.

Sem que a proposta de lei tivesse ainda sido aprovada, a CNPD aplicou ao Centro Hospitalar do Barreiro Montijo, EPE, uma entidade pública empresarial, uma coima de 400 mil euros por acesso indevido a dados clínicos por profissionais não médicos. Na altura, não havia a possibilidade do pedido de dispensa, pelo que, à partida, a dispensa não poderá ter lugar na presente situação.

Sem prejuízo da possibilidade de dispensa da coima, as entidades públicas continuarão sujeitas aos poderes de correção da CNPD. Assim, em caso de infração, serão obrigadas a comunicar à CNPD e, nos casos de elevado risco, aos cidadãos e a adotar as medidas necessárias a corrigir (se possível) e evitar futuras infrações.

Uma violação de dados pessoais poderá gerar responsabilidade civil da Administração pública. Um cidadão que tenha sofrido danos devido ao tratamento ilícito de dados pessoais pela Administração pública, tem o direito de exigir uma indemnização à entidade pública infratora.

Uma violação de dados pessoais poderá ainda causar elevados danos reputacionais à entidade pública e ter repercussões gravosas na sua esfera jurídica, que não ficará a coberto de um possível regime de isenção de aplicação de coimas.

MEDIDAS A IMPLEMENTAR

1. Designar o DPO. Selecionar a pessoa com um perfil adequado, sobretudo quando se trate de escolher um colaborador interno, que acumule outras funções, o que poderá não ser fácil. O DPO não é responsável por implementar o RGPD sozinho, mas por acompanhar a sua implementação.

2. Criar um grupo de trabalho multidisciplinar (com uma vertente jurídica, de recursos humanos, arquivo e informática). Este grupo de trabalho deve ser coordenado pelo DPO e participar, de forma regular, em ações de formação e sensibilização, principalmente para os colaboradores envolvidos no tratamento.

3. Realizar um diagnóstico e levantamento das operações de tratamento. Este levantamento deve ser feito por departamento/unidade orgânica, atendendo às categorias de dados pessoais, finalidades de tratamento, titulares dos dados e destinatários, comunicação a terceiros, prazos de conservação, etc., por forma a permitir um mapeamento dos fluxos de dados pela entidade pública.

4. Rever os fundamentos de licitude do tratamento, bem como políticas, procedimentos internos, contratos. Confirmar que tratamentos são necessários ao exercício de funções de interesse público ou dos poderes de autoridade pública e a aplicação de outros fundamentos (consentimento, contrato) e estar apto a comprová-lo. Acautelar as novas exigências, em particular ao nível dos acrescidos deveres de informação, dos contratos com subcontratados, do exercício de direitos pelos cidadãos e articulação do RGPD com a legislação de acesso aos documentos administrativos (LADA).

5. Implementar um registo das atividades de tratamento. Este registo é obrigatório se o tratamento implicar um risco para os direitos e liberdades dos cidadãos e não for ocasional ou disser respeito a categorias especiais de dados, e.g., dados de saúde ou biométricos.

6. Avaliar e rever a adequação dos sistemas de gestão e de segurança da informação. Instituir um processo para testar e avaliar a eficácia das medidas técnicas e organizativas, por forma a garantir a segurança do tratamento. Deve ser acautelado um plano de contingência em caso de violação de segurança com medidas de eliminação/mitigação de riscos, procedimentos, comunicação à CNPD e informação aos visados.

7. Assegurar formação aos colaboradores.

MACEDO▪VITORINO

SOBRE A MACEDO VITORINO

QUEM SOMOS & O QUE FAZEMOS

QUEM SOMOS

A MACEDO VITORINO foi fundada em 1996, centrando a sua atividade na assessoria a clientes nacionais e estrangeiros em sectores específicos de atividade, de que destacamos o sector financeiro, as telecomunicações, a energia e as infraestruturas.

Desde a sua constituição, a MACEDO VITORINO estabeleceu relações estreitas de correspondência e de parceria com algumas das mais prestigiadas sociedades de advogados internacionais da Europa e dos Estados Unidos, o que nos permite prestar aconselhamento em operações internacionais de forma eficaz.

As nossa atuação é citada pelos diretórios internacionais, Legal 500, IFLR 1000 e Chambers and Partners, nomeadamente nas áreas de Direito Bancário & Financeiro, Societário e «M&A»,, Mercado de Capitais, Direito Fiscal, Projetos e Contencioso.

A nossa prática é multifacetada. Assessoramos algumas das maiores empresas nacionais e internacionais em diversos sectores de atividade comercial e industrial, assumindo especial relevância, a banca, a indústria, as telecomunicações, capital de risco e a tecnologia.

A MACEDO VITORINO representa:

- EMPRESAS NACIONAIS E MULTINACIONAIS
- BANCOS E INSTITUIÇÕES FINANCEIRAS
- FUNDOS DE INVESTIMENTO
- SOCIEDADES DE INVESTIMENTO E FUNDOS DE «PRIVATE EQUITY»
- ASSOCIAÇÕES EMPRESARIAIS, CIENTÍFICAS E ACADÉMICAS
- EMBAIXADAS E GOVERNOS
- EMPRESÁRIOS INDIVIDUAIS
- CLIENTES PRIVADOS

MACEDOVITORINO•COM