

REGULAMENTO PROTECÇÃO DE DADOS

O que altera a partir de 25 de maio de 2018?

As medidas e os procedimentos a tomar

Contagem decrescente para a sua aplicação 25 de maio de 2018

O Regulamento Geral de Proteção de Dados (RGPD) Regulamento (EU) de 27 de Abril de 2016 passará a ter aplicação nos respetivos estados membros da EU a partir de 25 de maio de 2018.

O Regulamento aplica-se a todas as entidades que tratem de dados pessoais, ou seja, que realizem operações que envolvam dados pessoais, sejam aquelas que determinam as finalidades e os meios de tratamento de dados pessoais, mas também as que efetuam essas operações em regime de subcontratação pelo que o regulamento implica que **as empresas deverão começar de imediato** a adaptar-se internamente para o cumprimento da nova legislação

Entendemos ser necessário conhecer as regras impostas e avaliar o impacto que a nova regulamentação vai ter no seio das empresas no seu dia a dia, incluindo relações com os trabalhadores, com clientes e com fornecedores.

Em contagem decrescente para a sua aplicação começarão hoje uma serie de publicações com orientações para as empresas.

Começaremos com um esclarecimento geral e, diariamente, detalharemos as várias situações concretas com esclarecimentos do grupo de trabalho da comissão.

Informações a prestar

Segundo o regulamento existe a obrigação de facultar um conjunto de informações quando os dados sejam recolhidos juntos dos titulares ou junto de terceiros (arts 13 e 14do REG)

O QUE SÃO DADOS PESSOAIS?

Consideram-se dados pessoais os tradicionais dados, como nome , morada telefone , telemóvel , documentos de identificação e ainda dados de localização (geolocalização) e identificadores por via eletrónica.

Para além disso, passa a existir uma definição do que é a "definição de perfis", "pseudonimização", "dados genéticos", "dados biométricos e "dados relativos à saúde".

Deve assim ser revista toda a informação que é fornecida quando se recolhe dados seja por escrito seja por telefone seja através da web.

A empresa tem ainda que informar o titular do dados da a) base legal para a recolha dos dados b) a sua finalidade c) identidade e os contatos do responsável pelo tratamento d) a licitude da recolha e) a identificação do responsável pela recolha f) o prazo de conservação dos dados g) direito de oposição ao tratamento h) direito de limitação do tratamento i) direito a portabilidade bem como j) informações mais detalhadas sobre as transferências internacionais de dados a possibilidade de apresentar queixa junto da CNPD.

Dentro das exigências de maior transparência, as informações devem ser prestadas aos cidadãos de forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples.

As informações quando são dirigidas a crianças deverão ser em linguagem acessível a crianças.

Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos

titulares das responsabilidades parentais da criança. Os Estados-Membros têm liberdade para legislar uma idade inferior para os efeitos referidos, **desde que não seja inferior a 13 anos, ou seja são proibidos dados recolhidos de crianças com menos de 13 anos** mesmo com autorização dos pais.

Há que fazer uma validação de todo o tipo de impressos, contratos, políticas de privacidade utilizados e que servem para recolha de dados e verificar se cumprem todos os requisitos exigidos nomeadamente os descritos nos artigos 13 e 14 do regulamento.

Exercício dos direitos dos titulares dos dados

O titular dos dados tem direito à sua portabilidade, o que implica que a entidade que recolhe os dados terá de assegurar que transmite ao titular num formato sistematizado os seus dados pessoais e que essa forma seja susceptível de ser transmitida a terceiros, existe ainda a possibilidade limitação do tratamento e o direito à oposição bem como novos requisitos quanto ao direito à eliminação dos dados e quanto à notificação de terceiros sobre retificação ou apagamento ou limitação de tratamento solicitados pelos titulares.

A informação recolhida deverá ser armazenada num formato estruturado, de uso corrente e de leitura automática, e de procedimentos eficazes de comunicação com as entidades terceiras a quem transmitiu os dados, de modo a assegurar o exercício efetivo dos direitos.

Deverão ser revistos todos os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados

Documentação e registo de atividades de tratamento

Deve documentar/registar de forma detalhada todas os procedimentos relacionados com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação legal de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

Esta ação reveste-se de especial relevo no contexto da preparação para a aplicação do novo regulamento, permitindo fazer o levantamento integrado do que está a ser feito, permitindo validar o que é necessário corrigir e adaptar.

Contratos de subcontratação

Devem ser revistos os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo regulamento.

O novo RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de um conjunto de informações. Muitos dos contratos existentes necessitarão de ser modificados para cumprir as normas do regulamento.

Quando houver lugar a sub-subcontratação, compete ao subcontratante verificar se detém as autorizações respetivas dos responsáveis pelo tratamento, exigidas expressamente pelo novo regulamento; caso contrário, deve obtê-las até 25 de maio de 2018.

Medidas técnicas e organizativas e segurança do tratamento

Dever rever as políticas e práticas da organização à luz das novas obrigações do regulamento, e adotar as medidas técnicas e organizativas adequadas e necessárias para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD a partir do momento da sua aplicação.

Nessa avaliação, deve ter em conta a natureza, âmbito, contexto e finalidades dos tratamentos de dados, bem como os riscos que deles podem decorrer para os direitos e liberdades dos cidadãos.

Esta apreciação permite ainda tomar as medidas necessárias para confirmar um nível de segurança do tratamento adequado, que garanta designadamente a confidencialidade e a integridade dos dados e que previna a destruição, perda e alterações acidentais ou ilícitas ou, ainda, a divulgação ou acesso não autorizados de dados.

Encarregado de proteção de dados

Deve preparar a designação do encarregado de proteção de dados com a antecedência devida. Em alguns casos o regulamento impõe a contratação de um encarregado de proteção de dados (designado o regulamento como DPO).

.Casos em que é necessário contratar um "Encarregado da Proteção de Dados" (Data Protection Officer).

Deve ser designado um Encarregado da Proteção de Dados sempre que:

- a) O tratamento for efetuado por uma autoridade ou um organismo público
- b) As atividades principais do responsável pelo tratamento ou do subcontratante

consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala ou

- c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados

O EPD (DPO) desempenhará um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento.

Proteção de dados desde a conceção e avaliação de impacto

Deve avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

Deverá decidir e adotar as medidas mais ajustadas, tendentes à pseudonimização, à minimização dos dados, ao cumprimento dos prazos de conservação da informação ou à acessibilidade dos dados.

Se o tipo de tratamento, nomeadamente quando utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for susceptível de implicar um elevado risco para os titulares dos dados, deve ser efectuada uma avaliação de impacto das operações de tratamento previstas sobre a protecção de dados pessoais.

A avaliação é obrigatória caso ocorram:

- a) Avaliações sistemáticas e completas dos aspectos pessoais, baseada no tratamento automatizado, incluindo a definição de perfis;
- b) Operações de tratamento em grande escala de categorias especiais de dados; ou,
- c) Controlos sistemáticos de zonas acessíveis ao público em grande escala,

Violações de segurança

O responsável pelo tratamento notifica a autoridade de controlo competente da violação de dados pessoais até 72 horas após ter tido conhecimento da mesma. 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 respectivos efeitos e a medida de reparação adoptada.

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. Direito ao Esquecimento.

Direito “a ser esquecido”

O Regulamento consagra o Direito ao Apagamento dos Dados (“direito a ser esquecido”), significando isto que o titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada



Margarida Almeida Santos

Senior Partner
margarida.santos@dlas.pt



**DLAS
INTERNACIONAL**

ANGOLA |
BRASIL |
CHINA |
ESPAÑA |
FRANÇA |

SÓCIOS

JOSÉ DINIS LUCAS
MARGARIDA ALMEIDA SANTOS

ASSOCIADOS

MÁRIO DINIS LUCAS
ALEXANDRE FRANCO BRUNO
CRISTIANA SOBREIRO
RITA MORGADO
SANDRA DE BRITO TAVARES
PATRÍCIA DE ALMEIDA PINHEIRO
RITA DINIS LUCAS
DIANA DE ALMEIDA FERREIRA



DINIS LUCAS & ALMEIDA SANTOS
SOCIEDADE DE ADVOGADOS SP, R.L. | BOUTIQUE LAW FIRM ®

Avenida da República, n.º 50 - 7ªA - 1050-196 Lisboa
Tel: +351 217 816 010 | Fax: +351 217 816 011
Email: geral@dlas.pt
www.dlas.com.pt

Esta Newsletter é meramente informativa. Para efeitos de emissão de parecer em matéria de enquadramento fiscal, será necessário o fornecimento/definição de outros elementos concretos. Caso deseje obter esclarecimentos adicionais sobre este assunto contacte Margarida Almeida Santos (margarida.santos@dlas.pt)