European Commission confirms personal data exposed in AI-assisted attack on EU Academy



The European Commission has confirmed that an AI-assisted cyberattack exposed names and email addresses of EU Academy users. The investigation continues, and the data protection supervisor has been notified.

- The attack was detected on October 22 and first led to the temporary shutdown of several applications.
- Investigators later found a breach on EU Academy, a learning platform used by people outside the Commission.
- Names and email addresses are affected; the full scope is still being investigated.
- EU Academy access is suspended and the European Data Protection Supervisor has been notified.
- Attribution is pending; Euronews reports a suspected China-backed group, and the Commission has

> not named the AI tool used.

The European Commission has confirmed that the cyberattack it disclosed last week led to the compromise of personal information. Initially, it had said it found no evidence that staff data was affected, and several applications were temporarily shut down.

What is known

A spokesperson said the investigation found a breach affecting EU Academy, an online learning platform used by people outside the Commission to study courses on European Union policy. The exposed data includes users' names and email addresses, but the full extent is still being examined. Access to the platform has been suspended and the European Data Protection Supervisor has been notified.

The Commission has not contacted affected individuals directly, since the scale is not yet established. It posted a general notice to all users of the website instead. The attack was detected on October 22. The Commission said last week it was largely contained, but declined to say on Monday whether the incident is over.

Attribution and AI use

The Commission said AI was involved but has not named the tool. Euronews reports that the Commission suspects a China-backed group and that the attack is not yet fully contained. It also reports that the suspicion rests partly on the use of Artex, an AI-powered penetration testing framework with Chinese roots. The Commission says attribution will only come once the investigation concludes, so these points should be treated as unconfirmed.

Why it matters

The case shows that an initial finding of no personal data impact can change as an investigation proceeds. It also shows that platforms serving external users, such as training or customer portals, can hold personal data that needs the same protection as core systems.

What to do now

1. Inventory external-facing platforms (training, customer, partner portals) and record which personal data each one holds.
2. Review incident response playbooks so initial 'no personal data impact' statements are treated as provisional until scoping is complete.
3. Confirm PDPL breach assessment and notification steps, including contact with SDAIA, are ready for incidents involving names and email addresses.
4. Prepare a general user notice template for cases where affected individuals cannot yet be identified.

5. Add AI-assisted attack scenarios to threat modelling and detection testing for internet-facing applications.