

DATASIKKERHED PÅ IFS

VERSION 4.0 2018

DATASIKKERHED PÅ IFS

Hvorfor datasikkerhed?

- På IFS arbejder vi med personhenførbare-/personfølsomme data
- På IFS arbejder vi ofte med registre med store befolkningsgruppers data
- På IFS indsamler vi ofte informationer med store befolkningsgruppers data
- IFS er underlagt GDPR – den nye 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, Michael Lund Kristensen

På Health har vi en Databeskyttelseskoordinator, Jacob Hjort

Du SKAL holde dig opdateret med indholdet på denne AU hjemmeside:

<https://medarbejdere.au.dk/informationssikkerhed>

Du SKAL gennemgå selv læringskurset:

<https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/e-laeringskursus-om-persondataregler/>

AU INFORMATIONSSIKKERHED

The screenshot displays the AU Information Security website. The header is blue with the text 'MEDARBEJDERE.AU.DK' on the left and navigation icons (AU.DK, SYSTEM, FIND, MENU) on the right. Below the header, the page title 'INFORMATIONSSIKKERHED' is shown on the left, and 'English' with a search bar is on the right. A left sidebar lists various topics under 'Databeskyttelse', including 'e-læringskursus om persondataregler', 'Generel information', 'Om administration', 'Privatlivspolitik', 'Sikkerhedsbrud på AU', and 'Til forskere'. The main content area is titled 'Databeskyttelse - beskyttelse af personoplysninger'. It features a search bar and a 'FIND' button. Below this, there are three featured articles: 'Forskningsprojekt med personoplysninger', 'Håndtering af mail', and 'Databeskyttelsesforordningen eller GDPR'. Each article has a brief description and a right-pointing arrow. To the right of the main content, there are two additional sections: 'Har du spørgsmål?' (Do you have a question?) and 'Hotline - TTO'.

MEDARBEJDERE.AU.DK

AU.DK SYSTEM FIND MENU

INFORMATIONSSIKKERHED English

Du er her: [Informationssikkerhed](#) > [Databeskyttelse](#)

Databeskyttelse - beskyttelse af personoplysninger

FIND ALFABETISK

Forskningsprojekt med personoplysninger

Indsamling af alle typer personoplysninger i forbindelse med et forskningsprojekt skal registreres på AU. Husk at du skal anmelde, inden du påbegynder dataindsamlingen.

Håndtering af mail

Find de almindelige forholdsregler for håndtering af mail på AU, og læs om hvad du må og ikke må, hvis du sender mails med følsomme personoplysninger.

Databeskyttelsesforordningen eller GDPR

EU's databeskyttelsesforordningen skal beskytte oplysninger om en identificeret eller identificerbar fysisk person. Personoplysninger skal forstås meget bredt og dækker enhver oplysning, der kan henføres til en person.

Har du spørgsmål?

Kan du ikke finde svar på dit spørgsmål, kan du finde hjælp hos AU's datateam.

Find kontaktoplysninger

Hotline - TTO

IFS INFORMATIONS SIKKERHED

MEDARBEJDERE.AU.DK

AU.DKSYSTEMFINDMENU

MEDARBEJDERE - INSTITUT FOR FOLKESUNDHED

English

Du er her: AU > Medarbejdere > Institutter > Institut for Folkesundhed > Datamanagement

» Organisation

» Forskerstøtte: Hjælp til bedre fondsansøgninger

> Personaleforhold

> Praktisk information

» Økonomi og rejser

> IT, web og telefoni

» **Datamanagement**

> Kurser

> Bestilling

> Stata licens

> Kontakt

> Kommunikation og events

» Undervisning og uddannelse

» Ph.d.-studerende

> Kontakt

Datamanagement

Om Datamanagement

Sikkerhed

DST og Retningslinjer

Vejledning om SSI

Statistikprogrammer

Databaser, dataset

Spørgeskema

Login til SurveyXact



Hent vores [præsentationsbrochure](#)

> [Kontaktinformation](#)

> **Bemærk**, vi er flyttet til [bygning 1267](#), kontor 3.18 - 3.21

> Health AU IT: [Driftstatus](#)

HENVENDELSE OM DENNE SIDES INDHOLD: [WEBREDAKTIONEN, PH](#)
REVIDERET 21.06.2018

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

AU jura gruppen, legal@au.dk

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

Hvis ikke, så er det 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?

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

HOTLINE 9352 1494

(Åbningstider: mandag, onsdag og torsdag fra kl. 10-12)

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, KiAP (DAK-E), Labka II 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 **ANMELDESEPLIGT** til Datatilsynet ved overtrædelser

ANMELDELSESPLOIGT

- Du har PLOIGT til at underrette AUs DPO ved overtrædelser
- Du har PLOIGT til at underrette Datatilsynet ved overtrædelser
- Det SKAL gives underretning til de krænkede
- Det 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 personoplysninger 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 ud arbejder på

Som udgangspunkt må kun arbejde med data på AUs udstyr

- Computere skal på **uni.au.dk** domain
- Din computer skal var 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 (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 ud arbejder på

Du må ikke lagre data i skyen, da du skal kunne redegøre for hvor data fysisk befinder sig. Mange af disse tjenester lagre 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 adgang til data. Derfor bruger vi kun AU's CryptShares, som overholder disse krav.

Med CryptShares kan du dele data internt på AU's netværk med andre personer, der har et AUID. Eksterne brugere kan få et AUID.

IT Udstyr

Der er krav til det udstyr ud 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 lokal 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 forhold kan bruges VPN, VDI og CrypShares uden overladelse.
Kontakt Datamanagement.**

OVERFØRSEL AF DATA

Når du skal overfører 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 email, 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 email i mellem fælles postkasser f.eks. Region Midt til AU.

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

Fileoverførsler 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)

OVERFØRSEL AF DATA

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 ligger 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?
- Behøves vi at kende personers navne eller kan oplysningerne slettes?
- Kan vi bruge kommune eller regions koders 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 en højest nødvendigt

INFORMATIONSTYVERIER

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!



It-sikkerheden sejler i kommunerne
Gang på gang bliver kommuner taget i at sløse med it-sikkerheden

Ukrypterede CD'er med sundhedsdata på fem millioner danskere havnede hos kinesisk firma
Middelfart kommune har lagt login-oplysninger ud til et system, der indeholder personoplysninger om handicappede borgere

Kritik: Alt for mange brist i dansk it-sikkerhed

Elendig it-sikkerhed i staten: Dine oplysninger ligger åbne for hackere
Der er unødigt stor risiko for hackerangreb på den danske stat. Det vurderer Rigsrevisionen i en ny rapport, som slår fast, at statens it-sikkerhed er utilstrækkelig

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/databeskyttelse/sikkerhedsbrud-paa-au/>

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