NOTA INFORMATIVA 1/2018 SJ

PROTEÇÃO DE DADOS – O NOVO DESAFIO DAS AUTARQUIAS LOCAIS

O Regulamento Geral sobre a Proteção de Dados (Reg.º 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27.04.2016), veio definir o novo regime jurídico da proteção das pessoas singulares no que respeita ao tratamento e à livre circulação dos dados pessoais (artigo 1.º).

Com entrada em vigor e aplicação direta nos Estados Membros da União Europeia, incluindo Portugal, a partir de 25.05.2018, este Regulamento introduz uma disciplina jurídica exigente que altera o paradigma até aqui vigente, com particular impacto e efeitos práticos (passados, presentes e futuros) na Administração Pública.

Apresentam-se, de seguida, 12 FAQ's acerca do novo Regulamento Geral sobre a Proteção de Dados (RGPD) e ainda uma síntese das medidas a adoptar para a sua implementação.

1. Onde se aplica o novo RGPD?

Em todo o território da União Europeia (artigo 3.º).

2. A quem se aplica o RGPD?

O Regulamento aplica-se a todas as entidades que tratem dados pessoais (quer às entidades responsáveis pelo tratamento, quer aos subcontratantes que realizem operações que envolvam dados pessoais).

3. O que são Dados Pessoais para efeitos do RGPD?

Toda a informação relativa a pessoa singular identificada ou identificável (é identificável a pessoa singular que possa ser identificada, direta ou indiretamente, por recurso a um nome, um n.º de identificação, dados de localização, identificadores eletrónicos, genéticos, económicos, social…) - (artigo 4.º, n.º 1)

> *Exemplos de dados pessoais: Nome, morada, endereço eletrónico, número de IP, dados de localização, data de nascimento, número de identificação civil, número de identificação fiscal, número de identificação da Segurança Social, altura, peso e idade, composição do agregado familiar, padrão da íris e impressão digital, elementos de identidade física, fisiológica, genética, mental, económica, cultural ou social, perfis de Redes Sociais e informação recolhida por cookies, informação bancária, informação fiscal.*
>
> *Existem dados pessoais que estão enquadrados em categoriais especiais por revelarem informação do foro íntimo e alusiva à vida privada dos cidadãos: origem racial/étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados relativos à saúde, vida e orientação sexual ou vida privada, dados de crédito e solvabilidade, condenações penais e infrações. O tratamento destes dados especiais é proibido, com excepção dos casos em que está permitido o seu tratamento (artigo 9.º, n.º 2 do RGPD).*

Os dados pessoais podem ser divididos em diretos e indiretos.
Dados pessoais diretos: os que permitem, por si só, identificar de forma imediata o titular. Ex: nome ou fotografia.
Dados pessoais indiretos: os que apenas permitem identificar uma pessoa se forem complementados com outro(s) dado(s) ou informações(s) sobre o titular. Ex: N.º do Cartão de Cidadão - por si só, este dado não permite identificar o sujeito, mas se for consultado o Registo Civil, já é possível obter essa identificação.

4. Em que consiste o Tratamento de Dados Pessoais?

Consiste na operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição - (artigo 4.º, n.º 2).

5. Quando é que se considera lícito o Tratamento de Dados?

O tratamento é lícito quando (artigo 4.º, n.º 6):
a) houver consentimento do titular dos dados para uma ou mais finalidades específicas;
b) for necessário para a execução de um contrato no qual o titular dos dados é parte ou para diligências pré-contratuais a pedido do titular dos dados;
c) for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
d) for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

6. Para efeitos do RGPD, o que é o Consentimento?

Consiste na manifestação de vontade (declaração ou ação positiva) que, de forma livre, específica, informada e explícita, aceita que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. O consentimento tácito é considerado inválido - (artigo 4.º, n.º 11)

7. Que direitos são consagrados ao titular de dados?

O RGPD consagra vários direitos para o titular de dados (artigos 12.º e seguintes). Entre eles:

a) o direito à transparência - direito de saber que tratamentos são efetuados sobre os seus dados.

Ex: no caso de estarem a ser recolhidas imagens e som (ou poderem vir a sê-lo) deverá existir informação visível que informe os titulares sobre a realização das gravações.

b) o direito à informação - direito de solicitar ao responsável pelo tratamento dos dados, informações sobre o tipo de tratamento a que os seus dados estão a ser sujeitos.

Ex: no momento da recolha dos dados, o titular deve ser informado sobre o tratamento de que os mesmos serão alvo.

c) direito de acesso - o titular tem o direito de saber se os seus dados são ou não objeto de tratamento por parte de uma organização. Caso sejam alvo de tratamento, o titular tem o direito a aceder aos seus dados pessoais e às seguintes informações: finalidade do tratamento; categorias dos dados pessoais em questão; destinatários a quem os dados são, foram ou serão divulgados; prazo de conservação de dados; garantias de conhecimento e tratamento adequado sempre que os dados forem transferidos para país terceiro ou organização internacional; acesso a uma cópia dos dados pessoais em fase de tratamento.

d) direito de retificação – direito de solicitar a retificação de dados incorretos e preenchimento de dados incompletos.

e) direito ao apagamento – "direito ao esquecimento", isto é, de solicitar o apagamento dos dados, o que deverá decorrer sem demora injustificada.

f) direito à limitação do tratamento – direito a opor-se ao apagamento dos seus dados pessoais e solicitar a limitação do seu tratamento (inserção de uma marca nos dados pessoais conservados para limitar o seu tratamento no futuro).

g) direito de oposição – direito de se opor à utilização dos seus dados para efeitos de comercialização direta.

h) direito à notificação – os titulares dos dados devem ser notificados ou ser-lhes dado conhecimento nos casos em que os seus dados pessoais estejam a ser recolhidos ou tratados.

Ex: os colaboradores de uma empresa têm o direito de ser informados sobre as situações em que existe algum tipo de monitorização de equipamentos de trabalho ou geo-localização.

i) direito à não sujeição a decisões automatizadas – direito de solicitar intervenção humana em processos habitualmente automáticos.

j) direito à portabilidade – direito a que os dados sejam transferidos para outra empresa/entidade (à semelhança do que acontece com as operadoras de telecomunicações).

8. Quando é que é obrigatório o apagamento dos dados?

O apagamento dos dados (artigo 17.º) é obrigatório quando o titular o solicite e ainda nas seguintes situações: quando os dados deixam de ser necessários para a finalidade que motivou a sua recolha ou tratamento, quando o titular retira o consentimento para o tratamento (desde que não exista outro fundamento para esse tratamento), quando o titular se opõe ao tratamento e não existem interesses legítimos prevalecentes que justifiquem esse tratamento, quando os dados foram tratados ilicitamente, quando seja necessário dar cumprimento a uma obrigação jurídica decorrente do direito da União Europeia ou de um Estado Membro a que o responsável esteja sujeito ou quando os dados tenham sido recolhidos no contexto da oferta de serviços da sociedade da informação. Nota: o direito ao apagamento tem de ser conciliado com as obrigações jurídicas que o responsável pelo tratamento de dados deve assegurar

relativamente às entidades oficiais, que nesse caso se sobrepõem. Ex: o dever de manutenção de faturas emitidas.

9. Como proceder em caso de violação de Dados Pessoais?

O responsável pelo tratamento notifica a autoridade de controlo competente da violação de dados pessoais até 72 horas após ter tido conhecimento da mesma (artigo 33.º). Se este prazo não for cumprido, a notificação à autoridade de controlo deve ser acompanhada dos motivos do atraso. O subcontratante deve notificar o responsável pelo tratamento sem demora injustificada, após ter conhecimento de uma violação de dados pessoais. Quaisquer violações de dados pessoais devem ser documentadas, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Sempre que a violação dos dados pessoais for suscetível de implicar um elevado risco para os titulares dos dados, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada, descrevendo em linguagem clara e simples a natureza da violação dos dados pessoais e fornecendo as informações e recomendações previstas no Regulamento.

10. O RGPD consagrou regras quanto à Segurança dos Dados Pessoais?

O Regulamento obriga a que o responsável pelo tratamento e o subcontratante apliquem medidas técnicas e organizativas para assegurar um nível de segurança adequado (artigo 32.º), nomeadamente: pseudonimização, cifragem de dados, garantia de confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas…

11. Quais as responsabilidades/obrigações previstas no RGPD para os subcontratantes?

Os subcontratantes podem ser diretamente responsabilizados pelo tratamento em subcontratação, conforme o que estiver regulado no contrato que vincule o subcontratante ao responsável pelo tratamento. Os subcontratantes deverão apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento satisfaça os requisitos do Regulamento (artigo 28.º).

12. É obrigatório ter registos das atividades de tratamento?

Passa a ser obrigatório que cada responsável pelo tratamento e subcontratante conserve um registo de todas as atividades de tratamento sob a sua responsabilidade, do qual deverão constar um conjunto específico de informações devidamente definido no Regulamento (artigo 30.º). A Autoridade de Controlo poderá solicitar a disponibilização desses registos para verificação.

O RGPD NA PERSPECTIVA INTERNA DO MUNICÍPIO

Medidas a adotar para implementação do RGPD

1. Inventário e caracterização dos dados pessoais	Elencar os dados pessoais existentes na organização (quais são, a quem são transmitidos, quem tem acesso, onde se encontram, qual a finalidade do seu tratamento e o período de tempo durante o qual serão conservados).
2. Documentação e registo de atividades de tratamento de dados pessoais	Os responsáveis pelo tratamento e os subcontratantes devem organizar e manter um registo de todos os tratamentos de dados que executem (por isso, é imprescindível efetuar um levantamento integrado do estado atual dos processos de tratamento de dados pessoais).
3. Revisão da informação prestada aos titulares dos dados pessoais	A organização deve rever a informação que fornece aos titulares dos dados, independentemente do suporte (por escrito ou por telefone) ou do meio (diretamente junto do titular ou não), uma vez que o RGPD obriga os responsáveis pelo tratamento a prestar mais informações do que aquelas que são exigidas atualmente. A informação seja fornecida aos titulares dos dados de forma concisa, transparente, inteligível e de fácil acesso, com linguagem clara e simples.
4. Exercício dos direitos dos titulares dos dados pessoais	A organização deve rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, inclusivamente o modo de eliminação dos dados pessoais e o acesso a dados pessoais por via eletrónica e num formato de utilização comum. Deverá, também, ser assegurada a manutenção da informação num formato estruturado e de uso corrente, bem como procedimentos eficazes de comunicação com as entidades terceiras a quem são transmitidos dados, de forma a assegurar o efetivo exercício dos direitos dos titulares dos dados. A organização deve ainda atualizar os procedimentos a adotar no caso de haver pedidos dos titulares de dados pessoais ao abrigo das novas regras (ter presente o prazo para fornecimento de informações, a gratuitidade da resposta aos pedidos, a fundamentação das decisões de indeferimento do pedido e a informação relativamente à possibilidade de apresentar reclamação à CNPD e intentar ação judicial).
Pedidos apresentados pelos titulares dos dados pessoais	
5. Fundamento jurídico para o tratamento dos dados pessoais	A organização deverá identificar os fundamentos jurídicos para cada tratamento de dados, documentá-los, introduzi-los na política de privacidade e demonstrá-los nos pedidos apresentados pelos titulares dos dados.
Consentimento dos titulares dos dados pessoais	A organização deve verificar a forma e circunstâncias em que obteve o consentimento dos titulares para a recolha e tratamento de dados pessoais, quando este serve de fundamento jurídico para o tratamento. Como o RGPD alarga o conceito de consentimento e introduz condições mais exigentes, se o consentimento obtido não respeitar todos os novos requisitos, será necessário obter novo consentimento, sob pena de o tratamento ser ilícito por falta de fundamento jurídico. Nota: ter presente as regras específicas do RGPD para o consentimento de crianças e dos representantes legais.
6. Dados sensíveis	A organização deve proceder avaliar a natureza dos tratamentos de dados efetuados e apurar quais os que caem no conceito de dados sensíveis (abrange também os dados biométricos e genéticos) e aplicar condições específicas ao seu tratamento.

7. Proteção de dados pessoais desde a conceção e por defeito + Avaliação de Impacto	A organização deve proceder a uma avaliação rigorosa relativamente ao tipo de tratamentos de dados que tenha projetado realizar, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito. A avaliação de impacto é obrigatória sempre que um certo tipo de tratamento de dados seja suscetível de implicar um elevado risco para os direitos e liberdades dos titulares. Se a avaliação de impacto revelar que o tratamento de dados resultaria em elevados riscos e não haja mecanismos para mitigar adequadamente estes riscos, a organização deverá consultar a CNPD com vista a apurar se o referido tratamento cumpre ou não com os requisitos previstos no RGPD.
8. Contratos de subcontratação	A organização deve definir princípios para a contratação de parceiros externos que procedem ao tratamento de dados pessoais (subcontratantes). Devem ser revistos os instrumentos contratuais existentes. Os subcontratantes deverão apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas, de modo a que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos do titular dos dados.
9. Encarregado da proteção de dados pessoais – Data Protection Officer (DPO)	O DPO é uma das mais importantes inovações introduzidas pelo RGPD e poderá desempenhar um papel fulcral no período de transição, cabendo-lhe a responsabilidade de implementar e garantir que a organização cumpre todos os requisitos legais desde o início da aplicação do RGPD.
10. Segurança	A organização deve rever as políticas e adotar medidas técnicas adequadas para assegurar e comprovar que os tratamentos de dados se encontram em conformidade com o RGPD a partir de 25 de Maio de 2018.
11. Notificação de violações de dados pessoais	Devem ser adotados procedimentos internos de forma a tornar a organização apta para gerir casos de violações de dados pessoais, tais como a deteção, identificação e investigação das circunstâncias em que possam ocorrer violações e preparação de medidas mitigadoras e circuitos de informação entre responsável e subcontratante. As violações devem ser objeto de documentação. As violações suscetíveis de resultar num risco para os direitos dos titulares devem ser comunicadas à CNPD, no prazo de 72 horas após o seu conhecimento, e ao titular dos dados sempre que aquele risco seja elevado.
12. Transferências de dados pessoais para países terceiros ou organizações internacionais	A organização deve assegurar que existe fundamento legítimo para transferir dados pessoais para jurisdições que não sejam objeto de uma decisão de adequação.
13. Autoridade de controlo principal (One Stop Shop)	Se a organização em causa desenvolver a sua atividade em mais que um Estado Membro da União Europeia, a autoridade de controlo do estabelecimento principal do responsável pelo tratamento é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado.
14. Coimas	Em caso de violação das suas disposições, o RGPD introduz um quadro sancionatório que, na sua expressão máxima, pode atingir os € 20.000.000,00 ou 4% do volume de negócios global tendo como referência o exercício financeiro anterior, conforme o montante que seja mais elevado.

Nota: a presente nota informativa foi elaborada de forma geral e abstrata, não dispensando a leitura do RGPD.

Alguns cuidados práticos a adotar pelos colaboradores

- Não deixar as senhas de acesso anotadas em papéis sobre a mesa;
- Não compartilhar a senha com colegas;
- Não utilizar uma única palavra passe em diferentes sites e serviços;
- Escolher palavras passes menos óbvias;
- Alterar as senhas, pelo menos, duas vezes por ano;
- Se verificar que possui informação que não lhe diz respeito, comunique imediatamente ao departamento informático;
- Proteger os documentos *word* e *excel* importantes com password de abertura, caso a informação seja confidencial;
- Nunca permitir que as palavras passe sejam memorizadas no acesso recorrente a um serviço ou aplicação;
- Não deixar em cima da mesa e à vista, documentos com informação pessoal de caráter reservado (devem ser cuidadosamente guardados, para evitar a sua utilização indevida por terceiros);
- Guardar sigilo e abster-se de usar informações de carácter confidencial obtidas no desempenho das suas funções ou em virtude desse desempenho (dados informáticos de âmbito pessoal ou outros considerados confidenciais);
- Não utilizar dados pessoais para fins ilegítimos;
- Não comunicar dados pessoais a pessoas não autorizadas ao respetivo acesso ou tratamento;
- Não deixar os computadores sem proteção quando nos ausentamos da sala;
- Procurar, na medida do possível, salvaguardar a privacidade dos munícipes/colaboradores quando estão a ser atendidos (BUM/RH).