ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

Secção do puzzle: **Legislação**

Peça: **Regulamento Geral de Protecção de dados – preparar a conformidade**

junho 2020

Outras peças relacionadas com este tema:

- Regulamento Geral de Protecção de dados- garantir a conformidade

Índice

O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor a 25 de maio de 2018, e substituiu a lei de proteção de dados pessoais.

Neste documento, identificam-se dez áreas principais de atuação para preparar a conformidade com o novo regulamento.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

1. Informação aos titulares dos dados

O regulamento obriga a prestar um conjunto de informações, designadamente a base legal para o tratamento de dados, o prazo de conservação dos dados e a possibilidade de ser apresentada queixa junto da Comissão Nacional de Protecção de Dados.

Dentro das exigências de maior transparência, deve ter-se em atenção que as informações devem ser prestadas aos cidadãos de forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples.

Assim, terão de se reformular impressos, políticas de privacidade e todos os textos que prestam informação aos titulares dos dados.

2. Exercício dos direitos dos titulares dos dados

Deverão ser revistos os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, em especial no que respeita aos prazos máximos de resposta.

Os direitos dos titulares foram alargados em relação à atual lei, passando a existir o direito à **limitação do tratamento**, o direito à **portabilidade**, o direito à **eliminação dos dados** e quanto à notificação de terceiros sobre retificação, apagamento ou limitação de tratamento solicitados pelos titulares.

A 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.

2.1. Tratamento dos dados

Tem de existir fundamento jurídico para o tratamento de dados:

- **Consentimento do titular dos dados**
- **Necessidade de executar um contrato**

É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (…)

2.2. Portabilidade

O artigo 20.º do RGPD estabelece um novo direito à portabilidade dos dados, o qual está intimamente ligado ao direito de acesso.

Este direito permite aos titulares dos dados receber os dados pessoais que tenham fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento.

Este direito abrange os **dados fornecidos de forma ativa e consciente** pelo titular dos dados, bem como os **dados pessoais gerados pela sua atividade**.

Uma vez que possibilita a transmissão direta de dados pessoais entre dois responsáveis pelo tratamento, o direito à portabilidade facilitará a mudança para diferentes prestadores de serviços.

Os **dados pessoais derivados ou inferidos** a partir dos dados pessoais fornecidos pelo titular dos dados, por exemplo um perfil de utilizador criado através de uma análise de dados, **são excluídos do âmbito** de aplicação do direito à portabilidade dos dados, uma vez que não são fornecidos pelo titular dos dados, mas sim criados pelo responsável pelo tratamento.

Prazo de resposta a um pedido de portabilidade.

O responsável pelo tratamento fornece «ao titular as informações sobre as medidas tomadas [...], sem demora injustificada e no prazo de um mês a contar da data de receção do pedido». Este prazo de um mês pode ser alargado até três meses no máximo para os casos complexos.

Possibilidade de indeferir um pedido de portabilidade ou exigir o pagamento de uma taxa?

O artigo 12.º proíbe a exigência de pagamento de uma taxa pelo fornecimento dos dados pessoais, salvo se o responsável pelo tratamento puder demonstrar que os pedidos são manifestamente infundados ou excessivos, «nomeadamente devido ao seu caráter repetitivo»

3. Consentimento dos titulares dos dados

Tem de se 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, sendo 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.

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

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 aplicarem-se condições específicas para o seu tratamento.

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 também analisar-se 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 actividades de tratamento

Todas as atividades relacionadas com o tratamento de dados pessoais devem estar documentadas de forma detalhada, não apenas as que resultam diretamente da obrigação de manter um registo, mas também 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.

6. Subcontratação

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.

O RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de um vasto conjunto de informações. É muito provável que os contratos existentes necessitem de ser modificados para respeitar os termos 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.

7. Encarregado de protecção de dados

Designar o encarregado de proteção de dados que desempenha um papel fulcral para garantir que a organização cumpre todas as obrigações legais.

Deve ser dada especial atenção 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.

Mesmo que a organização não se encontre de momento em nenhuma das circunstâncias exigíveis, decidir ter um encarregado de proteção de dados tem evidentes vantagens para o cumprimento das obrigações.

8. Medidas técnicas e organizativas e segurança no tratamento

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.

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. Protecção de dados desde a concepção e avaliação do impacto

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.

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.

Nota: **Pseudonimização** - Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

10. Notificação de violações de segurança

Adotar procedimentos internos para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

Apenas devem ser reportadas à autoridade de controlo, as violações que sejam suscetíveis de resultar num risco para os direitos dos titulares. Todavia, todas as violações devem ser devidamente documentadas.

Nos 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.

11. Legislação aplicável (à data)

- *Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados* - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que entrou em vigor em 25 de maio de 2018;

- Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 de 27 de abril de 2016 - Lei n.º 58/2019, de 8 de agosto.