pbbr.a SOCIEDADE DE ADVOGADOS, SP, RL

Proteção de dados 02-2023

Nova diretriz da CNPD sobre Medidas de Segurança

A Comissão Nacional de Proteção de Dados (adiante "CNPD"), no âmbito de exercício das suas atribuições e competências - conferidas pelo Regulamento Geral sobre a Proteção de Dados (adiante "RGPD"), e, bem assim, pela lei que assegura a sua execução na ordem jurídica interna -, emitiu no final do mês de Janeiro, um conjunto de orientações dirigidas às organizações, relativas a medidas de segurança – Diretriz/2023/1.

Estas orientações surgem na sequência de um número crescente de ataques a sistemas de informação, em particular no ano passado, cujas consequências para os direitos dos titulares, no entender da CNPD, poderiam ser - na sua maioria - substancialmente reduzidas, se as organizações estivessem dotadas de medidas de segurança adequadas.

Com efeito, o objetivo primordial destas orientações é a sensibilização dos responsáveis pelos tratamentos de dados pessoais e dos subcontratantes para as suas obrigações legais no domínio da segurança dos tratamentos, designadamente as previstas no artigo 32.º do RGPD (*Segurança do tratamento*) e no artigo 33.º do RGPD (*Notificação de violação de dados pessoais)*. Neste sentido, por via da adoção de medidas técnicas e organizativas adequadas é possível estes agentes garantirem a segurança adequada dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Simultaneamente, a CNPD pretende alertar para a necessidade de ser realizado um maior investimento em meios de controle mais eficazes na proteção de sistemas de informação.

Assim, consoante o que for adequado tendo em conta as características de cada tratamento de dados pessoais efetuado e, naturalmente, atendendo às especificidades da concreta organização, a CNPD define, de forma sucinta, um conjunto de medidas técnicas e organizativas que devem ser consideradas pelas organizações.

No âmbito das medidas organizativas, a CNPD propõe *inter alia* a definição de um plano de resposta a incidentes e de recuperação de desastres, a criação de politicas de gestão de palavras-passe seguras e de gestão de ciclo de vida dos utilizadores, a classificação de informação de acordo com o nível de confidencialidade e sensibilidade, a verificação e avaliação periódica das medidas de segurança colocadas em prática e a realização de auditorias de segurança de TI, bem como a realização de avaliações de vulnerabilidade.

No que concerne às medidas técnicas, a CNPD divide o seu elenco em medidas relativas a autenticação, infraestruturas e sistemas, ferramentas de correio eletrónico, proteção contra *malware,* utilização de equipamentos em ambiente externo, armazenamento de documentos em papel que contenham dados pessoais e, por fim, relativas a transporte de informação que, por sua vez, integre dados pessoais.

O conjunto de medidas poderá ser consultado na sua íntegra em https://www.cnpd.pt/comunicacao-publica/noticias/diretriz-sobre-medidas-de-seguranca/.

Notamos que este elenco de medidas de segurança, apresentado pela CNPD, não tem caráter exaustivo e é forçosamente dinâmico. Atendendo à sua direta dependência do desenvolvimento tecnológico, o mesmo está, assim, sujeito a atualização sempre que se revelar necessário.

No mais, salientamos que, uma vez que se tratam de orientações, as mesmas não têm caracter vinculativo, sendo meramente recomendáveis.

Contacto:
Rita Roque de Pinho – rita.pinho@pbbr.pt
Adriana Alves Henriques – adriana.henriques@pbbr.pt