REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Impacto na Administração Pública

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

Introdução

Aproximadamente seis meses após a aplicação do Regulamento Geral de Proteção de Dados (RGPD), o setor público apresenta ainda um atraso significativo na sua implementação. O RGPD impõe novos desafios à Administração pública em matéria de proteção de dados que parecem estar a ser ignorados.

A «moratória» de três anos aplicável à Administração pública quanto a coimas, prevista na proposta de lei de execução do RGPD, contribuiu para desincentivar o esforço de muitas entidades públicas na implementação do RGPD.

Há também uma «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.

Contudo, frustrando as ilusões de muitos, 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.

Embora o RGPD permita aos Estados-membros determinar se as coimas devem ou não ser aplicadas a autoridades e organismos públicos, na ausência dessa lei nacional o RGPD é plenamente aplicável, pelo que a Administração pública não está isenta da aplicação de sanções pela CNPD.

A manter-se a redação da proposta de lei que se encontra em discussão, apenas as empresas públicas que sejam entidades públicas empresarias (EPE) seriam abrangidas pela isenção. Tal pode significar que a coima ao Hospital do Barreiro poderá vir a ser retirada mas isso não é certo ainda.

Certo é que, com ou sem isenção, 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 e porque, mais tarde ou mais cedo, haverá sanções para evitar a violação do RGPD.

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 terá de adequar as suas políticas de privacidade e rever procedimentos internos para dar resposta aos reforçados direitos dos cidadãos.

O RGPD vem alterar a forma como a Administração pública deverá 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 da 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 deverá 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, por exemplo, 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 terá 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 terá de 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 deve ser consolidada num único documento (e.g. em folha Excel) e poderá ter de ser disponibilizado 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, 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, terá de se assegurar que são respeitados 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 entre a entidade pública e o subcontratado, podendo fazer parte do clausulado do próprio contrato de prestação de serviços (ou outro, que defina o objeto da relação) ou constar de um documento autónomo, por exemplo, em um anexo ao contrato 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;
- Que o pessoal do subcontratado 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 terá de 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, num prazo de 18 meses, até 1 de outubro de 2019.

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, 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 resulta 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. Se o esforço de comunicação for desproporcionado deve ser feita uma comunicação pública.

Designação e funções do 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.

A este respeito, coloca-se a questão de saber se as empresas do setor empresarial do Estado (SEE) se incluem no conceito de «autoridade pública» do RGPD e ficam, por essa via, obrigadas a designar um DPO.

A proposta de lei, que visa a execução de algumas medidas do RGPD, fornece-nos algumas pistas ao equiparar as empresas do SEE, que não sigam uma forma jurídico-pública – ou seja, as que não são entidades públicas empresariais (EPEs) – às entidades privadas. Nestes casos, apenas ficam obrigadas a ter um DPO quando tenham por principal atividade o controlo sistemático e regular de titulares de dados em grande escala ou o tratamento de categorias especiais de dados em grande escala.

Não se sabe, no entanto, se a versão final, que vier a ser aprovada, manterá esta interpretação.

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 será 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 isenta 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 proposta de lei, que visa assegurar a execução do RGPD, ainda em discussão, prevê a não aplicação de coimas às entidades públicas nos primeiros três anos e sujeito a posterior reavaliação.

Não se sabe, no entanto, se a versão final, que vier a ser aprovada, manterá esta isenção e ainda que o faça, o certo é que nem todas as entidades públicas serão por ela abrangidas. Por exemplo, no SEE, a manter-se a redação da proposta de lei, apenas as empresas públicas que sejam EPE ficariam isentas de coimas.

Sem que a proposta de lei tenha ainda sido aprovada, o RGPD é aplicável, e as entidades públicas ficarão sujeitas a coimas, como no caso do Centro Hospitalar do Barreiro Montijo, EPE. A CNPD aplicou a esta entidade pública uma coima de 400 mil euros por acesso indevido a dados clínicos por profissionais não médicos.

Como ficará a coima se a isenção for para a frente? Será retirada? Manter-se-á, uma vez que, quando foi aplicada, não se previa a isenção?

Dúvidas subsistem, mas uma certeza existe: 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 ainda 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 pode 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, poderá não ser fácil. O DPO não é responsável por implementar o RGPD sozinho, mas por acompanhar a sua implementação, o que deverá ser feito desde o início.

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 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, os 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 a licitude do tratamento. Confirmar que tratamentos são necessários ao exercício de funções de interesse público ou de autoridade pública e a aplicação de outros fundamentos (consentimento, contrato) e estar apto a comprová-lo.

5. Rever políticas e procedimentos internos, contratos. Esta revisão é necessária para acautelar as novas exigências, em particular ao nível do consentimento, 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).

6. 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, biométricos.

7. Avaliar e rever a adequação dos sistemas de gestão e de segurança da informação. Os requisitos técnicos mínimos das redes e sistemas de informação da resolução do Conselho de Ministros n.º 41/2018 devem ser implementados até 1 de outubro de 2019. Deve ser instituído um processo para testar, apreciar e avaliar periodicamente a eficácia das medidas técnicas e organizativas, de forma a garantir a segurança do tratamento. Deve ainda ser acautelado um plano de contingência em caso de violação de segurança que defina as medidas de eliminação/mitigação de riscos, procedimentos a adotar, comunicação à CNPD e informação aos titulares dos dados.

QUEM SOMOS

A Nossa Prática em Proteção de Dados

Quem somos

A Macedo Vitorino & Associados 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 & Associados 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.

Somos citados na maior parte das áreas de trabalho analisadas pelo diretório internacional, The European Legal 500, nomeadamente em "Banking and Finance", "Capital Markets", "Public Law", "Corporate", "Tax", "Telecoms" e "Litigation".

A atuação da Macedo Vitorino & Associados é ainda destacada pela IFLR 1000 em "Project Finance", "Corporate Finance" e "Mergers and Acquisitions" e pela Chambers and Partners em "Banking & Finance", "Corporate and M&A", "Tax" e "TMT".

Assessoramos os nossos clientes em todas as questões relativas a proteção de dados e privacidade, incluindo:

- Realizar auditorias em matéria de proteção de dados pessoais;
- Preparar e apresentar notificações e pedidos de autorização junto da Comissão Nacional de Proteção de Dados, programas de «compliance», elaborar e rever políticas de privacidade, políticas de cookies;
- Elaborar e rever contratos e cláusulas específicas relativas a proteção de dados pessoais, incluindo contratos de subcontratação, software e licenciamento, e rever soluções tecnológicas, incluindo sistemas de «cloud» e de geolocalização;
- Prestar assessoria a operações de transferências internacionais de dados;
- Dar formação em matéria de proteção de dados pessoais;
- Assegurar o cumprimento legal de normas de proteção de dados em sectores específicos, como bancário e financeiro, saúde, telecomunicações e media, tecnologia de informação e comércio eletrónico.

Se quiser saber mais sobre a Macedo Vitorino & Associados por favor visite o nosso website www.macedovitorino.com ou contacte-nos para mva@macedovitorino.com.

Cláudia Fernandes Martins
cmartins@macedovitorino.com

Rua do Alecrim 26E | 1200-018 Lisboa | Portugal
Tel.: (351)21 324 19 00 | Fax: (351)21 324 19 29
www.macedovitorino.com