MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

MEDIDAS ORGANIZATIVAS E DE SEGURANÇA APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS

CNPD DISPONIBILIZA DIRETRIZ QUE VISA «SENSIBILIZAR» PARA AS «OBRIGAÇÕES NO DOMÌNIO DA SEGURANÇA DOS TRATAMENTOS DE DADOS PESSOAIS»

«A CNPD emitiu orientações para as organizações sobre medidas de segurança que devem ser adotadas para minimizar as consequências para os direitos das pessoas quando há ataques a sistemas de informação».

É desta forma que a Comissão Nacional de Proteção de Dados (CNPD) apresenta a primeira Diretriz emitida em 2023, a Diretriz/2023/1, de 10 de janeiro, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais.

A CNPD justifica a oportunidade de emissão destas orientações em face do número crescente de ataques a sistemas de informação que têm vindo a acontecer e que, na sua maioria, afetam a confidencialidade, a disponibilidade e/ou a integridade de dados pessoais. Segundo aquela autoridade, «na maior parte dos ataques a que se assistiu, as consequências para os direitos dos titulares dos dados poderiam ter sido senão evitadas, pelo menos substancialmente reduzidas»[1].

[1] No Relatório de atividades de 2022 – datado de 9 de fevereiro 2023 – a CNPD reporta ter registado 367 processos/notificações de *data breach*, destacando em 2022, quanto à sua origem, «o ***ramsonware*** (110) e a **falha humana** (81) como tendo sido as causas de grande parte das violações de dados pessoais notificadas. Com um peso ainda significativo como origem de incidentes ocorridos, assinalam-se as **falhas aplicacionais**, seja ao nível do desenho, da implementação e/ou da configuração (46), os esquemas de engenharia social como o ***phishing*** (43) e a exploração de outras vulnerabilidades (38) [...]», Relatório de Atividades 2022 da CNPD.

Trata-se de uma Diretriz que se destina:

- Aos responsáveis pelo tratamento de dados pessoais, antes de mais, mas também aos que tratem os dados pessoais por conta daqueles – os, chamados, subcontratantes[2]; e que se destina
- A entidades públicas e a entidades privadas[3].

O elenco de medidas de segurança do tratamento de dados pessoais que consta da Diretriz não é de adoção obrigatória – estão em causa meras orientações – e, como é sublinhado pela própria autoridade, também não deve ser visto como uma lista fechada[4].

As medidas recomendadas abarcam diferentes vertentes, sistematizadas conforme tabela abaixo:

Natureza da medida	Âmbito ou área de atuação das medidas
Medidas técnicas	Autenticação
	Infraestrutura e sistemas
	Ferramenta de correio eletrónico
	Proteção contra *malware*
	Utilização de equipamentos em ambiente externo
	Armazenamento de documentos em papel (que contenham dados pessoais)
	Transporte de informação (que integre dados pessoais)
Medidas organizativas (planos, políticas, procedimentos, práticas, etc.)	

Nas indicadas áreas de atuação, são contempladas recomendações múltiplas (medidas concretas) que abarcam realidades tão dispares como a definição e o exercício regular de planos de resposta a incidentes, os mecanismos de resiliência, a recuperação e o restabelecimento de sistemas, a

[2] Embora a CNPD sublinhe que «o recurso à subcontratação não altera o facto de o responsável pelo tratamento deter a responsabilidade global pela proteção dos dados pessoais.
[3] Embora, como é sabido, no caso da Administração Pública e do setor empresarial do Estado, em 2018, o Governo tivesse definido respetivamente, orientações técnicas e recomendações, em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas do RGPD (cf. Resolução do Conselho de Ministros n.º 41/2018, de 28 de março).
[4] Segundo alerta a CNPD «as medidas de segurança de tratamento dos dados pessoais que em seguida se elencam não têm caráter exaustivo e [...] [são] forçosamente dinâmicas, pela sua direta dependência do desenvolvimento tecnológico, estando, por isso, sujeitas a atualização sempre que se revelar necessário».

monitorização e a análise de fluxos de tráfego na rede, as políticas respeitantes a (e adoção de) credenciais de acesso robustas (complexidade e tamanho das palavras-passe adotadas), a aplicação de autenticações multifator, a adoção de alarmísticas, a realização de auditorias e avaliações de vulnerabilidades, a sua documentação e correção, a implementação de medidas de sensibilização de colaboradores, a atualização do *firmware* dos equipamentos de rede, as medidas de robustecimento de segurança de postos de trabalho e de servidores, a organização e o desenho de sistemas e infraestruturas segmentadas (para prevenir a propagação de *malware*), a adoção de políticas e de procedimentos claros no uso de correio eletrónico (adequados a evitar situações acidentais tipicamente geradoras de incidentes e violações de dados), os sistemas de *backup*, os mecanismos e as soluções de acesso remoto seguro (por exemplo, VPN), as características dos locais de armazenamento de dados em papel (para garantia de integridade), as medidas de controlo e de registo de acessos (também para os dados conservados em suporte papel), o recurso à encriptação segura no transporte de dados em dispositivos de massa, entre outras.

A Diretriz contém ainda uma secção dedicada aos deveres do responsável pelo tratamento de dados, em caso de violação de dados pessoais (*data breach*).

Mencionam-se, em especial, os deveres de:

- Notificação da violação à CNPD, até 72 horas após conhecimento da sua ocorrência, sempre que aquela seja suscetível de resultar num risco para os direitos e liberdades dos titulares;
- Documentação de quaisquer violações ocorridas – compreendendo os factos relacionados com a violação, os respetivos efeitos e medidas de reparação adotadas – caso o responsável conclua que a notificação à CNPD não é exigível[5];
- Comunicação aos titulares da ocorrência da violação quando ela for suscetível de implicar um elevado risco para os direitos e liberdades daqueles, logo que seja razoavelmente possível.

[5] Sendo exigível (embora a Diretriz não o diga expressamente) que o responsável faça uma avaliação dos riscos que podem resultar da violação e conclua que ela não é suscetível de resultar num risco para os direitos e liberdades dos titulares.

E a este propósito, a CNPD inclui recomendações, em linha com orientações já emitidas pelo Comité Europeu para a Proteção de Dados.

A Diretriz lembra também que o responsável – nos tratamentos de dados que realiza diretamente – deve **dispor de e aplicar uma política interna para detetar e gerir incidentes** de segurança com impacto na proteção de dados. Nos tratamentos de dados confiados a subcontratantes, o responsável deve **dispor de mecanismos de controlo eficazes** quanto à atuação destes.

Tiago Félix da Costa [+info]
Helena Tapp Barroso [+info]