BindNews

01 de fevereiro de 2023

# DIRETRIZ N.º 2023/1 DA COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

A proteção de dados pessoais tem-se tornado cada vez mais relevante no ordenamento jurídico europeu e português. Nessa medida, o Regulamento Geral sobre Proteção de Dados e a Lei n.º 58/2019 vieram definir um conjunto de obrigações e deveres que recaem sobre todas as entidades que procedem ao tratamento de dados pessoais, impondo elevadas coimas às organizações que não cumpram os seus deveres.

Nesse seguimento, a Comissão Nacional de Proteção de Dados (CNPD), a autoridade de controlo portuguesa em matéria de proteção de dados pessoais, **publicou a Diretriz n.º 2023/1 que vem definir as medidas de segurança técnicas e organizativas essenciais a considerar e aplicar pelos responsáveis pelo tratamento dos dados (e respetivos subcontratantes)**. Tais medidas têm como objetivo conferir às operações de tratamento de dados a realizar um nível de segurança adequado ao risco que se lhes encontra associado, nomeadamente no que se refere à capacidade das organizações para garantir a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento.

A CNPD vem, assim, proferir uma lista de orientações relativamente às medidas técnicas e organizativas a adotar pelas organizações, mediante as quais se poderá garantir a

Bind
SOCIEDADE DE ADVOGADOS

LISBOA

Rua Julieta Ferrão, 10, 8.º
1600-131 Lisboa – Portugal

T. +351 213 104 120

bind@bindrl.pt
**www.bindrl.pt**

segurança adequada dos dados pessoais, em particular contra o tratamento não autorizado de dados, a sua perda, destruição ou danificação acidental. A lista inclui uma série de medidas relativas às próprias estruturas organizativas dos responsáveis pelo tratamento dos dados, bem como de natureza técnica e que as organizações deverão implementar de acordo com os tratamentos de dados em causa, em particular no que se refere à autenticação de credenciais, à infraestrutura e sistemas, às ferramentas de correio eletrónico, à proteção contra *malware*, à utilização de equipamentos em ambiente externo, ao armazenamento de documentação e ao transporte de informação. A título de mero exemplo, destacamos as seguintes medidas que surgem de natureza essencial para a CNPD:

- Adoção de procedimentos de análise para a monitorização dos fluxos de tráfego na rede;
- Criação de uma política de gestão de ciclo de vida dos utilizadores, para garantir que cada trabalhador tem acesso apenas aos dados necessários para executar as suas funções;
- Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, alterando-as com frequência;
- Desenhar e organizar os sistemas e a infraestrutura por forma a segmentar ou isolar os sistemas e as redes de dados para prevenir a propagação de malware dentro da organização e para sistemas externos;
- Reforçar o sistema com ferramentas antiphishing e antispam, que permitam bloquear ligações e/ou anexos com código malicioso;
- Criar um sistema de cópias de segurança (backup) atualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa;
- Permitir acessos apenas por VPN;
- Controlar os acessos, com registo das respetivas data e hora, de quem acede e do(s) específico(s) documento(s) acedido(s);

- Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB).

Por outro lado, com a presente Diretriz, a CNPD procura igualmente esclarecer as organizações das diversas obrigações e procedimentos a ter em conta perante uma violação de dados pessoais, discorrendo sobre as várias fases do procedimento de notificação e/ou documentação de um incidente de segurança, que as diversas organizações deverão cumprir, tanto na qualidade de responsáveis pelo tratamento dos dados, como na qualidade de subcontratantes.

Esta Diretriz surge na decorrência do número crescente de ataques aos sistemas de informação que se têm verificado nos últimos tempos, que colocam em causa as infraestruturas dos sistemas, bem como os próprios direitos dos titulares dos dados pessoais. O objetivo será, então, que os responsáveis pelo tratamento e os subcontratantes definam antecipadamente e coloquem em prática planos de prevenção, atendendo às medidas técnicas e organizativas elencadas.

Ressalvamos, contudo, que as medidas especificadas pela CNPD não consubstanciam uma lista fechada, nem, por outro lado, a sua verificação garante o total cumprimento das obrigações definidas na legislação atualmente em vigor nestas matérias. A adoção das medidas deverá sempre ser adequada às características e sensibilidade dos tratamentos de dados pessoais realizados em cada caso e às especificidades de cada organização, por forma a garantir a segurança do tratamento dos dados pessoais, bem como uma resposta apropriada e atempada em caso de violação de dados pessoais.

*O presente resumo não dispensa a consulta do texto integral da Portaria n.º 305/2022, 22 de dezembro, não constituindo o mesmo aconselhamento jurídico.*

BindNews

19 de Dezembro de 2022

Joana Almeida Gonçalves

Margarida Neiva Antunes

Bind
SOCIEDADE DE ADVOGADOS

LISBOA

Rua Julieta Ferrão, 10, 8.º
1600-131 Lisboa – Portugal

T. +351 213 104 120

bind@bindrl.pt
**www.bindrl.pt**