RETNINGSLINJERNE FOR PERSONFØLSOMME OPLYSNINGER (2016)

VER 3.0

AARHUS
UNIVERSITET

RETNINGSLINJERNE FOR PERSONFØLSOMME OPLYSNINGER

Indhold

- Hvad siger reglerne - og nye regler fra 2015?
- Sikkerhed i praksis
- Opbevaring af digitale data
- Flytning af data
- AU tiltag

HVAD SIGER REGLERNE?

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, indeholder i kapitel 12:
kilde: www.retsinfo.dk

- **”Som hovedregel skal enhver behandling af personoplysninger, som omfattes af loven, anmeldes til Datatilsynet, inden behandlingen iværksættes.”**

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

HVAD SIGER REGLERNE?

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, indeholder i kapitel 12:
kilde: www.retsinfo.dk

- ”Myndigheden skal kun anmelde de *behandlinger af personoplysninger*, som myndigheden er dataansvarlig for. Der er ingen pligt til at anmelde behandlinger, der alene omfatter anonyme oplysninger.
- Ifølge lov om behandling af personoplysninger § 3, nr. 1, forstås ved personoplysninger »enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)«.

HVAD SIGER REGLERNE?

Sundhedsvidenskabelige forskningsprojekter

kilde: http://www.datatilsynet.dk

- Ved »… sundhedsvidenskabelige forskningsprojekter er **undtaget** fra kravet om anmeldelse til og tilladelse fra Datatilsynet, hvis projektet er omfattet af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter og har tilladelse fra en videnskabsetisk komite.

- …Undtagelsen fra anmeldelse gælder kun for projekter, som foretages for en **privat dataansvarlig**. Offentlige projekter skal stadig anmeldes.

HVAD SIGER REGLERNE?

- Der kan derudover være krav om særskilte tilladelser fra diverse myndigheder SSI, LPR, DAK-E, LABKA etc.
- SSI er blevet opsplitter 1. Nov. 2015 ! Nyt Sundhedsdatastyrelsen.
- Hertil gælder Instituttets sikkerheds- og ansættelsespolitik
- **Ansvaret er dit!**

HVAD SIGER REGLERNE?

Hvordan får jeg tilladelse fra Datatilsynet?

På AU skal du kontakte og anmelde til:

- **Tove Bæk Jensen**
  tbj@au.dk
  28992554
- http://www.au.dk/videnudveksling/innovation/forskningssamarbejde/datatilsynet/

  Tilladelsen opnås på ca. 14 dage
  - Hvis ansøgningen overholer loven!

HVAD SIGER REGLERNE?

Bemærk!

Hvor gælder min tilladelse?

Den gælder i DK - og EU hvis du har spurgt om lov.

Du må f.eks. ikke tage til USA og arbejde på dine data, da du så laver en overførsel af informationerne til et 3. partsland (uden for EU).
- Gælder også Fjernskrivebord, Citrix etc.!

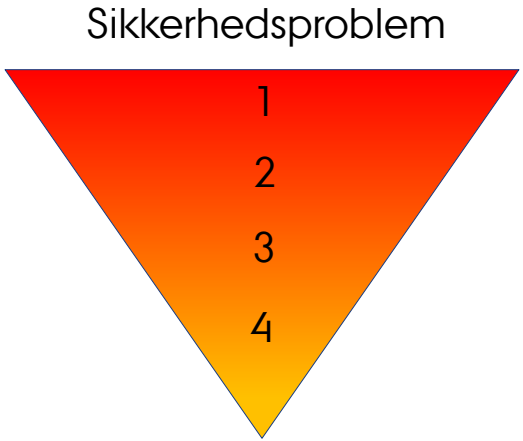
Du skal beskrive ALT, hvad du gør med data i din ansøgning.

SIKKERHED I PRAKSIS

Sikkerhed i praksis

- Hvem må se mine data?
- Hvordan sikre man sig?
- Hvordan opbevare jeg data?
- Hvordan sender jeg data?
- Er der andre løsninger?

SIKKERHED I PRAKSIS

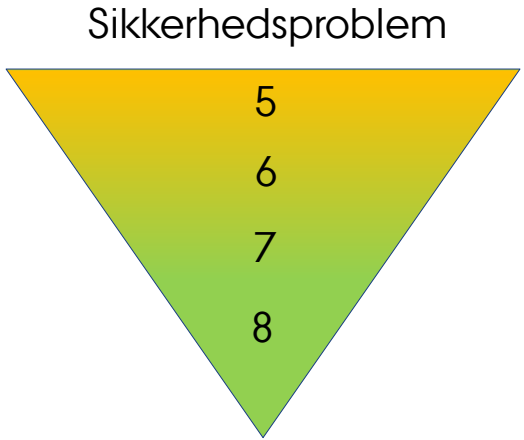


Data kan være personfølsomme på flere måder:

1. Der indgår et cpr. nummer.
2. Der indgår navn, adresse, tlf. nummer, e-mail etc.
3. Personer er med på billeder eller er på anden måde visuelt genkendelige.
4. Oplysningerne er anonyme, men enkelt personer kan afledes af data.

Betragt nummereringen, som en rangliste for størrelse af dit sikkerhedsproblem!

SIKKERHED I PRAKSIS



Der hvor vi gerne skal hen med vores data er, hvor:
(hvis det er muligt)

5. Oplysningerne er anonyme
6. Oplysningerne er ikke umiddelbart identificerbare.
7. Vi har aggregerede / grafiske fremstillinger i stedet for tabeller
8. Vi har kun statistiske resultater

SIKKERHED I PRAKSIS

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?

SIKKERHED I PRAKSIS

Hvordan ser dine data ud for andre?

Variable	Værdi	Enhed
Vægt	72	Kg
Højde	174	cm
Køn	K	K/M
Alder	41	År

	72	
	174	
	0	
	41	

- Tabelen er nem at læse for os – men også for udenforstående!
- Kategorier, variable navne, enheder etc. kan bruge som en nøgle til data

SIKKERHED I PRAKSIS

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

"En kommunen fik indbrud, fik brækket et brandsikkert skab op og fik stjålet få cpr-numre, navne, adresser etc. fra de personer, som havde bestilt et nyt kørekort i den forgangene uge."

- 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

SIKKERHED I PRAKSIS

Vi skal undgå spredning af data!

”Need to Know Security Policy”

- Hvem skal vide hvad?
- Har du styr på kopierne?
- Er alle variable i en f.eks. tabel nødvendige for andres arbejde?
- Behøves de andre tabeller - eller er f.eks. et histogram nok?

SIKKERHED I PRAKSIS

Hvem har egentlig adgang til dine data?

- Kan nogen komme ind på dit kontor og tilegne sig dine informationer?
- Er adgangen til opbevaringsstedet aflåst?
- Er informationerne låst inde i f.eks. skab, når du er på toilettet eller til kaffe?
- Låser du din computer, når du går fra den?
- Kommer der nogen, når du er gået hjem?

SIKKERHED I PRAKSIS

Hvem har egentlig adgang til dine data?

- Har du en kopi derhjemme til godnat læsning?
- Hvem holder øje med den kopi, når du er på arbejde?
- Hvad sker der, hvis nogen stjæler din PC - eller du glemmer den toget?
- Er din harddisk krypteret?
- Hvor ligger du dine nøgler?

SIKKERHED I PRAKSIS

Konklusion

- Opbevar aldrig flere oplysninger end nødvendigt!
- Tænk på: Flere låse og koder er bedre!
- **Husk: Selv om du er paranoid – så bliver du helt sikkert forfulgt!**

OPBEVARING AF DIGITALE DATA

Digitalisering gør det både nemmere for os
– MEN, også for dem, der uretmæssigt vil tilegne sig vores data!

- Hvor sker tyverierne?
- Er nogle digitale opbevaringsmedier mere sårebare end andre?
- Hvordan sender jeg data?

OPBEVARING AF DIGITALE DATA

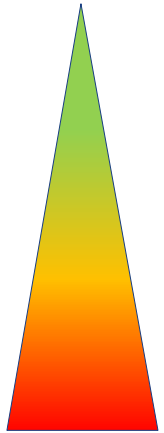
Hvor sker tyverierne?

- De fleste tyverier sker der, hvor tyven ikke behøves at være fysisk til stede
- De færrest opdager at de er blevet bestjålet (**kopieret**) – der mangler ikke noget!
- Tyverierne sker oftest der, hvor sikkerhedsniveauet er dårligst
- Tyverierne sker oftest der, hvor data ikke er krypteret, kodet etc.
- Tyverierne sker oftest der, hvor man kan søge i ditatalt i data efter oplysninger.

OPBEVARING AF DIGITALE DATA

Sikkerhedsniveauer/Sikkerhedszoner på netværk

- **Lukkede netværk,** 100% lukkede for omverden. PET, Forsvaret etc.
- **Lukkede netværk, med tunnel adgang.** DSTs forskermaskiner
- **Beskyttede netværk,** alle brugere er kendte. AU, virksomheder etc.
- **Hjemme netværk,** udefineret sikkerhed, anonym, WiFi, worms etc.
- **Hotspots,** ukendt sikkerhed, anonym, WiFi. Bus, tog, hoteller etc.
- **Internettet generelt.** Hvad der er her – det har alle, hvis de vil havde det!



OPBEVARING AF DIGITALE DATA

- **Du skal nøje overveje, hvor du befinder dig**
  - og hvor du bevæger dig hen med dine handlinger!

- **Når du får tilladelser til at opbevare, indsamle eller se på data,**
  så er der altid krav til hvor, hvem og hvordan du må bruge informationerne!

- Eksempel: DST hjemtagning af data (zone skifte)

OPBEVARING AF DIGITALE DATA

Opbevaringsmedier

Lokale medier. DVD/CD, USB-Sticks, HDD, SD Cards etc.

- Kan ikke tilgås, med mindre de sidder i en computer
- Kan fysisk stjæles, glemmes etc.
- **Slettet data kan genskabes!**
- Skal destrueres fysisk efter brug!
- Hvem tager backup?

OPBEVARING AF DIGITALE DATA

Opbevaringsmedier

Netværksdrev. AU personlig drev, AU fælles drev etc.

- Adgangskontrol – men, hvem?
- Backup – men, hvor bliver kopien af?
- Kan ikke stjæles fysisk
- Kan i teorien hackes fra internettet
- Trafikken foregår kun inden for AU's netværk.

OPBEVARING AF DIGITALE DATA

Opbevaringsmedier

Skydrev. DropBox, OneDriver, SkyDrive, Google Drev, etc.

- Tilgås via internettet !!!
- Udbyder kan kræve (betingelserne) lov til at kikke, søge i data – og bruge data !!!
- Kan ligge udenfor EU – problematisk pga. lovgivning !!! **Nu ulovligt! Også Krypteret!**
- At data trafik bliver logget af teleudbyderne, NSA + mange andre !!!
- ~~Betragtes af datatilsynet som en "databehandler" – kræver tilladelse !!!~~

OPBEVARING AF DIGITALE DATA

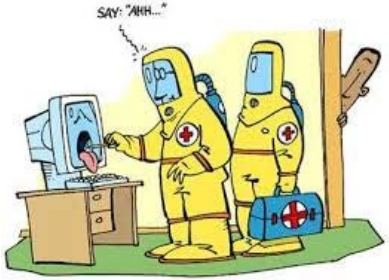
Internettet og data logninger

- Alle teleselvskaber er pålagt at logge netværkstrafik ved lov!
  Dvs. at der er kopier derude af alle dine e-mails, skydrives, download etc.
- Som eksempel på, hvor meget det logges, så kan vi bruge et tal fra NSA i US:
  I 2008 rundede NSA, alene, logning af data svarende til alle informationer, der er i kongressens bibliotek (det største bibliotek i verden).
  Det var så ikke i løbet af hele 2008 – men, i minuttet i 2008!
- "The Bad Guys" kan mindst lige så meget!

OPBEVARING AF DIGITALE DATA

Uha! – Jeg bliver bare på min egen PC

- Din PC kan være på nettet:
  a) **Så er døren åben for hackning, loggers, trackers, hijackers, malware etc.**
  b) Dine data bliver måske, uden du ved det, kopieret til nettet af "backup" programmer etc.
- Din programmer kopiere dine data til f.eks.
  a) Undo-data for at du kan lave "fortryd". Disse data ligger f.eks. skjult i Word-filer.
  b) Gemmer kopier data i lokale file, der er optimeret for hurtig databehandling.
  c) Gemmer kopier i Windows "swap" fil.
- Din PC bliver stjålet!
- Din PC går i stykker og bliver sendt til reparation!



OPBEVARING AF DIGITALE DATA

Kryptering – de nye krav

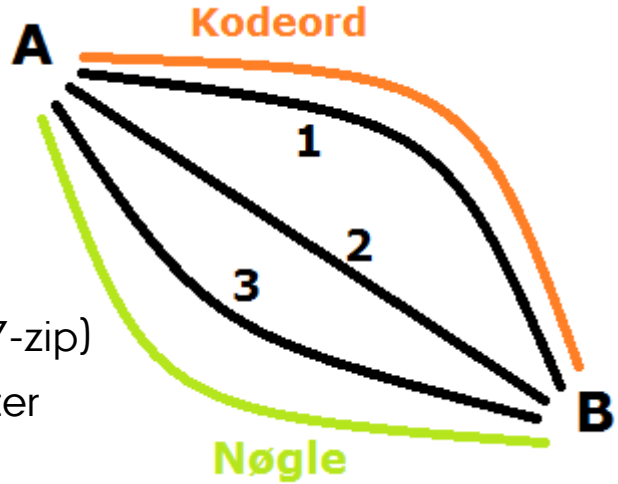
- Alle bærbare enheder skal være krypterede!
- Alle overførsler af data skal være krypterede!
- Databaser skal være krypterede!
  - hvad er en database og en overførsel?
- Filservere skal ikke med, der er en masse indirekte krav
  - nemmeste løsning er kryptering!
  AU klar med kryptering og nye krypterede netværksdrev (CrypShares)!

FLYTNING AF DIGITALE DATA

Hvad gør vi så?

- Huske – mindst mulig information!
- Huske – **"Need to Know Security Policy"**
- Og gør det samme som er gjort siden oldtiden:

1) Krypter det hele og del pakken op i små bider (7-zip)
2) Send pakkerne forskudt i tid og ad forskellige ruter
3) Send krypteringsnøglen for sig
4) Aftal et ekstra mundtligt kodeord



FLYTNING AF DIGITALE DATA

Selv om den nævnte metode er rimelig sikker og meget besværligt at bryde, så er intet, der er mere sikkert end at lade være!

VI SENDER ALDRIG DATA MED CPR-NUMRE !!!

via e-mails, skydrev, ftp etc., heller ikke selv om de er krypterede, opdelte etc.

Her skal der som minimum bruges en VPN-adgang.

- og data skal stadig være krypteret, opdelt etc.

Eller en kurer, taxa eller lign. f.eks. en krypteret DVD er også en mulighed!

HVAD TILBYDER AU

VPN / Fjernskrivebord / Citrix
Kryptering af alle PC'er og bærbare
Krypteret filserver – CryptShares!
Krypterede USB nøgler i webshoppen
Krypteret Web (SSL) / Secure FTP
Statens Sikre Email (Logiva)
Mobiler – TouchDown for SmartPhones
Destruktion på Bartholin og Tandlægeskolen.

OPSAMLING

- 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!

AARHUS
UNIVERSITET