University of Copenhagen confirms test-environment breach affecting 525,000 people



The University of Copenhagen confirmed that attackers accessed one of its test environments holding personal data of 525,000 people. The source excerpt gives no further detail.

- The University of Copenhagen in Denmark confirmed the incident.
- Hackers accessed one of its test environments.
- The environment contained personal data of 525,000 people.
- The available source text does not describe the data types, cause or timeline.

What was reported

The University of Copenhagen in Denmark has confirmed that hackers gained access to one of its test

environments. According to the report, that environment held personal data relating to 525,000 people.

The excerpt available to us is short. It does not say which categories of data were affected, how the attackers got in, when the intrusion happened, or what the university has done in response. We have therefore not included any of those points.

Why it matters for regulated institutions

The case is a reminder that test and development environments can hold real personal data and may be less tightly controlled than production systems. Where live data is copied into such environments, the exposure can be as serious as a production breach, and the obligations around protecting that data do not shrink because the system is labelled as testing.

Institutions in the Kingdom that process personal data of customers, students, patients or employees should treat this as a prompt to check their own non-production estate, rather than as a reason for alarm.

Next steps

A short, practical review is enough to start: find out where personal data sits outside production, confirm who can reach it, and decide whether it needs to be there at all. Findings should be recorded and any gaps added to the existing risk register.

What to do now

1. Inventory test, development and staging environments that hold personal data.
2. Replace real personal data in non-production systems with masked or synthetic data where possible.
3. Apply the same access control, logging and monitoring standards to test environments as to production.
4. Review whether data copied to test systems is covered by your PDPL obligations and breach-response procedures.
5. Record findings in the risk register and assign owners for remediation.