CNPD ANUNCIA MEDIDAS ORGANIZATIVAS E DE SEGURANÇA APLICÁVEIS AOS TRATAMENTO DE DADOS PESSOAIS

A CNPD recomenda ao responsável pelo tratamento de dados e ao subcontratante a adoção de medidas de segurança adequadas ao tipo de dados e à especificidade da organização em causa, de forma a garantir o cumprimento com o RGPD.

CONTACTOS

CLÁUDIA FERNANDES MARTINS
CMARTINS@MACEDOVITORINO.COM

JOANA FUZETA DA PONTE
JFUZETADAPONTE@MACEDOVITORINO.COM

A Comissão Nacional de Proteção de Dados ("CNPD") emitiu a primeira Diretriz de 2023, Diretriz/2023/1 ("Diretriz"), na qual apresenta um conjunto de medidas de segurança aplicáveis ao tratamento de dados pessoais.

A Diretriz surge na sequência da CNPD considerar oportuno sensibilizar os responsáveis pelos tratamentos e os subcontratantes para as suas obrigações no domínio da segurança dos tratamentos de dados pessoais, tendo em conta o aumento crescente, no último ano, de ataques a sistemas de informação que afetaram dados pessoais.

Importa recordar que, nos termos dos números 1 e 2 do artigo 32.º do Regulamento (UE) n.º 679/2016, de 27 de Abril ("RGPD") o responsável pelo tratamento de dados tem o dever de avaliar e aplicar as medidas técnicas e organizativas necessárias para conferir ao tratamento dos dados pessoais um nível de segurança adequado ao risco, incluindo a capacidade para garantir a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento.

Neste sentido, a CNPD apresenta algumas medidas que, consoante as caraterísticas e sensibilidade de cada tratamento, bem como as especificidades da organização em causa, devem ser consideradas.

Eis algumas das medidas apresentadas:

(i) Organizativas

(ii) Definir e exercitar regularmente o plano de resposta a incidentes e recuperação do desastre, prevendo os mecanismos necessários para garantir a segurança da informação e a resiliência dos sistemas e serviços, bem como assegurar que a disponibilidade dos dados é restabelecida atempadamente após um incidente;

(iii) Classificar a informação de acordo com o nível de confidencialidade e sensibilidade e adotar as medidas organizativas e técnicas adequadas à classificação;

(iv) Definir políticas de gestão de palavras-passe seguras (v.g. requisitos para tamanho, composição e armazenamento);

(v) Garantir que cada trabalhador tem acesso apenas aos dados necessários à execução das suas funções, criando uma política de "gestão de ciclo de vida dos utilizadores";

(vi) Realizar auditorias de tecnologias de informação, de forma a serem identificados os "alvos mais frágeis" e serem adotadas medidas adequadas;

(vii) Criar uma política interna para documentar eventuais violações de dados pessoais e saber como agir em caso de violação;

(viii) Fomentar junto dos colaboradores uma política de privacidade e segurança;

(ix) Efetuar avaliações periódicas das medidas adotadas e proceder à sua revisão sempre que necessário.

(B) Técnicas

A CNPD apresenta um conjunto de medidas técnicas diferenciadas, nomeadamente: de

(i) Autenticação

a) Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 carateres), as quais devem ser alteradas com frequência;

b) Equacionar a aplicação de autenticação multifator sempre que a informação ou os utilizadores assim o justifiquem.

(ii) Infraestrutura e sistemas;

a) Garantir a atualização dos sistemas operativos e das aplicações;

b) Garantir a segmentação ou isolamento dos sistemas e redes de dados;

c) Monitorizar a utilização do software instalado;

d) Bloquear os redirecionamentos suspeitos através de motores de busca.

(iii) Ferramenta de correio eletrônico

a) Garantir a elaboração de políticas internas com regras claras sobre o envio de mensagens de e-mail com dados pessoais;

b) Ponderar a criação de listas de distribuição ou grupos de contacto para prevenir o envio massivo de mensagens por destinatários indevidos;

c) Encriptar com código, ao qual só o destinatário tenha acesso, os emails e/ou anexos enviados que contenham dados pessoais;

d) Realizar ações de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico de acordo com os procedimentos definidos, dando a conhecer os "erros mais comums" que podem suscitar uma situação de violação de dados pessoais.

(iv) Proteção contra malware

a) Utilizar encriptação segura especialmente no caso de credenciais de acesso, de dados especiais , de dados de natureza altamente pessoal8 ou de dados financeiros;

b) Adotar ferramentas que bloquem ameaças em tempo real.

(v) Utilização de equipamentos em ambiente externo

a) Bloquear as contas após várias tentativas inválidas de login;

b) Aplicar cifragem dos dados;

c) Definir regras claras e adequadas para a utilização de equipamentos em ambiente externo.

(vi) Armazenamento de documentos em papel que contenham dados pessoais

a) Utilização de papel com elevada durabilidade;

b) Conservar documentação em locais com temperatura e humidade adequadas;

c) Proteger os documentos que contêm dados sensíveis em locais seguros (v.g. fechados, resistentes ao fogo e inundação);

d) Garantir a destruição "segura" dos documentos,

(vii) Transporte de informação que integre dados pessoais.

a) Adotar medidas que impeçam a leitura, cópia, alteração ou eliminação de dados no transporte da informação;

b) Utilizar dispositivos em massa ou arquivo potencialmente permanente.

A CNPD, como seria expectável, chama a atenção para o facto das medidas apresentadas "*não terem caráter exaustivo e serem forçosamente dinâmicas, pela sua direta dependência do desenvolvimento tecnológico, estando, por isso, sujeitas a atualização sempre que se revelar necessário*".