UNIVERSITY OF COPENHAGEN

06 MAY 2026

Copenhagen University regrets to inform that, due to a security breach at a supplier (data processor) your personal information may have been compromised and possibly obtained by an unauthorized third party.

The affected system

The affected system is Absalon, which in some cases is referred to as Canvas (System name).

The data in question

Copenhagen University has not yet been fully informed by the supplier on all relevant aspects of the case, but we expect names, UCPH-e-mail addresses, and messages sent in Absalon, for instance between students and teachers or students and other students. In Absalon/Canvas you still have access to see which information you have exchanged via messages, in order to obtain your personal overview as to the affected data.
It is important to underline that there has been no access to CPR numbers (Social security numbers), as these are not stored in Absalon/Canvas unless you have shared them via messages in Absalon/Canvas.

What happened

Copenhagen University does not currently have a full overview regarding what and how this happened, and what has been carried out to stop it. But the current understanding is that a malicious hacker group has carried out an attack against the supplier, and is now attempting to extort money in exchange for not publishing the files.

The supplier has not yet informed Copenhagen University whether it is all students and staff in Absalon/Canvas that have been affected by the breach, but Copenhagen University assumes this to be the case.
The unauthorized third party in question is currently unknown to Copenhagen University. Copenhagen University is aware that a named extortion group has assumed responsibility for the breach, and claim to have accessed data tied to 275 million individuals across around 8800 organizations. It is our current assessment that the incident is global in nature. This has later been confirmed by the supplier late in the evening on May 5th, 2026.

What is Copenhagen University doing

Copenhagen University has attempted to gather all available information in regard to the incident, at a moment where information from the supplier is sparse. This has been done by carrying out our own forensics activities aimed to obtain as much information as possible.
Copenhagen University has furthermore raised several questions and concerns with the supplier, and expect to receive information as soon as possible about the nature of the breach.
Additionally, we are requesting further information related to the security prior before and after the security incident. We intend to use this information, to make sure the supplier lives up to its obligations to protect information entrusted to it by Copenhagen University.
Lastly, Copenhagen University has notified the Danish Data Protection Agency regarding the incident on May 5th, 2026.

Future use of Absalon/Canvas

Currently the system is still operating. Absalon/Canvas is a necessary component for the university education systems. You can continue to use Absalon/Canvas. The supplier has informed us that they have carried out security patches of the system. You are however advised to consider carefully which information you choose to exchange via messages in Absalon/Canvas. Absalon has not been approved for sensitive and confidential personal information. We advise against sharing such personal information on the platform.

What can you do now

The relevance of the following advice depends on our current understanding being correct:

- If your e-mail or phone number has been leaked, stolen or otherwise accessed by unauthorized persons, they can use this information to contact you.
  If at the same time the unauthorized persons know more information about you, for instance that you are studying or working at Copenhagen University, they can use this information to attempt to send you credible phishing (e-mail) / smishing (SMS) attacks. These attacks attempt to obtain information, often passwords or credit card information from you. This most often takes place by sending links claiming to be urgent matters. On those grounds Copenhagen University advice all staff and students to always exercise extra caution when receiving any unexpected communication that brings urgent matters that need immediate attention.
  Remember that you can always verify claims by contacting the university directly through our communication channels provided on the Copenhagen University website.

- Private messages: Depending on what they contain, a sophisticated attacker could attempt to use such information to convince you that they are someone you know personally. Always consider the possibility that even people you know well could have their accounts stolen and impersonated by a malicious person. Never share payment details or passwords with anyone.

- Course affiliation: The consequences of this data depends on individual circumstances. To some people studying a certain course is public domain, where as others prefer to keep such information private. On those grounds it is very difficult to provide guidance to our students.
- Furthermore Copenhagen University advice all students and staff to enable multifactor authentication where possible for all digital services.

  However, we would like to underline that Absalon/Canvas respects if you have requested Name and Address Protection via borger.dk. This means that in those cases, your name associated with course affiliation and messages will be your Copenhagen University username as first name and last name.

  Should you have enabled name and address protection, but also decided to use the UCPH alias system and enter a name there, please

be aware that this is the name that will likely be involved in the breach.

However should you have decided to overwrite this by instating an alias in the KU systems, then we expect that the chosen alias will appear instead.

If you have any questions, you can contact Copenhagen University at: digitalisering@adm.ku.dk

As always: If you suspect that someone has abused your account or data, please reach out to IT support: UCPH IT – University of Copenhagen

If you have questions regarding your rights or concerns in relation to what the incident means to you can contact information for Copenhagen University Data Protection Officer
Data Protection Officer: Mads Tolderlund
E-mail: dpo@adm.ku.dk

Your questions will be answered as soon as possible, but we expect a high volume, and will likely not be able to get back to everyone immediately.