10 MEDIDAS PARA PREPARAR A APLICAÇÃO DO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

O **Regulamento Geral de Proteção de Dados (RGPD)** passará a ser aplicado diretamente a partir de 25 de maio de 2018, e vem substituir a atual diretiva e lei de proteção de dados pessoais. O novo quadro legal traz algumas mudanças significativas que terão diferente impacto na vida das organizações, consoante a sua natureza, área de atividade, dimensão e tipo de tratamentos de dados pessoais que realizem.

Assim, empresas e entidades públicas devem começar desde já a preparar internamente a sua organização para a aplicação do RGPD. É essencial conhecer as novas regras, analisar as novas obrigações, verificar o nível atual de cumprimento e adotar as medidas necessárias durante este período de transição para assegurar que tudo está pronto atempadamente.

Neste documento, estão identificadas dez áreas principais de atuação para prosseguir nos próximos meses. A CNPD continuará a dar orientações às entidades públicas e privadas sobre o regulamento, incluindo em áreas específicas que estão a ser objeto de discussão entre as autoridades de proteção de dados da União Europeia com vista a uma aplicação concertada e uniforme do RGPD.

1. INFORMAÇÃO AOS TITULARES DOS DADOS

Deve rever a informação que fornece aos titulares dos dados, por escrito ou por telefone, no âmbito da recolha de dados, seja esta realizada diretamente junto do titular ou não.

O regulamento obriga a prestar mais informações do que atualmente, designadamente a 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. Dentro das exigências de maior transparência, ter em atenção que as informações devem ser prestadas aos cidadãos de forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Deve ser tido particular cuidado quando as informações são dirigidas a crianças.

Assim, tem de reformular impressos, políticas de privacidade e todos os textos que prestem informação aos titulares dos dados, ao mesmo tempo que verifica se está efetivamente a fornecer, em todas as situações, a informação exigida por lei.

2. EXERCÍCIO DOS DIREITOS DOS TITULARES DOS DADOS

Deve rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, atendendo a novas exigências específicas do regulamento neste domínio quanto à tramitação dos pedidos, em especial aos prazos máximos de resposta. Todo o procedimento deve ser devidamente documentado.

Por outro lado, os direitos dos titulares foram alargados em relação à atual lei, passando a existir o direito à limitação do tratamento e o direito à portabilidade, 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.

Assim, a sua organização deve estar preparada para aplicar as novas obrigações, nomeadamente através da manutenção da informação num formato estruturado, de uso corrente e de leitura automática, quando aplicável, e de procedimentos eficazes de comunicação com as entidades terceiras a quem transmitiu os dados, de modo a assegurar o exercício efetivo dos direitos.

Por se tratar de direitos fundamentais dos cidadãos, esta é uma área de intervenção essencial, a qual sofreu várias alterações do ponto de vista procedimental, pelo que requer a maior cautela na sua adaptação às novas disposições legais.

3. CONSENTIMENTO DOS TITULARES DOS DADOS

Deve verificar a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais. O regulamento alarga o conceito de consentimento e introduz novas condições para a sua obtenção, pelo que é necessário apurar se o consentimento obtido pelo responsável pelo tratamento respeita todas as novas exigências.

Se assim não for, é imprescindível obter novo consentimento dos titulares dos dados em conformidade com as disposições do RGPD, sob pena de o tratamento de dados se tornar ilícito por falta de base legal.

Particular atenção deve ser dada ao consentimento dos menores ou dos seus representantes legais, considerando as exigências específicas do regulamento para este efeito.

4. DADOS SENSÍVEIS

Deve avaliar a natureza dos tratamentos de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições es-

pecíficas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas.

O regulamento veio estender o leque das categorias especiais de dados, integrando por exemplo os dados biométricos, que passaram a fazer parte do elenco de dados sensíveis.

Deve analisar também o contexto e a escala destes tratamentos de dados para verificar se daí decorrem obrigações particulares, tais como a designação de um encarregado de proteção de dados.

5. DOCUMENTAÇÃO E REGISTO DE ATIVIDADES DE TRATAMENTO

Deve documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação 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.

Uma vez que o regulamento prevê que as entidades em regime de subcontratação, designadas de "subcontratantes", passem a ter quase as mesmas obrigações que os responsáveis pelos tratamentos, estando de igual modo obrigadas a provar que cumprem tudo o que lhes é exigido, a prossecução desta medida de forma atempada é vital, pois terão de começar do zero.

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

6. CONTRATOS DE SUBCONTRATAÇÃO

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

Apesar de se manterem os princípios já vigentes na atual lei de proteção de dados, o RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de um vasto conjunto de informações. Assim, será muito provável que os contratos existentes necessitem de ser modificados para respeitar os termos do regulamento. Tal requer algum tempo, se houver várias subcontratações, pelo que é conveniente aprontar esta análise.

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 maio de 2018.

7. ENCARREGADO DE PROTEÇÃO DE DADOS

Deve preparar a designação do encarregado de proteção de dados com a antecedência devida, até porque este poderá desempenhar um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento.

Nesse contexto, especial atenção deve ser concedida à posição do encarregado de proteção de dados dentro da organização e ao reporte direto ao mais alto nível, bem como às funções que lhe são atribuídas pelo RGPD, cujo pleno desempenho requer a satisfação de determinadas condições.

Além das situações previstas no regulamento em que a organização está obrigada a designar um encarregado de proteção de dados, como é o caso das entidades públicas, o responsável pelo tratamento e o subcontratante podem sempre, mesmo não se encontrando no momento em nenhuma das circunstâncias exigíveis, decidir ter um encarregado de proteção de dados na sua organização, pelas evidentes vantagens que tal pode significar para o nível de cumprimento das obrigações.

8. 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.

9. 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.

Embora estes princípios já fossem aplicados no âmbito do princípio da qualidade dos dados, o RGPD vem expressamente prever a sua adoção no momento da definição dos meios de tratamento e no momento do próprio tratamento de dados, pelo que deve ser equacionada a sua aplicação atempada.

A fim de decidir sobre as medidas mais ajustadas, seja tendentes à pseudonimização, à minimização dos dados, ao cumprimento dos prazos de conservação da informação ou à acessibilidade dos dados, deve ter em devida conta as características do tratamento e os efeitos que este pode ter nos direitos dos cidadãos; se for suscetível de resultar num elevado risco, deve realizar uma avaliação de impacto sobre a proteção de dados, de modo a adotar as medidas adequadas para mitigar os riscos.

10. NOTIFICAÇÃO DE VIOLAÇÕES DE SEGURANÇA

Deve adotar 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 e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

Nem todas as violações devem ser reportadas à autoridade de controlo, apenas aquelas que sejam suscetíveis de resultar num risco para os direitos dos titulares. Todavia, todas as violações devem ser devidamente documentadas conforme preceituado no regulamento.

Também nalguns casos, em que possa resultar um elevado risco para os titulares, é exigido que estes sejam notificados, pelo que deve ser analisado desde logo o tipo de tratamentos de dados realizados e o potencial risco que pode ocorrer em caso de uma violação de segurança.

28 de janeiro de 2017