Published on *The National Law Review* https://natlawreview.com

When Data Breaches Cost Twice – AEPD's Landmark Fine Shows That Being the Victim of a Cyberattack Doesn't Excuse GDPR Failures

Article By:

Claire Murphy

In a cautionary decision for companies handling personal data, the Spanish Data Protection Authority (AEPD) issued a substantial fine to a telecommunications distributor following a significant data breach. In April 2021, the company at the center of the case had been targeted by a ransomware attack using Babuk malware, which encrypted files and interrupted operations. When the company refused to pay the ransom, cybercriminals published the personal data of around 13 million individuals on the dark web, exposing affected users to serious risks of fraud and identity theft.

After investigating, the AEPD found the company in violation of key provisions of the General Data Protection Regulation (GDPR), specifically articles 5.1(f) and 32. These articles require companies to protect the confidentiality and security of personal data through appropriate technical and organizational safeguards. The AEPD concluded that the company failed to meet these standards, resulting in fines totalling €6.5 million.

A notable element of the ruling was the AEPD's clarification of the GDPR's dual requirements under articles 5.1(f) and 32. These provisions address different goals – while Article 5.1(f) focuses on protecting data confidentiality and integrity, Article 32 requires risk-based security measures to prevent breaches from occurring in the first place. The AEPD emphasized that these obligations are separate but complementary, underscoring that breaches can involve both a loss of confidentiality and inadequate safeguards, each carrying different potential penalties.

While the company had implemented some security measures, the AEPD deemed them inadequate given the sensitivity and volume of the data processed. The regulator highlighted that the company lacked effective protocols in key areas, such as password management, perimeter security configuration, network monitoring, and employee training on data protection. Critically, the company also failed to anonymize or encrypt data, leaving it accessible in clear text – something that allowed attackers to share it publicly.

The ruling emphasized that organizations are expected to anticipate risks and implement safeguards to protect personal data in the event of a breach. Although the company did not act intentionally, the AEPD found its security shortcomings to be negligent, underscoring the principle that companies processing high volumes of personal data must exercise a higher standard of care.

The AEPD identified several factors that aggravated the sanctions, including the scale of the data breach, the number of affected individuals, and the potential harms resulting from the data's exposure on the dark web.

This case serves as a critical reminder – companies must take a proactive, comprehensive approach to data protection. Cyber threats are a constant risk, but GDPR compliance requires implementing strong safeguards to minimize harm. Organizations should consider this ruling as an urgent call to assess and strengthen their security strategies and ensure that employees receive thorough and ongoing data protection training.

National Law Review, Volume XIV, Number 318