Encarregado de Proteção de Dados

| Recomendação - 10 de outubro de 2018

Considerando:

- As disposições do Regulamento UE n.º 2016/679, de 27 de abril de 2016, designado por Regulamento Geral sobre a Proteção de Dados (RGPD), quanto às responsabilidades do Responsável pelo Tratamento de Dados e do Encarregado da Proteção de Dados (DPO), descritas respetivamente nos artigos 24.º, 38.º e 39.º do RGPD.

- O necessário envolvimento do DPO em todas as questões relativas à proteção dos dados pessoais.

- Que nos termos do artigo 38.º do RGPD, o Responsável pelo Tratamento de Dados deve assegurar que o DPO seja «envolvido, de forma adequada e em tempo útil, [em] todas as questões relacionadas com a proteção de dados pessoais». Constituindo boas práticas que:

  - O DPO seja convidado a participar regularmente nas reuniões de direção intermédia e superior, sendo a sua presença recomendada sempre que sejam adotadas decisões com implicações na proteção de dados.
  - As informações pertinentes sejam transmitidas oportunamente ao DPO, para que este possa prestar um aconselhamento adequado;
  - O parecer do DPO seja sempre devidamente ponderado. Em caso de desacordo, constitui boa prática que sejam enunciados os motivos para não seguir o parecer do DPO;
  - O DPO seja consultado imediatamente após a ocorrência de uma violação de dados ou outro incidente.

- Que em relação às avaliações de impacto sobre a proteção de dados, o RGPD prevê explicitamente o envolvimento do DPO desde o início e especifica que, ao efetuar essas avaliações de impacto, o Responsável pelo Tratamento dos Dados deve solicitar o parecer do DPO.

- Que o Responsável pelo Tratamento dos Dados deve assegurar que o DPO seja informado e consultado durante a fase inicial de qualquer processo a fim de facilitar o cumprimento do RGPD e promover uma abordagem de proteção da privacidade desde a conceção.

- Que a prática descrita deve constituir o procedimento normal da governação da SGEC.

- Que é importante que o DPO seja considerado como interlocutor no seio da SGEC e que faça parte dos grupos de trabalho incumbidos de gerir as atividades de tratamento de dados na SGEC.

- Que é fundamental que o DPO, e a sua equipa, seja envolvido, desde a fase mais precoce, em todas as questões relacionadas com a proteção de dados.

Apresentam-se as seguintes recomendações, relativas à gestão da conformidade e monitorização do cumprimento do RGPD:

1. **Rever a informação que é fornecida aos titulares dos dados.**

Deve ser efetuada uma avaliação das políticas de privacidade, dos impressos e outros documentos que prestem ou solicitem informação aos titulares dos dados de modo a cumprir com o RGPD.

As Politicas de Privacidade, de utilização de cookies e de direito de autor devem ser publicadas, e ficar acessíveis, no *site* institucional.

Nos termos do artigo 37.º, n.º 7, do RGPD, o Responsável pelo Tratamento de Dados tem de publicar os contactos do DPO, e comunicar os contactos do DPO à Comissão Nacional da Proteção de Dados (CNPD).

Os titulares dos dados (tanto dentro como fora da SGEC) e as autoridades de controlo devem poder contactar, de forma fácil e direta, com o DPO, sem necessitar de contactar outra parte da SGEC. A garantia da confidencialidade das comunicações com o DPO é igualmente importante, de forma a afastar a relutância dos trabalhadores em apresentar qualquer queixa.

Assim, recomenda-se que os trabalhadores da SGEC sejam informados do nome e contactos do DPO, através, por exemplo, da intranet, do Outlook e da lista telefónica interna.

2. **Garantir, a todo o tempo, ao titular dos direitos pessoais o direito de acesso, retificação, atualização, oposição e apagamento dos seus dados pessoais.**

A prática usual consiste na criação de um endereço de correio eletrónico específico.

O Responsável pelo Tratamento de Dados tem a obrigação de informar o titular dos dados sobre o modo como os seus dados estão a ser utilizados (art.º 12.º e 14.º do RGPD).

O direito de informação obriga a que as informações fornecidas aos titulares dos dados sejam de fácil acesso e compreensão e formuladas numa linguagem clara e simples. É essencial que o titular dos dados compreenda o que está a acontecer aos seus dados.[1]

3. **Avaliar rigorosamente o tipo de tratamentos de dados a realizar.**

Deve ser analisado o tratamento de dados, a 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.

> Questões a colocar: Preciso de todos os dados pessoais cedidos? (minimização de dados); Preciso de realizar todos os tratamentos, atualmente efetuados, sobre esses dados pessoais? (proporcionalidade do tratamento): Preciso do acesso a esses dados pessoais e para quê? (responsabilidade e finalidade) O acesso a esses dados pessoais fica registado e como? Quem controla ou monitoriza o registo dos acessos?
>
> O tratamento de dados pessoais deve ter subjacente o princípio da precaução: quanto menos dados pessoais tratar e quanto menos tratamentos de dados pessoais realizar menos riscos estou a gerar para o titular dos dados pessoais.

4. **Rever os processos internos**.

Em muitos casos, existe uma obrigação jurídica da SGEC, que justifica o acesso a determinados dados pessoais, mas importa que sejam revistos todos os processos que utilizem dados pessoais, para determinar a sua conformidade com o RGPD.

5. **Rever,** quando for o caso, **os termos do consentimento**.

Ter especial atenção aos menores. São menores as pessoas singulares com idade inferior a 18 anos.

[1] As medidas integradas nesta recomendação já se encontram implementadas pela Secretaria-Geral da Educação e Ciência.

6. **Avaliar a natureza do tratamento dos dados efetuados**.

Devem ser apurados os dados pessoais que se podem enquadrar no conceito de dados sensíveis, ou em categoria especiais de dados, e aplicarem-se condições específicas.

O objetivo é reduzir os tratamentos de dados pessoais a um mínimo possível para a realização das finalidades dos mesmos: dados em excesso e desnecessários devem ser apagados.

O Responsável pelo Tratamento dos Dados deverá adotar medidas para se certificar, com um grau de certeza razoável, que os dados são exatos e estão atualizados.

Os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, exceto para fins de arquivo de interesse público, investigação científica, histórica ou para fins estatísticos.

A fim de assegurar que os dados pessoais sejam conservados apenas durante o período necessário, o Responsável pelo Tratamento dos Dados deverá fixar os prazos para o apagamento ou a revisão periódica.

7. **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.

8. **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 SGEC esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

9. **Rever as medidas técnicas e organizativas a adotar (pseudonimização, controlos de acesso, gestão de privilégios) e das medidas de segurança da informação.**

- Dar cumprimento ao disposto na Resolução do Conselho de Ministros n.º 41/2018, de 28 de março: https://dre.pt/application/conteudo/114937034

10. **Adotar procedimentos internos** e ao nível da subcontratação, se for o caso, para responder aos casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre Responsável pelo Tratamento dos Dados e o subcontratante, envolvimento do DPO e notificação à CNPD.

Anabela Afonso
Encarregada de Proteção de Dados