

Regulamento Geral sobre a Proteção de Dados

Linhas Gerais



O novo **Regulamento Geral sobre a Proteção de Dados**, constante do **Regulamento (UE) 2016/679**, foi publicado no Jornal Oficial da União Europeia no dia **4 de maio de 2016**. Este regulamento revoga toda a legislação publicada antes da era digital.

Este normativo comunitário, designado por **RGPD**, é aplicável a partir do dia **25 de maio de 2018**.

São 99 artigos que trazem algumas mudanças significativas, que terão diferente impacto na vida, nomeadamente na Administração Pública, consoante a sua natureza, área de atividade, dimensão e tipo de tratamentos de dados pessoais que realizem, das quais se destacam:

- A **alteração do modelo de regulação**, que passa de um modelo de hétero-regulação, onde as organizações notificam e solicitam autorização à CNPD para os seus tratamentos de dados pessoais, para um modelo de autorregulação, no qual têm a responsabilidade pela interpretação, operacionalização e manutenção da conformidade com o RGPD, ficando sujeitas à ação inspetiva da Autoridade de Controlo.
- O **alargamento do conceito de dados pessoais**, que passa a incluir quaisquer dados suscetíveis de identificar, mesmo que de forma indireta, um determinado indivíduo.
- O **reforço dos direitos** dos titulares de dados pessoais (nomeadamente o direito ao esquecimento e o direito à portabilidade), cuja implementação pode exigir alterações ao nível dos processos de negócio e dos sistemas de informação.
- O reconhecimento da importância da dimensão da proteção dos dados na manutenção do **direito à privacidade**.
- A **obrigatoriedade de reporte** à Autoridade de Controlo de quaisquer incidentes relativos ao comprometimento de dados pessoais e, em certas condições, aos próprios titulares afetados.

À luz das orientações emanadas a este propósito, pela Comissão Nacional de Proteção de Dados (CNPd), podem ser identificadas 10 áreas de atuação que asseguram a uma transição para o novo quadro legislativo.

1. Informação aos titulares dos dados

- O titular do dados deve ser informado de forma concisa, inteligível, utilizando uma linguagem clara e simples, quanto à base legal para o tratamento de dados, o prazo de conservação dos dados, informações mais detalhadas sobre as transferências internacionais, a possibilidade de apresentar queixa junto da CNPD.

2. Exercício dos direitos dos titulares dos dados

- Novas exigências específicas quanto à tramitação dos pedidos, em especial aos prazos máximos de resposta.
- Todo o procedimento deve ser devidamente documentado.
- Passa a existir o direito à limitação do tratamento e o direito à portabilidade.
- Existência de novos requisitos quanto ao direito à eliminação dos dados e quanto à notificação de terceiros sobre retificação, apagamento ou limitação de tratamento de dados solicitados pelos titulares.

3. Consentimento dos titulares dos dados

- Introdução de novas condições para a obtenção do consentimento, pelo que é necessário apurar se o consentimento obtido respeita todas as novas exigências, sob pena de o tratamento de dados se tornar ilícito por falta de base legal.

4. Dados sensíveis

- A natureza dos tratamentos de dados efetuados deve ser avaliada, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas.

5. Documentação e registo de atividades de tratamento

- Todas as atividades relacionadas com o tratamento de dados pessoais devem ser documentadas de forma detalhada, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

6. Contratos de subcontratação

- Os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais devem ser revistos, por forma a verificar se contêm todos os elementos exigidos.

7. Encarregado de proteção de dados (DPO)

- Será nomeada uma pessoa responsável que deverá garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do Regulamento.

8. Medidas técnicas e organizativas e segurança do tratamento

- As medidas técnicas e organizativas adotadas deverão assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD.
- 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.

9. Proteção de dados desde a conceção e avaliação de impacto

- Deve ser feita uma avaliação rigorosa ao tipo de tratamentos de dados que se projete 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, por forma a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

10. Notificação de violações de segurança

- Devem ser adotados procedimentos internos e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados (DPO) e notificação à CNPD.

No exercício das nossas funções, devemos reter o seguinte:

- Dados pessoais são todas as informações relativas a uma pessoa identificada ou identificável (nome, morada, património, vencimento, datas, números de cartões, números de telefone, endereços de rede (IP), vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc.);
- Não devemos reunir dados pessoais em papel ou em formato eletrónico sem estar previsto nos processos com que trabalhamos;
- Cuidado ao enviar dados pessoais, pois estes devem estar sempre encriptados ou protegidos;
- Cuidado ao destruir ou eliminar dados pessoais, porque estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
- Cuidado com os dados pessoais que trocamos com os nossos parceiros e em especial com parceiros fora da União Europeia;
- Documentos com dados médicos, e dados de menores são mais sensíveis pelo que devemos ter um cuidado redobrado na sua utilização;
- Se perdermos equipamentos ou documentos que contenham dados pessoais, ou aqueles forem furtados/roubados, devemos informar de imediato o Superior Hierárquico.

Ao proteger a informação dos outros estamos a defender a nossa