Em caso de *data breach*, como reagir?

Com a experiência entretanto adquirida pelas autoridades de controlo no contexto do RGPD, o CEPD aprovou novas orientações sobre as notificações de violações da dados. Este documento estará em consulta pública até ao dia 2 de março.

O Comité Europeu de Proteção de Dados (CEPD) aprovou, no dia 14 de janeiro de 2021, as Orientações 1/2021, as primeiras de 2021, sobre exemplos práticos e úteis de notificações de violações de dados pessoais (*data breach*) ("Orientações").

Estas Orientações complementam as *Guidelines WP250* adotadas pelo Grupo de Trabalho do Artigo 29.º em 2018, acrescentando a experiência entretanto adquirida pelas autoridades de controlo dos vários Estados-Membros com a aplicação do RGPD.

Em comparação com as anteriores orientações, as atuais adotam uma abordagem mais prática, sublinhando a importância de uma análise de risco, na qual se possa avaliar as possíveis causas de violação de dados. Fornecem, igualmente exemplos de violação de proteção de dados (os mais comuns) e os procedimentos a adotar, salientando a importância de documentar todo o processo em caso de violação de dados.

São seis os grupos de exemplos dados: (i) *ransomware*; (ii) acesso indevido a dados pessoais através da internet; (iii) violação decorrente da atuação humana dentro das empresas; (iv)) dispositivos ou documentos perdidos ou roubados; (v) violação decorrente do envio de correspondência; e (vi) outros casos (envolvendo ''engenharia social'').

Já os exemplos em concreto que são indicados pelo CEPD (cerca de 18) vão desde a apresentação de uma candidatura online a uma vaga de emprego, ao preenchimento de crendenciais num site de uma instituição bancária até à violação de dados pessoais em contexto hospitar.

Ou seja, são situações do dia-a-dia, que poderão desencadear uma violação de dados, a que nenhuma pessoa ou entidade estará de antemão a salvo. É, portanto, recomendável a adoção das salvaguardas necessárias e, em caso de violação de dados, desencadear as seguintes medidas:

1. Investigar a violação, para que, identificando a origem da violação, se possa avaliar as medidas a tomar. O ideal é que já exista um "plano de contigência" previamente delineado para o efeito;
2. De seguida, diligenciar pelas medidas necessárias à mitigação dos prejuízos resultantes da violação (como, por exemplo, retornar todos os sistemas informáticos afetados a um estado ''limpo'' e remediar a sua vulnerabilidade) e comunicar o ocorrido à autoridade de controlo competente (no caso português, a Comissão Nacional de Proteção de Dados). A comunicação da violação deve ser feita em 72 horas a contar do seu conhecimento, quando seja suscetível de implicar um risco para os direitos e liberdades das pessoas envolvidas (dos titulares dos dados);
3. Por fim, se a violação de dados configurar (ou for susceptível de configurar) um elevado risco para os direitos e liberdades, também tem de ser comunicada ao titular dos dados.

Estas Orientações estarão em consulta pública até ao próximo dia 2 de março.

Contactos

Cláudia Fernandes Martins
cmartins@macedovitorino.com

André Feiteiro
afeiteiro@macedovitorino.com

Débora Dutra
ddutra@macedovitorino.com