

Regulamento Geral de Proteção de Dados – RGPD

A MAIOR MUDANÇA NAS LEIS DE PROTEÇÃO DE DADOS DOS ÚLTIMOS 20 ANOS!

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais exigindo um quadro de proteção sólido e mais coerente na União Europeia.

Surge assim a necessidade de um Regulamento que introduz alterações importantes sobre a proteção das pessoas singulares relativamente ao tratamento de dados pessoais impondo novas obrigações aos cidadãos, empresas e outras organizações privadas e públicas.

A QUEM SE APLICA?

O Novo Regulamento aplica-se ao tratamento de dados pessoais das pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, e por meios total ou parcialmente automatizados, e também por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados e efetuado no contexto das atividades de um estabelecimento (organização ou empresa) de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

Assim qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento responsável pelo tratamento situado na União Europeia deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado ou não na União Europeia.

QUAIS AS SANÇÕES PELA VIOLAÇÃO?

Qualquer organização/empresa responsável pelo tratamento de dados responde pelos danos causados por um tratamento que viole o regulamento, sendo obrigado a indemnizar a pessoa que tenha sofrido danos materiais ou imateriais devido a essa violação.

Essa organização/ empresa que viole as regras do regulamento está também sujeita a aplicação de coimas pela respetiva autoridade de controlo, que podem ir em determinadas situações até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

O QUE DEVE FAZER?

Deve-se apoiar num parceiro capaz de o acompanhar ao longo de todo o processo estratégico de implementação do Regulamento, eliminando risco de incumprimento e eventuais coimas.

A inCentea é a primeira consultora nacional certificada em 4 normativos, um dos quais focado na segurança de informação, e possui o know-how necessário para ajudar a capacitar a sua empresa a dar resposta aos artigos impostos por este Regulamento.

QUANDO ENTRA EM VIGOR?

O regulamento é aplicável a partir de 25 de maio de 2018, sendo que os Estados-Membros adotam e publicam, até 6 de maio de 2018, as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à DIRETIVA (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

Os Estados-Membros terão assim de aplicar as referidas disposições da diretiva a partir de 6 de maio de 2018.





QUAIS SÃO OS ASPETOS MAIS RELEVANTES?

- Harmonização Legislativa passando a existir um único documento legal sobre Proteção de Dados Pessoais em todos os vinte e oito Estados Membros.
- Reconhecer aos cidadãos o "direito a ser esquecido" o "direito ao apagamento", o "direito à portabilidade dos dados", o "direito de oposição a Profiling", o "direito à limitação do tratamento" e o "direito de oposição".
- Obrigação de notificar violações de dados pessoais (data breaches) à Comissão Nacional de Proteção de Dados e ao titular dos dados.
- Aplicação do Regulamento aos controllers (entidades que controlam os dados) bem como ao processors (entidades que tratam os dados).
- Conceito de balcão único para organizações que tenham delegações em diferentes países da EU.
- Regras de especial tutela a menores.
- Ser necessário a realização de Privacy Impact Assessments (PIA).
- Criação da figura Data Protection Officer (DPO).
- Introdução de novas premissas no tratamento dos dados como proteção desde a conceção (privacy by design) e por defeito (Privacy by default) e a pseudonimização dos dados.
- A proteção das pessoas singulares deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas.
- Garantir a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais.
- Elaboração de códigos de conduta.
- Direito de apresentar reclamação a uma autoridade de controlo.
- Supressão do mecanismo de autorização prévia pela Comissão Nacional de Proteção de Dados (CNPd), passando esta entidade a ter um papel fiscalizador.