WORKSHOP BSS

Databeskyttelse

AARHUS
UNIVERSITET

18. DECEMBER 2017

OLE BOULUND KNUDSEN
INFORMATIONSSIKKERHEDSCHEF

OPBEVARING AF DATA

Der findes mange forskellige muligheder for opbevaring:

- Netværksdrev
- Forskningssystemer (Fx RedCap)
- Sharepoint
- Workzone
- Lokal pc
- USB diske
- Cloudtjenester (Dropbox, Onedrive, Box, Google Drev ….)

EKSISTERENDE REGLER

AU har

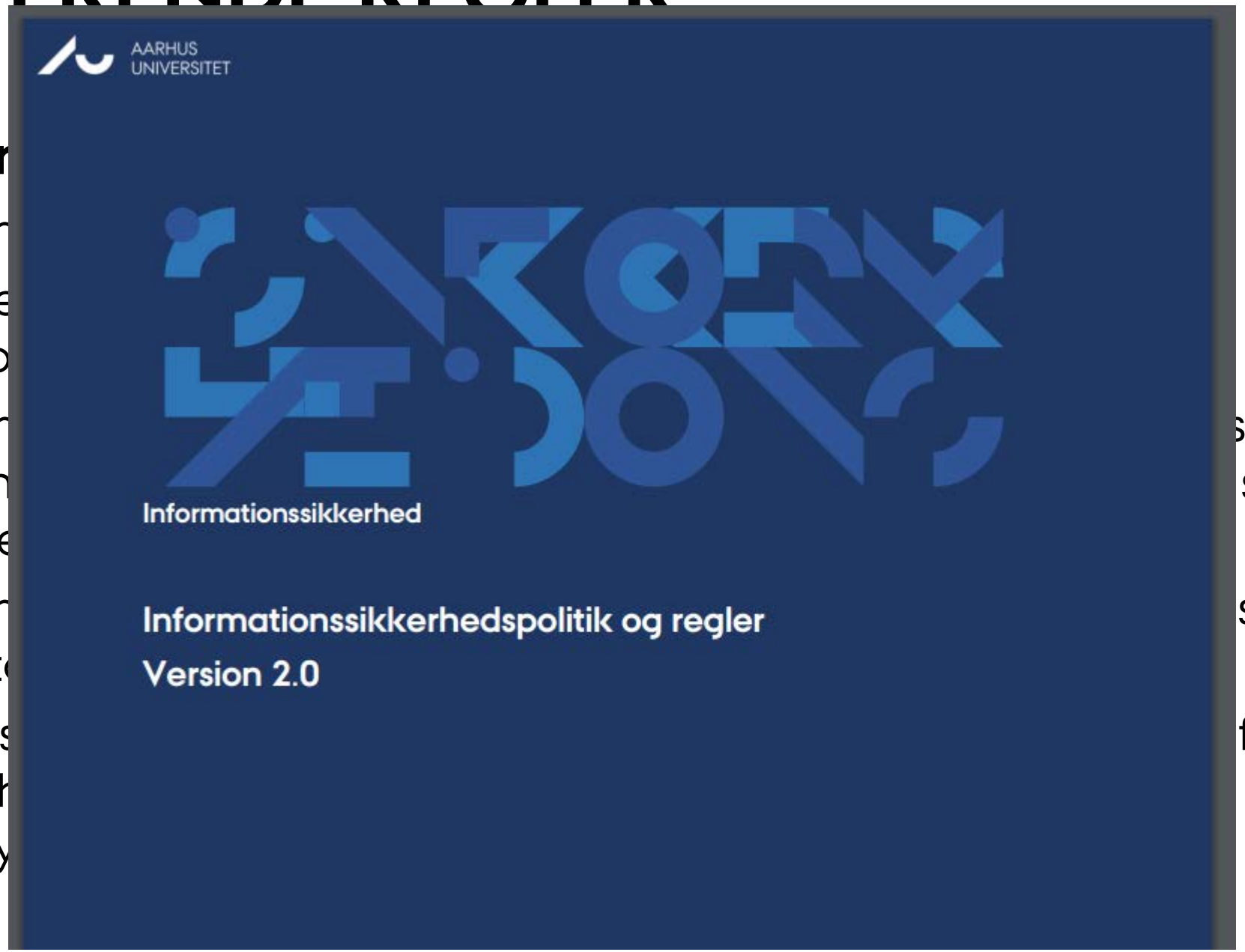
Følsomm

Definere
personо

Følsomm skal
begræn skal
overveje

Følsomm styr, og
hvis dat

Vær ogs f
databeh
datatilsy



LOGNING - HVORDAN?

§ 19. Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Stk. 4. Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

HVOR KAN MAN OPBEVARE DATA?

- Mens data er ”aktive” (dvs ikke i ”endelig form”) kan man anvende universitetets netværksdrev.

- Man kan også anvende dedikerede forskningssystemer o.lign.

- Man må som udgangspunkt IKKE opbevare følsomme data på Cloudtjenester, medmindre man har et gyldigt aftalegrundlag med den pågældende udbyder.

HVOR KAN MAN OPBEVARE DATA?

Når man er færdig med et forskningsprojekt:

Tre muligheder:

1. Anonymiser data – så kan man gemme dem hvor som helst.
2. Slet data
3. Arkiver data (fx Dansk Data Arkiv)

HVORDAN KAN MAN DELE DATA?

Internt:

- Netværksdrev
- Sharepoint
- (Snart OneDrive)
- Diverse forskningssystemer

Eksternt: (bemærk at aftalegrundlag skal være på plads!)

- Sharepoint
- (Snart OneDrive)
- Filesender.deic.dk
- Data.deic.dk
- Evt. udstille data – fx gennem en VDI løsning

PERSONDATA - MAIL

Man må gerne sende mails med følsomme data til andre, men…

- Internt mellem AU brugere betragtes som "Sikker post", men bemærk at mailen skal slettes efter senest 30 dage (både i sendt post og i modtagerens indbakke).
- Eksternt skal man bruge en af de "sikker post" løsninger, som AU råder over – så man kan sende krypteret enten direkte til en modpart (bemærk – kræver "NemID") eller til en persons E-Boks.

PÅ VEJ...

- Kryptering af alle Mac og PC klienter, der er medlem af uni.au.dk domænet. (Maskiner som styres af AU IT/Supporten)
- Oversigt over de forskellige muligheder for opbevaring og deling, samt konkrete retningslinjer.
- Større fokus på forskningsområdet omkring databeskyttelsesforordningen og datamanagement.

ANBEFALINGER

- Anvend **altid** krypterede USB nøgler til arbejdsbrug.
- Brug et skærmfilter på din pc, hvis du arbejder med følsomme eller fortrolige data.
- Brug et "langt" password – gerne mere end 16 tegn når du anvender kryptering – og lad være med at genbruge. (Gælder også til dit AU password)
- Følg med på informationssikkerhed.au.dk – her kommer løbende information om både it- og datasikkerhed.

SPØRGSMÅL

AARHUS
UNIVERSITET