CUATRECASAS

Diretriz da CNPD sobre medidas organizativas e de segurança

A Comissão Nacional de Proteção de Dados (CNPD) emitiu várias orientações aos responsáveis pelo tratamento de dados e aos subcontratantes.

Portugal - Legal Flash

30 de janeiro de 2023

Aspetos-Chave

- A Comissão Nacional de Proteção de Dados aprovou a sua primeira Diretriz de 2023 sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais.

- A Diretriz surge num contexto de aumento crescente, em especial no ano de 2022, de ataques a sistemas de informação com um enorme grau de dimensão e complexidade que têm afetado dados pessoais.

- Os ataques devem-se, sobretudo: (i) às fragilidades das infraestruturas, (ii) à falta de formação dos utilizadores para detetarem campanhas de *phishing*, e (iii) à ausência de consciencialização dos responsáveis pelo tratamento quanto aos riscos para os direitos dos titulares, devido à falta de investimento em mecanismos de segurança.

Principais destaques da Diretriz

- Nos últimos anos temos assistido a um crescimento exponencial de ataques a sistemas de informação que têm afetado os direitos dos titulares dos dados pessoais. Neste sentido, a CNPD na prossecução da atribuição de promoção da sensibilização dos responsáveis pelo tratamento e dos subcontratantes optou por emitir orientações relativas às suas obrigações no domínio da segurança do tratamento de dados pessoais, de forma não exaustiva atendendo ao desenvolvimento tecnológico.

- A CNPD reforça a importância da obrigação dos responsáveis pelo tratamento de notificarem a autoridade de controlo quando existam violações de dados pessoais que representem risco para os direitos e liberdades dos titulares dos dados, em tempo útil e até 72 horas após a ocorrência do mesmo e a obrigação de documentar quaisquer violações de dados assim como de dar conhecimento aos titulares dos dados da ocorrência de uma violação de dados caso represente um risco para os seus direitos e liberdades.

- Para tal, a CNPD estabelece que, de forma a que os responsáveis pelo tratamento de dados pessoais sejam capazes de assegurar a proteção dos direitos dos titulares dos dados, é necessário que previamente se afira se são cumpridas todas as regras de proteção de dados em consonância com os princípios estabelecidos no n.º 1 do artigo 5.º do RGPD.

- Neste sentido, esclarece que o cumprimento das regras de proteção de dados se encontra dependente da adaptação dos seus modelos de negócio ou de gestão público, assim como de meios técnicos e organizativos, através de avaliações contínuas atendendo ao impacto que as novas tecnologias implicam no funcionamento das organizações e nas operações de tratamento.

- A CNPD estabelece que as medidas de segurança organizativas e técnicas devem ser adequadas às caraterísticas e sensibilidade de cada tratamento efetuado e às especificidades de cada organização.

- No âmbito das medidas organizativas, a CNPD estabelece que as entidades devem definir e atualizar regularmente o plano de resposta a incidentes, classificar a informação de acordo com a sensibilidade e confidencialidade, documentar as políticas de segurança, definir as melhores práticas de segurança de informação a adotar e, entre outras, fomentar junto dos colaboradores uma cultura de privacidade e segurança de informação.

- Em relação às medidas técnicas, a CNPD estabelece orientações em relação aos métodos de autenticação focando-se na necessidade da criação de palavras-passe seguras e na aplicação de autenticação multifator.

- Acresce, quanto à infraestrutura e sistemas, que se deve garantir a sua atualização, a organização e desenho de sistemas e infraestrutura que possibilitem a segmentação ou isolamento dos sistemas e redes de dados e a necessidade de reforçar a segurança dos postos de trabalho e servidores.

- Na mesma linha, a CNPD sublinha a necessidade de definir políticas e procedimentos internos sobre a utilização da ferramenta de correio eletrónico, a implementação de medidas de proteção contra *malware*, a forma como o armazenamento de documentos em papel que contenham dados pessoais deve ser realizada e as medidas relativas ao transporte de informação que integre dados pessoais.

- Por fim, a CNPD recomenda e incentiva os responsáveis pelo tratamento e os subcontratantes a atuarem de forma antecipada, através de **medidas preventivas e de proteção**, alertando, nomeadamente para a importância crescente de ter um plano de respostas a incidentes atendendo às medidas de segurança elencadas na presente Diretriz.

Disposições Finais

Dada a importância desta matéria, alertamos para a necessidade de:

- Implementar um **plano de resposta a incidentes** que inclua uma avaliação do risco para os titulares dos dados de forma a assegurar que o responsável pelo tratamento consiga concluir se deve notificar a CNPD relativamente a violações de dados.

- Adotar as **medidas de segurança, organizativas e técnicas**, atendendo às caraterísticas da entidade e às caraterísticas dos tratamentos de dados pessoais efetuados.

Para obter informação adicional sobre o conteúdo deste documento, por favor dirija-se ao seu contacto habitual na *Cuatrecasas.*