DATASIKKERHED PÅ IFS

VERSION 4.3 2021

AARHUS
UNIVERSITY
DEPARTMENT OF PUBLIC HEALTH

NIELS-SØREN BØGH
SPECIALIST COORDINATOR

DATASIKKERHED PÅ IFS

Hvorfor datasikkerhed?

- På IFS arbejder vi med personhenførbare-/personfølsomme data

- På IFS arbejder vi ofte med registre med store befolkningsgruppers persondata
- På IFS indsamler vi ofte informationer med befolkningsgruppers persondata
- På IFS laves kvalitative studier, hvor GDPR er en særlig stor udfordring.

- IFS er underlagt GDPR – dataforordning i EU

- Vi lever af at låne borgernes data – derfor skal borgerne kunne stole på os!

AU INFORMATIONSSIKKEHED

AU har generelle regler og politikker for datasikkerhed

Med GDPR har vi en DPO på AU – Databeskyttelsesrådgiver, Søren Broberg Nielsen
På Health har vi en Databeskyttelseskoordinator, Jacob Hjort

Du SKAL holde dig opdateret med indholdet på denne AU hjemmeside:
https://medarbejdere.au.dk/informationssikkerhed
https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/

Du SKAL gennemgå selvlæringskurset:
https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/e-laeringskursus-om-persondataregler/

AU INFORMATIONS SIKKERHED

- Databeskyttelse (GDPR)
  - Til forskere
  - Til administrative medarbejdere og ledere
  - Til undervisere og vejledere
  - Til studerende
  - e-læringskursus om persondataregler
  - Anmeld sikkerhedsbrud
  - AU's behandling af personoplysninger
  - Generel information
  - Om frivillige foreninger
  - Privatlivspolitik
  - Kontakt
- Informationssikkerhedspolitik
- Klassifikation af data
- Anmeld sikkerhedsbrud
- Phishing
- Awareness-materiale
- Kontakt os

GDPR: Personoplysninger og forskning

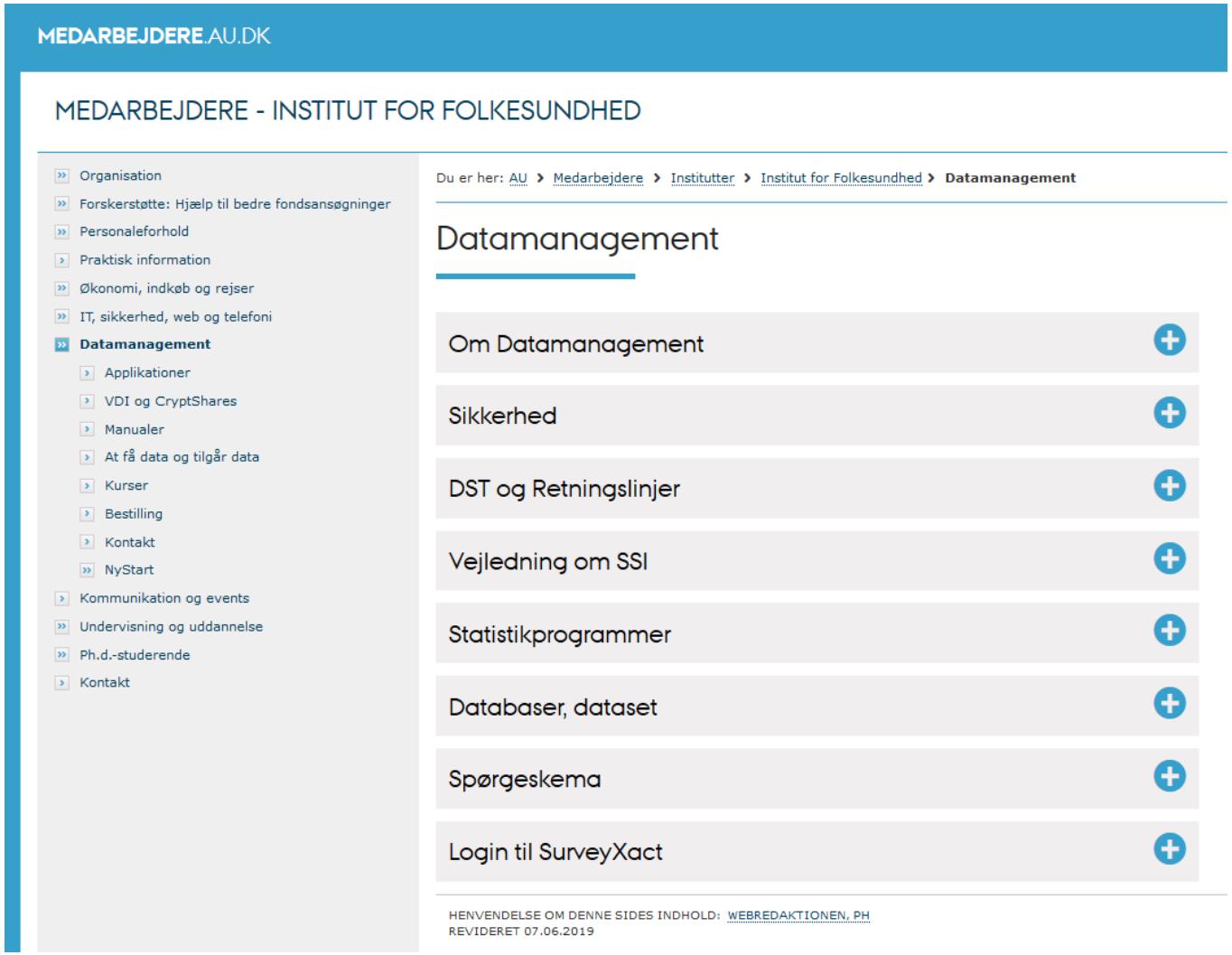
Arbejder du med personoplysninger i din forskning, er det vigtigt, at du følger lovgivningen på området. Få et overblik over, hvad du skal have styr på ift. GDPR:

- FØR du starter dit forskningsprojekt
- UNDER dit forskningsprojekt
- EFTER dit forskningsprojekt er færdigt

Har du spørgsmål?

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

IFS INFORMATIONS SIKKERHED



HVAD BETYDER GDPR FOR DIT ARBEJDE?

Hvad betyder GDPR for dit arbejde?

Når du starter et forskningsprojekt med personhenførbare data:

1. Datatilsynet – Fortegnelsen – "Tilladelsen" til at indsamle persondata

   Fortegnelsen fortegnelse@au.dk, Tlf.: 8715 3205

   Når du har lavet denne registrering på AU, er din forskning et AU projekt.

   Hvis ikke, så er der tale om privat forskning – og du står selv med ansvaret!

HVAD BETYDER GDPR FOR DIT ARBEJDE?

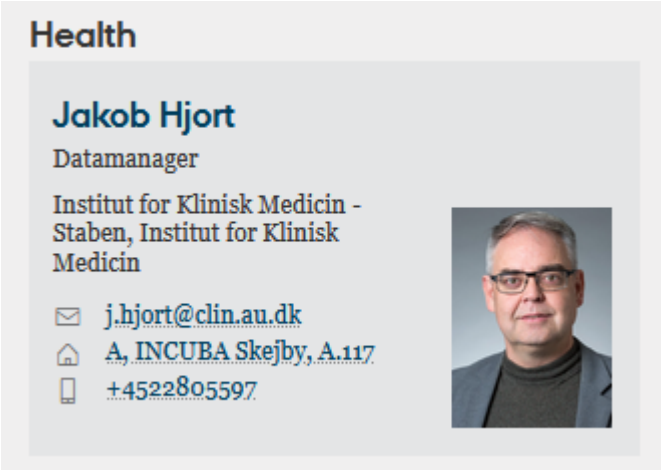
Hvad betyder GDPR for dit arbejde?

Når du starter et forskningsprojekt med personhenførbare data:

2. Hvem er Dataansvarlig, og hvem er Databehandler?

   Databehandleraftaler, Overladelses- og videregivelsesaftaler, lande udenfor EU m.m.
   TTO, tto@au.dk

3. Databeskyttelseskoordinator på Health



HVAD BETYDER GDPR FOR DIT ARBEJDE?

Når du starter et forskningsprojekt med personhenførbare data:

3. I mange projekter skal der derudover indhentes tilladelser/aftaler:
   DST, SDS, DAK-E, Labka II, CPR m.v.

   (Dette kan tage lang tid, så kom tidligt i gang!)

4. Du skal tænke over, at data har en "livscyklus", og til sidst skal data slettes

5. Der er krav til det udstyr, du må arbejde med data på

6. Du har ANMELDELSESPLIGT til Datatilsynet ved overtrædelser

ANMELDELSESPLIGT

Kontakt straks din Institutleder og Datamanagement
- Jo før vi ved det, jo bedre kan vi hjælpe
- Vi har kun 72 timer til at lave en anmeldelse!

Søren Broberg Nielsen
Databeskyttelsesrådgiver/DPO
AU Forskning og Eksterne Relationer - Technology Transfer Office
soren.broberg@au.dk
5530
+4587153198

- Du har PLIGT til at underrette AUs DPO ved overtrædelser
- Du har PLIGT til at underrette Datatilsynet ved overtrædelser
- Der SKAL gives underretning til de krænkede
- Der kan gives administrative bøder for overtrædelser
- Der kan være erstatningsberettigelse for krænkelse - ca. 1000 kr. pr. krænkede
  - 1000 kr. til hver af de 5,5 mio. danskere i dit datasæt!
- Derudover gælder

Individdata er fortrolige, jf.
Forvaltningslovens § 27, stk. 3 og Straffelovens §152.

BORGERNE HAR RETTIGHEDER

Når Aarhus Universitet behandler dine personoplysninger (privatlivspolitik):

Rettighed	Betydning
Indsigt	Du har ret til at se de personoplysninger, som den dataansvarlige behandler om dig, og få en række oplysninger om behandlingen.
Berigtigelse	Du har ret til at få urigtige/forkerte personoplysninger om dig rettet.
Sletning	Ret til sletning eller "retten til at blive glemt".
Begrænsning	Ret til begrænsning af behandling.
Dataportabilitet	Du har i visse tilfælde ret til at modtage dine person-oplysninger og til at anmode om, at personoplysningerne bliver overført fra én dataansvarlig til en anden.

BORGERNE HAR RETTIGHEDER

Når Aarhus Universitet behandler dine personoplysninger:

Rettighed	Betydning
Indsigelse	Du har ret til at gøre indsigelse mod en ellers lovlig behandling af dine personoplysninger.
Automatisk behandling	Ret til ikke at være genstand for en automatisk afgørelse udelukkende baseret på automatisk behandling, herunder profilering.

Rettigheder kan være begrænset af anden lovgivning eller underlagt undtagelser, fx i relation til forskning og offentlig myndighedsudøvelse.

IT UDSTYR

Der er krav til det udstyr du arbejder på

Derfor bliver kommunen politianmeldt:

Datatilsynet har ved vurderingen af, at der bør idømmes en bøde, lagt vægt på, at Favrskov Kommune forud for 12. august 2020 ikke havde foretaget kryptering af harddiskene på kommunens bærbare computere. Endvidere har tilsynet lagt vægt på, at der på den pågældende computer blev behandlet fortrolige og helbredsmæssige oplysninger om personer med nedsat fysisk eller psykisk funktionsevne og som var knyttet til et botilbud.

Kilde: Datatilsynet

Indstillet til bøde på 75.000 kr.

Som udgangspunkt må du kun arbejde med data på AUs udstyr

- Computere skal på **uni.au.dk** domain
- Din computer skal være krypteret – AU Bit-Locker System
- Dine enheder mobiler, kameraer, diktafoner osv. skal være krypterede
- Du skal bruge AU sikkerhedssoftware e.g. AUs McAfee Enterprise
- Du skal bruge CryptShares/VDI (specielt netværksdrev) til dine persondata
- Du må kun arbejde på AUs netværk VPN
- USB Sticks, memory cards (SD), hardiske etc. skal være krypterede

IT UDSTYR

Der er krav til det udstyr du arbejder på

Du må **ikke lagre data i skyen**, da du skal kunne redegøre for, hvor data fysisk befinder sig.

Mange af disse tjenester lagrer desuden data uden for EU. Du kan ikke redegøre tilstrækkeligt for at data opbevares ifg. GDPR. Det er heller ikke muligt at føre det lovpligtige tilsyn.

Der er krav til logning af al aktivitet og hvem, der har afgang til data.
Derfor bruger vi kun AU's CryptShares, som overholder disse krav.

Med **CryptShares/VDI** kan du dele data internt på AU's netværk med andre personer, der har et AUID og en gyldig tilladelse. Eksterne brugere kan få et AUID.

IT UDSTYR

Der er krav til det udstyr du arbejder på

Arbejd ALDRIG med data direkte på din computer eller på privat IT udstyr.

Data skal ligge indenfor AUs sikkerheds mur på CryptShares – og ikke lokalt på maskinen.

Arbejder du hjemme skal du lave en VPN forbindelse via (remote.au.dk)
Herefter laver du en Remote Desktop (fjerneskrivebord) til din computer på AU.

Har du en bærbar/Mac computer og derfor ikke har en computer stående på AU, så kan du få VDI adgang. Dette er en Virtuel Computer på AUs netværk.

LANDE UDENFOR EU

Jeg skal arbejde med data uden for EU, hvad gør jeg?

En i min projekt gruppe sidder uden for EU, hvad gør jeg?

Lande uden for EU er 3. partslande, som ikke omfattet af EU's GDPR aftale.
Derfor må du ikke bare tage data med eller videregive data.

Du skal her via TTO for at få udarbejdet en Overladeles- eller Overdragelsestilladelse til at overføre data til f.eks. et universitet uden for EU.
Dette kan være en omfattende proces...

Note. Under særlige forholde kan bruges VPN, VDI og CrypShares uden overladelse. Kontakt Datamanagement.

OVERFØRSEL AF DATA

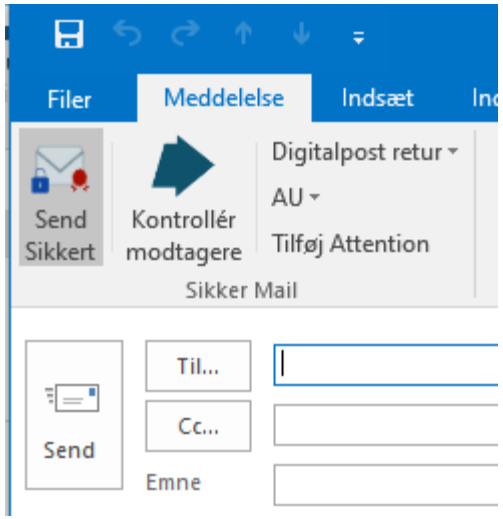
Når du skal overføre personhenførbare data, skal du være opmærksom på flere krav.

- Modtager skal være omfattet af en databehandleraftale
- Data der overføres elektronisk skal være krypteret
- Vi sender kun direkte fra A til B.

Vi overfører altså ALDRIG persondata med e-mail, ftp, skydrev osv.
Eller bruger tjenester, som efterlader kopier undervejs e.g. en mailserver.

Sendes data med kurer bruges krypterede DVD eller krypterede USB Sticks.
Nøglen sendes herefter f.eks. med sms og en kode udleveres kun ved en opringning.

OVERFØRSEL AF DATA



Logiva – sikker email

Er en udvidelse til Outlook der giver en "**Send Sikkert**" knap

Logiva sender sikker e-mail imellem fælles postkasser f.eks. fra AU til Region Midt .

Posten er kun krypteret imellem de fælles postkasser og kan derfor læses af alle der har adgang til fællespostkassen f.eks. også personer i IT.

Filoverførsler med Logiva skal derfor være krypteret en ekstra gang med e.g. 7-zip, så du er sikker på at kun rette modtager kan afkode filen. (A til B)

(Begrænset til små filer, typisk 10 MB)

OVERFØRSEL AF DATA

Department of Public Health
- Upload of files to Datamanagement

PhDmUpload.au.dk

Skal du selv modtage data kan du eller en samarbejdspartner blive oprettet på **PhDmUpload.au.dk** hos Datamanagement.

Dette er en krypteret web-løsning, som kan sende data direkte til Datamanagement

F.eks. en samarbejdspartner logger ind på hjemmesiden og uploader filerne.

Efter modtagelsen lægger Datamanagement data ned på dit CryptShare.

HVILKE INFORMATIONER?

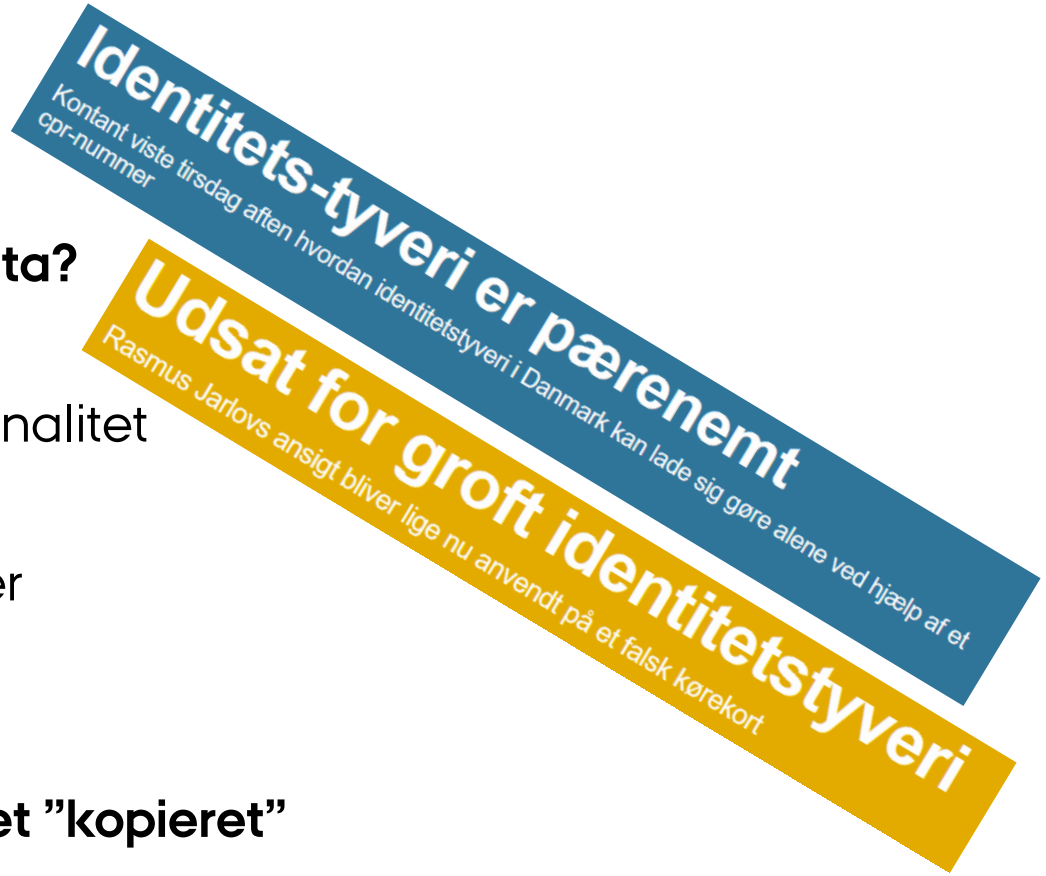
Kan vi gøre noget for at mindske risikoen?

Kan vi (om)kode vores data?

- Kan vi bruge 1, 2, 3… i stedet for cpr?
- Behøver vi at kende personers navne eller kan oplysningerne slettes?
- Kan vi bruge kommune- eller regionskoder i stedet for adresse?
- Kan vi omkode diagnoser til 1, 2, 3 i stedet for standard diagnoser?
- Kan vi inddele personer i interval-grupper?
- Har vi brug for præcise datoer og tidspunkt – eller er f.eks. alder i år nok?

Altså, brug nøglefiler til data og del ikke flere information end højest nødvendigt

INFORMATIONS TYVERIER



Jamen, er der virkelig nogen, der gider stjæle vores data?

- Oplysningerne kan bruges til svindel og anden kriminalitet
- Oplysningerne kan bruges til identitetstyverier
- Oplysningerne kan bruge til at skade andre personer
- Oplysningerne kan krænke personers privatsfære

Tyverier bliver ikke opdaget – da vi oftest bare er blevet "kopieret"

Pas på når du f.eks. videregiver dit udstyr til service
- dette kan være en videregivelse hvis der er data på enheden!

HVORFOR ER VI NERVØSE?

- Vi kan forske fordi borgerne stoler på os!
- Overhold AUs og Instituttets IT-politikker!
- Tænk over din adfærd!
- Brug AU's tilbud og faciliteter
- Kom til DM, hvis du er i tvivl

Ansvaret er dit!

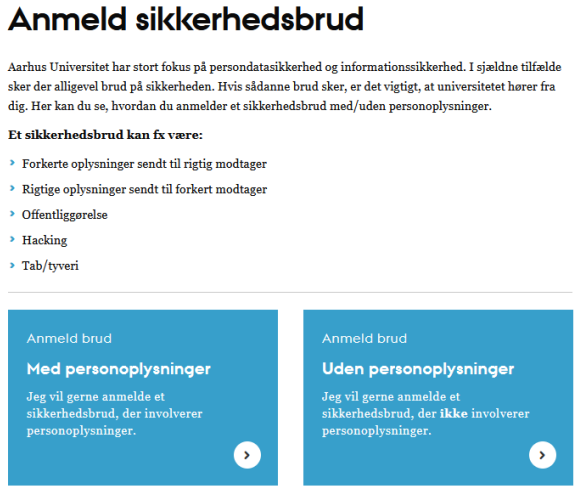
SIKKERHEDSBRUD PÅ AU

I sjældne tilfælde sker der alligevel brud på sikkerheden.

Hvis sådanne brud sker, er det vigtigt, at vi hører fra dig.

Du kan anmelde et sikkerhedsbrud via formularen her på siden:
https://medarbejdere.au.dk/informationssikkerhed/anmeld-sikkerhedsbrud/

Bliver du opmærksom på risikoer eller steder hvor datasikkerheden ikke er i orden, så sig til så problemet kan blive løst.



> Selv paranoide kan blive forfulgt
>
> - PSYKIATEREN

MEN, PÅ NETTET KAN DU VÆRE SIKKER PÅ DET!

AARHUS
UNIVERSITY