VIEIRA DE ALMEIDA

GDPR FINES TRACKER

SEGURANÇA DO TRATAMENTO

VdA EXPERTISE

Novembro 2021

Incumprimento de obrigações de segurança do tratamento de dados dá origem a coima de EUR 400.000.

A Autoridade de Proteção de Dados Holandesa aplicou uma coima, de EUR 400,000, à companhia Transavia, por incumprimento da obrigação de implementação de medidas técnicas e organizativas, nos termos exigidos pelo Regulamento Geral sobre a Proteção de Dados (RGPD).

O caso remonta a setembro de 2019 quando a Transavia foi alvo de um ciberataque. Concluiu-se que o atacante poderia potencialmente ter acedido a dados pessoais de 25 milhões de passageiros, tendo-se comprovado o acesso a dados de mais de 83.000 passageiros.

Na sequência da notificação da violação de dados pessoais, a Autoridade de Proteção de Dados Holandesa detetou graves falhas de segurança que terão, segundo esta autoridade, permitido o acesso do hacker aos sistemas da Transavia.

Em particular, destacam-se as seguintes falhas:

- Existência de passwords fracas – não existia uma política de passwords com regras de construção e revisão de passwords;
- Ausência de um processo de autenticação robusto – apenas era exigida password, não existindo um procedimento de autenticação *multi-factor*;
- Ineficiente processo de atribuição de acesso - uma vez acedidas as duas contas da Transavia, o hacker acedeu a um conjunto de sistemas, já que não existia um procedimento de atribuição de acessos aos sistemas baseado na regra "need to know."

Neste caso, a Autoridade de Proteção de Dados Holandesa concluiu que a Transavia não tinha levado a cabo uma avaliação efetiva dos riscos de segurança nos termos exigidos pelo RGPD, pelo que não identificou e implementou as medidas de segurança do tratamento adequadas ao risco.

Este não é o primeiro caso em que uma organização, na sequência de um incidente, é condenada por uma autoridade de controlo, por insuficiente adoção de medidas técnicas e organizativas para proteção dos dados pessoais.

As autoridades de proteção de dados europeias já emitiram mais de 200 decisões aplicando coimas por não cumprimento das obrigações de segurança do tratamento de dados, nos termos do RGPD. A este respeito, são de destacar os casos da British Airways e Marriott.

Assim, as organizações que adotarem medidas técnicas e contratuais robustas, bem como planos de segurança e de mitigação de riscos, estarão em melhores condições para acautelar eventuais responsabilidades.

Para este efeito, a adoção de um programa de ciber-resiliência, com uma abordagem holística, cobrindo os temas jurídicos, tecnológicos, procedimentais e organizacionais é essencial face ao aumento dos incidentes, o reforço da carga regulatória e o aumento da exigência das autoridades de proteção de dados.

Contactos

MAGDA COCCO
MPC@VDA.PT

INÊS ANTAS DE BARROS
IAB@VDA.PT

MARIA DE LURDES GONÇALVES
MLG@VDA.PT