

Sådan overholder du GDPR-sikkerheden i hverdagen



Lås din skærm, når du går fra den (Windows-tast + L).



Bær dit id-kort synligt.



Luk ikke fremmede ind i AU's bygninger.



Benyt lange passwords, både til PC og til systemer.



Brug ikke samme password til flere systemer, hjemmesider m.m.



Brug ikke samme password på arbejdsudstyr, som du bruger privat.



Ryd løbende op i din Outlook, drev mm.



Opbevar ikke fortrolige og/eller følsomme oplysninger på dit personlige drev eller din pc's skrivebord.



Kalenderindstillinger må ikke indeholde fortrolige oplysninger og/eller følsomme personoplysninger.



Når du sender en mail internt med adgang til et dokument: lav så vidt muligt et link til f.eks. Workzone i stedet for at vedhæfte dokumentet.



Vær sikker på, at du videregiver oplysninger til rette modtager, f.eks. når du sender en mail.



Undgå at printe fortrolige og/eller følsomme personoplysninger (makuler dokumenterne, hvis du printer).



Efterlad aldrig prints med fortrolige og/eller følsomme personoplysninger – heller ikke på dit skrivebord.

Sådan skal du slette personoplysninger i Outlook

Følsomme personoplysninger

Følsomme personoplysninger:

- Helbred, race, etnisk oprindelse.
- Politisk, filosofisk eller religiøs overbevisning.
- Fagforeningsmæssige tilhørsforhold.
- Seksualitet og seksuelle orientering.
- Biometriske oplysninger.
- Genetiske oplysninger

CPR-nummer

(Fortrolig personoplysning)

Andre almindelige fortrolige personoplysninger, f.eks.:

- Hemmelig adresse
- Testbedømmelser
- Oplysninger om privatøkonomi eller andre private forhold

Almindelige personoplysninger

Almindelige, ikke fortrolige oplysninger, f.eks.:

- Navn og adresse
- E-mail
- Tlf.nr.
- CV
- AU-ID
- Initialer
- Journalnumre

Kontaktoplysninger

Kun kontaktoplysninger

Dokumenter og mails, der ikke indeholder andre oplysninger end autosignatur, samt navn og e-mail på afsender eller modtager.

Skal slettes i Outlook, når mailen er journaliseret, dog indenfor 30 dage.

Disse oplysninger skal sendes sikkert via "sikkermail-plugin'et" i Outlook eller kan uploades til et sikkert sted i skyen, hvor modtageren afhenter.

Interne mails mellem AU-medarbejdere er klassificeret som sikre mails.

Skal slettes i Outlook, når den sagsbehandling, som mailen vedrører, er afsluttet, eller når mailen er journaliseret.

Sørg generelt for at rydde op i Outlook.

Må ligge i Outlook, med mindre der ikke er et sagligt behov for at bevare den, eller mailen er journaliseret.

Sørg generelt for at rydde op i Outlook.

Sådan gør du, hvis du oplever et GDPR-brud på sikkerheden

Alle medarbejdere har pligt til at rapportere brud på sikkerheden, eller mistanke herom.

Et sikkerhedsbrud kan være:

- o Bortkommen mobil, adgangskort eller pc.
- o Ubudne gæster i AU's bygninger.
- o Tyveri af udstyr.
- o Mistanke om misbrug.
- o Modtagelse af mistænkelig mail.
- o Afsendelse af mail til forkert mailadresse/modtager.
- o Uvedkommende får uberettiget adgang til data.
- o Fortrolige/følsomme personoplysninger sendes med almindelig, ukrypteret mail.



Har du observeret et sikkerhedsbrud, eller har du mistanke om et muligt brud, skal du straks (!) sende en formular via dette link:

<https://medarbejdere.au.dk/informations/sikkerhed/databeskyttelse/sikkerhedsbrud-paa-au/>

Har du spørgsmål omkring GDPR kan du skrive til: dpo@au.dk