How to abide by the GDPR rules
(General Data Protection Regulation)

- Lock your screen when you leave it (press Windows key + L).
- Make sure your ID card is visible.
- Don't let strangers into AU buildings.
- Create long passwords for your PC and for the systems.
- Never use the same password for several systems, homepages, etc.
- Never use the same password on AU equipment as on private equipment.
- Tidy your Outlook, drives, etc. regularly.
- Never store confidential and/or sensitive information on your personal drive or on the desktop of your PC.
- Calendar settings must never contain confidential information and/or sensitive, personal data.
- When sending an email internally with access to a document: Create a link to for instance WorkZone in stead of attaching the actual document.
- Make sure you pass on information to the correct recipient when sending emails.
- Avoid printing confidential and/or sensitive, personal data (shred the documents, if you print).
- Never leave prints with confidential and/or sensitive, personal information - not even on your desk.

How to delete personal information in Outlook

Sensitive personal data

Sensitive personal data:

- Health, race, ethnic background
- Political, philosophical, or religious beliefs
- Trade union affiliations.
- Sexuality and sexual orientation
- Biometric data.
- Genetic data

When the mail has been filed, you need to delete the mail within 30 days.

This information must be mailed via the "*safe mail plug-in*" in Outlook, or be uploaded in the sky, where the recipient can retrieve the mail.

Internal mails among employees at AU are classified as safe mails.

Normal personal data

CPR-number:

(Confidential, personal data)

Other ordinary, confidential, and personal data such as:

- Unlisted address
- Test scores
- Info about personal finances or other private circumstances

Ordinary, non-confidential data are for instance:

- Name and address
- E-mail
- Phone number
- Curriculum Vitae
- AU-ID
- Initials
- File number

Must be deleted in Outlook, when the case handling of the mail has been completed – or when the mail has been filed.

Always remember to tidy your Outlook.

Contact data

Contact data only:

Documents and mails containing no other data than auto signature, and name and e-mail of sender or recipient.

Can be stored in Outlook, unless there is no reasoned need to keep it, or the mail has been filed.

Always remember to tidy your Outlook.

BREACH of SAFETY – what do you need to do?

All employees are obligated to report a breach of safety, or in case of suspicion.

A breach of safety could be:

- A missing mobile, admission card, or PC
- Uninvited guests in AU's buildings.
- Equipment theft.
- Suspicion of misuse.
- Reception of suspicious mails.
- Sending mails to a wrong mail address/recipient.
- Unauthorized person gets unauthorized access to data.
- Confidential/sensitive personal data are sent via an ordinary, non-encrypted mail.

Have you observed a breach of security, or are you suspicious about a potential breach, you must send a form via below link immediately:

Security breach at AU

If you have any questions about GDPR (General Data Protection Regulation), please send an email to: dpo@au.dk