

**Question for written answer E-003669/2025
to the Commission**
Rule 144
Nikolaos Anadiotis (NI)

Subject: Cyberattacks and digital vulnerability of European airports

Recent cyberattacks on the shared platform Muse, carried out with ransomware, as confirmed by the competent EU agency (ENISA), paralysed the electronic systems for transporting passengers and baggage at key European airports.¹

They demonstrate the vulnerability of the digital environment and raise serious concerns about the dependence of critical infrastructure on central digital systems of third-party providers,² as well as the potential risk of a massive leak of passenger personal data. There is an urgent need to ensure security, privacy and general well-being.

In view of the above:

1. What immediate measures does the Commission propose or require to ensure the operational resilience of airports against ransomware attacks, in particular when third-party shared platforms are used?
2. Does the Commission intend to establish minimum mandatory security standards - technical and organisational - and certification and transparency rules for providers of critical aviation systems?
3. What measures are being put in place to prevent the loss of important data or the mass leakage of passengers' personal information, with a view to their immediate protection?

Submitted: 22.9.2025

¹ <https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22>; <https://apnews.com/article/europe-airports-cyberattack-29b6d890baf7ac3a22f0f2b2f169b890>

² <https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22>