REGULAMENTO GERAL DE PROTECÇÃO DE DADOS

O QUE HÁ DE NOVO?

REGULAMENTO (EU) 679/2016, DE 27 DE ABRIL, DO PARLAMENTO EUROPEU E DO CONSELHO

No passado dia 25 de Maio de 2016, entrou em vigor o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016 (doravante o "**Regulamento**"), relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

DATA DE ENTRADA EM VIGOR

Pese embora tenha entrado em vigor já em Maio de 2016, o Regulamento apenas terá **aplicação obrigatória geral a partir do dia 25 de Maio de 2018** no ordenamento jurídico de todos os Estados membros.

APLICAÇÃO DIRECTA A PARTIR DE 25 DE MAIO DE 2018

Sendo um Regulamento, e não uma Directiva, **tem aplicação directa na ordem jurídica interna de todos os Estados membros**, sem necessidade de transposição. Significa isto que, a partir do dia 25 de Maio de 2018, todas as entidades públicas e privadas dentro da União Europeia (e mesmo as que estejam fora, mas que tratem dados pessoais de cidadãos europeus), estão vinculados ao cumprimento desta nova normativa

Ainda que nem tudo seja totalmente novo, o Regulamento impõe, ainda assim, novas regras e obrigações às organizações privadas e públicas, que farão com que as matérias de Protecção de Dados passem a ser levadas em conta, necessariamente, na sua gestão.

AUMENTO SUBSTANCIAL DAS COIMAS POR INCUMPRIMENTO

A liderar as novidades preconizadas pelo Regulamento está **o aumento substancial das coimas por incumprimento**: estão previstas coimas que podem ascender a € 20.000.000,00 ou a 4% da facturação anual. Caso se verifique, como é desejável, um maior investimento público nas actividades de fiscalização sobre esta matéria, as questões de privacidade deverão passar a ser uma prioridade na gestão de qualquer entidade, pública ou privada.

CRIAÇÃO DA FIGURA DO ENCARREGADO DE

Outra das novidades do Regulamento é a **criação da figura do Encarregado de Protecção de Dados** (ou, na sigla inglesa, *DPO – Data*

PROTECÇÃO DE DADOS

QUEM ESTÁ OBRIGADO A DESIGNAR UM *DPO*

Protection Officer). A nomeação do *DPO* será obrigatória para:

- As autoridades e organismos públicos;
- Entidades que procedam a tratamentos em larga escala de dados sensíveis (ex.: hospitais, seguradoras, empresas que prestem serviços na área da saúde, aeroportos, etc.);
- Entidades que efectuem tratamento de dados pessoais, também em larga escala, que exijam um controlo regular e sistemáticos dos dados (ex.: bancos, operadoras de telecomunicações, grandes retalhistas, etc.).

FUNÇÕES DO *DPO*

O *DPO* terá como principais funções:

a) Aconselhamento e monitorização do *compliance* com as Regras de Proecção de Dados e do Regulamento;
b) Formação e sensibilização para matérias de protecção de dados pessoais;
c) Realização de auditorias;
d) Aconselhamento em avaliações de impacto sobre protecção de dados;
e) Colaboração com as autoridades de protecção de dados;
f) Relacionamento com os titulares dos dados, nomeadamente no âmbito do exercício dos seus direitos.

DEVER DE *ACCOUNTABILITY*

No âmbito do dever de *accountability,* surge uma nova obrigação a cargo de todas as entidades, que consiste em **proceder ao registo de tratamento de dados pessoais**. O responsável pelo tratamento deve poder comprovar que o tratamento é realizado em conformidade com o Regulamento, na eventualidade de ser fiscalizado nesse sentido. O Regulamento estabelece ainda os elementos mínimos que devem ser incluídos nesse registo.

AVALIAÇÃO DE IMPACTO

Uma avaliação de impacto consiste, em traços gerais, numa avaliação levada a cabo pelo responsável pelo tratamento – aqui recorrendo normalmente ao seu *DPO* – para **identificar e minimizar os riscos por incumprimento das regras de protecção de dados**. No entanto, apenas as entidades que efectuem tratamento automatizado de dados, incluindo *profiling*, que levem a decisões que afectem o titular dos dados, que

ALTERAÇÃO DOS PODERES DAS ENTIDADES FISCALIZADORAS – DO CONTROLO PRÉVIO À FISCALIZAÇÃO EFECTIVA

façam operações de tratamento em larga escala de dados sensíveis ou que efectuem um controlo sistemáticos de zonas acessíveis ao público em grande escala estão obrigadas a realizar avaliações de impacto periódicas.

A introdução de avaliações de impacto decorre, em parte, do facto das autoridades fiscalizadoras, e designadamente a Comissão Nacional de Protecção de Dados, com a entrada em vigor do Regulamento, deixar de possuir poderes de autorização ou de controlo prévios à utilização dos dados. Ou seja, doravante, **passarão a ser as entidades as responsáveis por garantir a conformidade do tratamento dos dados a que tenham acesso de acordo e conforme o Regulamento**. As entidades fiscalizadoras adoptarão um papel puramente fiscalizador, actuando seja por denúncia seja por via de acções concertadas em determinados sectores de actividade.

SEGURANÇA E NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

A segurança dos dados apresenta-se como factor essencial ao cumprimento do Regulamento. As entidades devem adoptar "*medidas técnicas e organizativas adequadas*" para assegurar a protecção dos dados a que tenham acesso, garantindo sempre, e em última análise, que os mesmos não são utilizados para fins diversos para os quais foram recolhidos.

Havendo conhecimento de uma violação nesta matéria, o responsável pelo tratamento – que são as entidades – terá a seu cargo, na maioria dos casos, uma obrigação de notificação à autoridade de protecção de dados.

CONSENTIMENTO

O consentimento continua a ser um dos fundamentos para a legitimidade do tratamento de dados pessoais, mas agora com regras mais exigentes quanto à sua obtenção. A partir da entrada em vigor do Regulamento, **deixarão de ser permitidos os consentimentos feitos através de *opt-out***, ou seja, por via do silêncio, das opções pré-validadas ou da omissão. O Regulamento exige agora que todos os consentimentos sejam feitos através de um acto positivo expresso e inequívoco, utilizando linguagem clara e simples, que não deixe quaisquer dúvidas quanto ao conhecimento dos fins previstos e à intenção do titular dos dados.

Outra das novidades do Regulamento em matéria de consentimento prende-se com a **revogação do consentimento**: esta deve ser tão fácil de concretizar como a obtenção do consentimento em si.

Da mesma forma, caso um consentimento seja dado para fins múltiplos, deverá ser dado consentimento expresso e informado para todos esses fins.

DIREITOS DOS TITULARES

O Regulamento vem adicionar ao catálogo dos direitos dos titulares dos dados pessoais novos direitos, dos quais se destacam o direito ao apagamento dos dados (ou direito ao esquecimento) e o direito à portabilidade dos dados.

DIREITO AO ESQUECIMENTO

No caso do **direito ao esquecimento**, é agora permitido ao titular dos dados a solicitação ao responsável pelo tratamento o apagamento dos seus dados. O responsável pelo tratamento, mediante esta solicitação, fica obrigado ao seu apagamento, salvo se existir alguma obrigação legal à sua conservação. De referir, ainda, que a anonimização dos dados não substitui o direito ao esquecimento.

DIREITO À PORTABILIDADE

O **direito à portabilidade** confere aos titulares o direito a solicitarem ao responsável pelo tratamento dos dados o seu carregamento ou mesmo a sua transferência num formato de uso comum para que o titular possa usá-los com outra entidade.

Mantém-se ainda, especialmente reforçados todos os demais direitos já antes em vigor, como sejam, por exemplo, o direito de acesso e de rectificação.

RESPONSÁVEIS PELO TRATAMENTO E SUBCONTRATANTES

As personagens principais que compõem a temática da Protecção de Dados mantém-se: titular dos dados, responsável pelo seu tratamento e subcontratantes. No entanto, **o Regulamento reforça agora as responsabilidades a cargo dos subcontratantes**, passando estes a ser, solidariamente com o responsável pelo tratamento, responsáveis por um eventual incumprimento ou violação, na medida da sua interferência.

PRIVACY BY DESIGN
PRIVACY BY DEFAULT

Como princípios orientadores, todas as entidades – sejam elas responsáveis pelo tratamento ou subcontratantes – devem ter presente os princípios do ***privacy by design*** **e** ***privacy by default***, ou seja:

- A privacidade dos dados deve ser tida em conta desde a génese da construção de todas as bases de dados; e
- O acesso e o tratamento a dados pessoais deve ser feito de forma legítima, transparente, e limitada aos propósitos para os quais a informação é recolhida.

Todas nossas Briefings podem ser consultadas em **www.vaassociados.com**

Para informação adicional, por favor contacte:
Duarte Vasconcelos - sócio responsável pelo Departamento de Direito Comercial
duarte.vasconcelos@vaassociados.com **ou** **geral@vaassociados.com**

Vasconcelos, Arruda & Associados – Sociedade de Advogados RL
NIF 510 122 507 - Rua Joshua Benoliel, n.º 6, 7-A - 1250 - 133 Lisboa
T: +351 218 299 340
E-mail: geral@vaassociados.com

www.vaassociados.com