REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS JÁ ENTROU EM VIGOR

O que regula?

O Regulamento UE 2016/679 introduz alterações significativas às atuais regras de Proteção de Dados (Diretiva 95/46/CE do Parlamento Europeu e do Conselho) com vista à sua simplificação e modernização, sendo diretamente aplicável a todos os estados membros da União Europeia, sem necessidade de qualquer transposição.

A partir de quando é aplicável às empresas?

A partir de **25 de Maio de 2018.**

E até lá?

Mantém-se em vigor a Lei 67/98 de 26 de Outubro, ou seja, continuará a ser necessário, nomeadamente, efetuar as notificações à Comissão Nacional de Proteção de Dados (CNPD). No entanto, todas as empresas deverão tomar as medidas organizativas necessárias para se adaptarem às novas obrigações impostas pelo Regulamento.

Daremos conta da concretização das normas de execução do presente Regulamento, à medida que as mesmas forem emitidas pelas agências nacionais, europeias e pelo Comité Europeu para a Proteção de Dados.

A quem se aplica?

A todas as empresas situadas em Portugal, ou em qualquer outro estado membro, que tratem dados pessoais (de clientes, recursos humanos, fornecedores, utilizadores, consumidores, etc.), bem como a todas as empresas situadas fora da União Europeia que processem dados pessoais de cidadãos europeus, nomeadamente através da oferta de bens e serviços.

Quais as principais obrigações impostas às empresas?

i. Manter, em certas circunstâncias, registos atualizados contendo a descrição dos ficheiros de dados pessoais que a empresa possui, incluindo dados processados, destinatários dos dados, finalidades, medidas de segurança, etc., os quais deverão estar disponíveis para consulta pela autoridade de controlo (o estado português deverá instituir uma autoridade independente, a nível nacional, para o controlo do cumprimento das normas do Regulamento);

ii. Demonstrar à autoridade de controlo, mediante solicitação desta, que a empresa cumpre as disposições do Regulamento no que respeita, nomeadamente, a medidas de segurança, conservação dos dados, consentimento dos titulares, etc.;

iii. Notificar a autoridade de controlo, no prazo máximo de 72 horas, de qualquer violação de dados pessoais (data breach) que implique um risco para os titulares dos dados;

iv. Nomear um Encarregado para a Proteção de Dados (externo ou interno), sempre que, em geral, o tratamento seja efetuado por uma autoridade ou organismo público ou quando as atividades principais do responsável pelo tratamento ou subcontratante se traduzam em operações de tratamento que exijam um controlo regular e sistemático dos dados em grande escala ou em operações de tratamento em grande escala de categorias especiais de dados (dados de saúde, dados de crédito, etc.) e de dados pessoais relacionados com condenações penais e infrações;

v. Entregar, a pedido do titular dos dados, uma cópia estruturada da informação mantida sobre ele (direito de portabilidade);

vi. Sempre que estejam em causa tratamentos de alto risco (lista exemplificativa a ser definida pelas autoridades competentes) deverão ser realizadas avaliações de impacto do tratamento de dados pessoais, cujo resultado poderá implicar a consulta prévia da autoridade de controlo;

vii. Prestar informações adicionais aos titulares dos dados acerca do tratamento a efetuar nomeadamente sobre o prazo de conservação, finalidades e direito a apresentar uma reclamação à autoridade de proteção de dados.

Quais as principais alterações face à anterior normativa?

i. O Regulamento aplicar-se-á a quaisquer empresas que ofereçam produtos ou prestem serviços a cidadãos europeus, independentemente de, como se verifica atualmente, possuírem sede, estabelecimento ou servidores na União Europeia;

ii. Deixará de existir a obrigatoriedade de notificar à CNPD todos os tratamentos de dados pessoais não isentos, pelo que quaisquer notificações/autorizações emitidas ou pendentes em 25 de Maio de 2018 deixarão de ter efeitos jurídicos. A partir dessa data e segundo o texto do Regulamento, será somente obrigatório notificar a autoridade de controlo da ocorrência de determinadas violações de dados pessoais;

iii. O montante máximo das coimas aplicáveis sofrerá um aumento muito significativo: passa dos cerca de 30 mil euros atuais para 20 milhões de euros ou 4% do volume de negócios anual da empresa;

iv. Foi introduzida a obrigatoriedade de avaliar previamente o impacto dos tratamentos de dados pessoais suscetíveis de afetar os direitos dos cidadãos (privacy impact assessement) e a necessidade, em determinadas circunstâncias, de nomear um encarregado para a proteção de dados (data protection officer), sendo que estas ações, embora constituam boas práticas atualmente, não tinham ainda sido objeto de imposição legal;

v. As empresas terão de lidar apenas com uma única autoridade de controlo em toda a UE (balção único) e não, como acontece presentemente, com todas as autoridades de proteção de dados em cujos países possuam um estabelecimento que trate dados pessoais para as suas próprias finalidades;

vi. Reforço dos direitos dos titulares dos dados: (i) maior rigor no tipo de informações a prestar ao titular de dados (para além dos dados relativos à identidade da empresa responsável pelo tratamento, finalidades, destinatários dos dados e direito de oposição/retificação, será também obrigatório informar o titular dos dados do prazo de conservação dos mesmos e do direito a apresentar uma reclamação à autoridade de controlo), (ii) introdução do direito a serem apagados os dados pessoais ("direito a ser esquecido") bem como do direito de portabilidade de dados já referido.

Quais as sancões por incumprimento?

As coimas poderão chegar a 4% da faturação anual global ou a €20.000.000,00.

Quais os aspetos com maior incidência a nível estritamente laboral?

i. Cada Estado-Membro, seja por meio de legislação ou através de instrumentos de regulamentação coletiva poderá prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que concerne às condições do tratamento dos dados pessoais em contexto laboral, com base no consentimento dos trabalhadores, para efeitos de recrutamento, execução do contrato de trabalho e cessação da relação laboral;

ii. A obrigação de conservação de registo escrito e eletrónico das atividades de tratamentos de dados pessoais previstas no Regulamento mencionado (e suas categorias e finalidades) não se aplicará às empresas ou organizações com menos de 250 trabalhadores, a não ser que o tratamento efetuado possa implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional, ou abranja as categorias especiais de dados (tais como origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, biométricos, saúde ou vida/orientação sexual);

iii. O encarregado da proteção de dados tem, entre o mais, a função de informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do Regulamento e de outras disposições legais aplicáveis.

Para aceder ao texto do Regulamento clique aqui.

MAIS INFORMAÇÃO:

JOÃO MIRANDA DE SOUSA
Managing Partner da Garrigues Portugal

Propriedade Industrial e Intelectual
Direito da Informação
joao.miranda@garrigues.com
T +351 213 821 200

JOÃO PAULO TEIXEIRA DE MATOS
Sócio

Direito Europeu e da Concorrência
Direito Laboral
joao.teixeira.matos@garrigues.com
T +351 213 821 200

Siga-nos:

www.garrigues.com