IT-Ansvar

God skik – og ansvarlighed

Persondataforordningen

Jørgen Granborg

a·data
software til sundheden

Hvem er jeg…

- Direktør i
  - A-Data
- Bestyrelses formand i
  - DMDD A/S
  - Nasure A/S
  - PLSP A/S
- Formand for PL-Forum

- og hvorfor beskæftiger jeg mig så med

IT-Ansvar

Persondataforordningen

God skik og ansvarlighed

a·data
software til sundheden

Vi kommer langt omkring

- Dine egne
- Dine patienter
- Persondataforordningen
- De helt klare no-go

a·data
software til sundheden

Er det dyrt?

- Købe

Ja

- Bøde

Det kan det blive

- Tænke

Men det behøver det ikke at være

a·data
software til sundheden

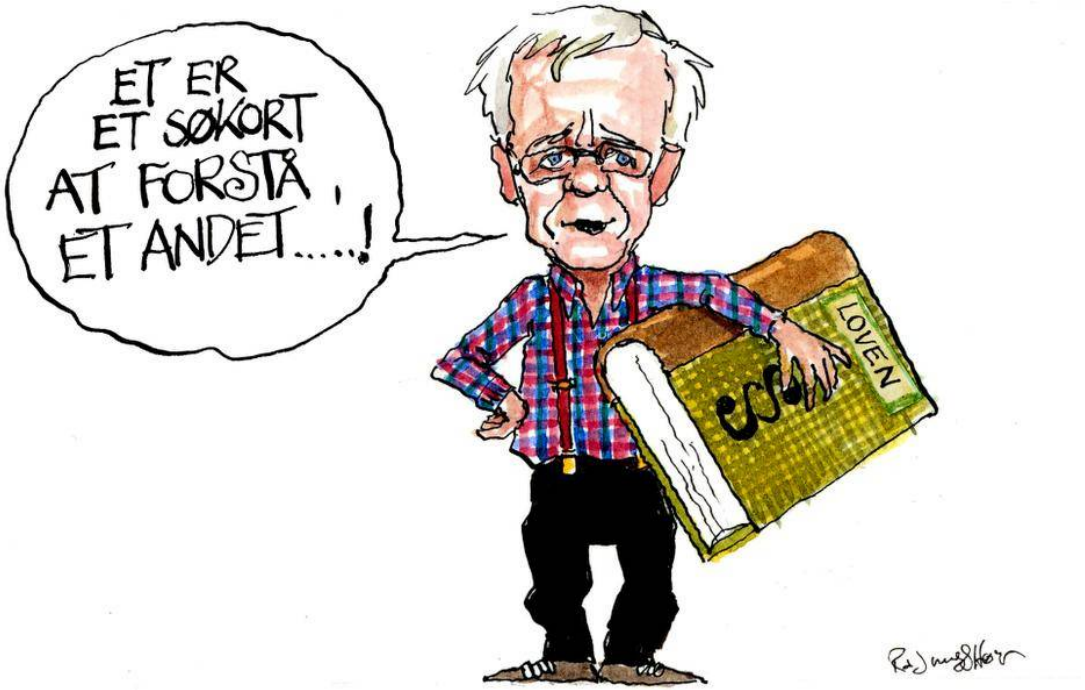
Bøder - sanktioner

Følgende sanktioner kan blive pålagt:

- en skriftlig advarsel i tilfælde af førstegangs- og ikke-tilsigtede brud
- krav om jævnlige tilsyn
- en bøde på op til 10.000.000 EUR eller, for virksomheder, op til 2% af forrige regnskabsårs totale årlige omsætning på verdensbasis. Største beløb gælder (Artikel 83 stk. 4 [5]))
- en bøde på op til 20.000.000 EUR, eller, for virksomheder, op til 4% af forrige regnskabsårs totale årlige omsætning på verdensbasis. Største beløb gælder (Artikel 83, Afsnit 5 og 6[5])

a·data
software til sundheden

Det handler om sund fornuft



a·data
software til sundheden

Og
ansvarlighed

a·data
software til sundheden

Alle de ord – og hvad ligger bag

a·data
software til sundheden

Dataansvarlig

I persondatalovens § 3, nr. 4, defineres "*den dataansvarlige*" som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

a·data
software til sundheden

Databehandler

I persondatalovens § 3, nr. 5, defineres en ”*databehandler*”, som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

a·data
software til sundheden

Personfølsomme oplysninger

En personfølsom oplysning er en oplysning om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Med den nye forordning omfattes også genetiske og biometriske* data.

*biometriske data: personoplysninger om fysiske karakteristika, såsom ansigtsbillede eller fingeraftryksoplysninger.

a·data
software til sundheden

Databehandleraftale

En dataansvarlig kan vælge at overlade det til en anden at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne. Den, der herefter udfører databehandlingen, betegnes som databehandler. En databehandler kan være en (fysisk) person, en virksomhed, en offentlig myndighed etc.

Databehandleren må ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

Behandlingen ved en databehandler kræver, at der indgås en skriftlig aftale herom imellem den dataansvarlige og databehandleren (en såkaldt databehandleraftale).

Den ansvarlige er altid ansvarlig – uanset aftale

a·data
software til sundheden

Databehandler aftale

Hvem skal i have en databehandler aftale med – sådan ret praktisk:

- Jeres tandlægesystem
- De samarbejdspartnere – der udfører opgaver der indebærer at de behandler personfølsomme data for jer

Den kommende tid vil blive mere skarp på dette, nogen siger

Revisorer, "Danmark" m.fl. Andre siger nej – mit råd er at se hvad tiden viser – og spørge.

Tandlægeforeningen og Datatilsynet har lavet glimrende forslag til databehandleraftaler.

a·data
software til sundheden

Samtykke

- Samtykke er et aktivt tilvalg
- Samtykket er formuleret i et klart og enkelt sprog, som er letforståeligt for en person i målgruppen
- Samtykket specificerer formålet med den påtænkte behandling af data
- Navnet på den/de dataansvarlige fremgår af samtykketeksten
- I oplyser om muligheden for at trække samtykket tilbage
- I kan dokumentere, hvem der har givet samtykke, hvornår og hvordan samtykket blev givet, hvad den enkelte har samtykket til, og at samtykket reelt er afgivet frivilligt, og I følger regelmæssigt op på, at samtykket stadig er aktuelt og korrekt, og at formålet med behandlingen eller selve behandlingen ikke har ændret sig

Vejledning om samtykke

a·data
software til sundheden

Dine egne

[Datatilsynets FAQ]

a·data
software til sundheden

Dine ansatte

- Bruger du billeder på hjemmesiden
- Overvåger du de ansattes internetbrug
- Overvåger/læser du e-mails adresseret dine medarbejdere
- Videoovervågning
- Personalearkiv

a·data
software til sundheden

Din arbejdsplads, dit ansvar

- At pc'en er opdateret med seneste version af antivirus – PR-013
- At undlade at notere password på papir og lign
- At undgå kollegaer ser du taster dine passwords
- At personlige passwords ikke må udlånes/oplyses til andre
- At logge af domæne og telefon, når pc'en forlades
- At slukke pc'en når arbejdstid ophører
- Ikke at udveksle personfølsomme data (ukrypteret) via email, messenger, chat mm

Din udleverede **pc/tablet må kun anvendes til arbejdsmæssige formål.**

a·data
software til sundheden

Dine ansøgere

Når du modtager stillingsansøgninger, giver det mening at fortælle dine interne om retningslinjer.

At gemme ansøgninger kræver samtykke.

Forespørgsler andre steder og at gemme oplysninger kræver samtykke.

a·data
software til sundheden

Dine patienter

a·data
software til sundheden

Kommunikation

- E-mail – no-go – cpr-nummer
- Ingen helbredsoplysninger
- Ingen forsikrings oplysninger

- Samtykke skal registreres ved videregivelse
- Klare linjer

a·data
software til sundheden

Persondataforordningen (GDPR)

25. Maj 2018

a·data
software til sundheden

Hvem er omfattet

Som udgangspunkt vil de nye regler finde anvendelse på alle, der foretager behandling af personoplysninger, dvs. både offentlige myndigheder, organisationer og virksomheder. Også virksomheder uden for EU kan blive omfattet, bl.a. hvis de tilbyder varer eller tjenester til borgere i EU. Dette er en vigtig nyskabelse i forhold til forordningens rækkevidde. De nye regler favner altså bredt, og ***reelt vil alle virksomheder skulle forholde sig til de nye regler***

a·data
software til sundheden

Vigtigste ændringer

- *et større ansvar og flere forpligtelser i forbindelse med behandlingen af*
- *"privacy by design"/"privacy by default".*
- *nogle virksomheder skal udpege eller ansætte en såkaldt DPO*
- *flere rettigheder til den registrerede fx "retten til at blive glemt" og "retten til dataportabilitet.*

a·data
software til sundheden

DPO – hvem skal

- Hvis man er en offentlig myndighed (undtagen domstole)
- Hvis man er en virksomhed, hvis primære ydelse er at behandle persondata, som forudsætter jævnlig og systematisk overvågning af de registrerede personer
- Hvis man er en virksomhed, hvis primære ydelse er at behandle ”særlige kategorier af oplysninger” om registrerede personer, fx politisk tilhørsforhold, helbredsoplysninger, seksuel orientering etc.
- Selvom i som klinik opfylder disse krav, så er der sat en størrelses begrænsning ind, så som udgangspunkt skal klinikker IKKE have en DPO.
- Dog giver det mening at en række af de opgaver der ligger hos en DPO lægges hos en medarbejder i klinikkerne, således at man sikrer sig at ansvaret for de rutiner klinikken har, ligger hos en og samme person.

a·data
software til sundheden

DPO opgaver

DPO’ens primære opgave er via rådgivning og overvågning at sikre organisationens overholdelse af persondataforordningen og interne politikker om beskyttelse af personoplysninger.

a·data
software til sundheden

DPO opgaver

- Holder opsyn med korrekt databeskyttelse
- Rådgivning og anbefalinger mht. rettigheder og forpligtelser ift. databehandling
- Håndterer registrerede personers forespørgsler vedr. deres persondata
- Holder ledelsen orienteret om dens forpligtelser i forhold persondataloven
- Fungerer som primær kontaktperson for tilsynsmyndigheder (fx Datatilsynet)
- Er ansvarlig for at overvåge datalæk, og give besked til relevante myndigheder om eventuelle læk af persondata
- Dokumentation af offentlige og lovgivningsmæssige krav til bortskaffelse og destruktion af data, samt tilgang til data.

a·data
software til sundheden

Anbefalinger – at komme i gang

- Vælg ansvarlig (DPO)
- IT-håndbog
- Beskriv data geografi
- Skriv til samarbejdspartnere – og opbevar svaret
    - Forsikringsselskaber og sikrer jer at de varetager samtykke
    - Samarbejds parter som varetager opgaver for jer skal i have en databehandleraftale med – hvis i tvivl så spørg dem.

a·data
software til sundheden

Anmeldelsesordning

Databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018.

Som noget nyt stiller forordningen krav om, at alle dataansvarlige og databehandlere fører interne fortegnelser over deres behandling af personoplysninger.

Fortegnelseskravet erstatter således den hidtil gældende anmeldelsesordning.

a·data
software til sundheden

Databehandleraftale

Du er ansvarlig, og du **skal** have en

Databehandleraftale

med dit journalsystem – og den skal indeholde en beskrivelse af, hvilke opgaver de varetager for dig,

...og uanset hvad, så er det stadig dit ansvar.

a·data
software til sundheden

I klinikken

- Antivirus
- Router opdatering
- Opdatering af operativsystemer servicepacks
- Opdatering programmel
- Brug af mobiltelefon

a·data
software til sundheden

Server – låst fast

Har du fysisk adgang til en server, er du meget tæt på at få adgang til data.

a·data
software til sundheden

Adgangskoder

- Fortrolige – personlige
- Min. 12 tegn – gerne en sætning
- Skiftes en gang imellem
- Slettes ved ophør
- Kun adgang til det nødvendige
- <Win><L> giver god mening

a·data
software til sundheden

Tavshedspligt – fortrolighed

a·data
software til sundheden

Tavshedspligt

Du har adgang til

Personfølsomme data

men tavshedspligten gælder alt.

a·data
software til sundheden

Tavshedspligt

Din tavshedspligt gælder

under og efter

din ansættelse

a·data
software til sundheden

Personfølsomme data

- Kan ikke fortryde
- Svært at undskylde
- Svært at udbedre tab

a·data
software til sundheden

Datatilsynet – svigt skal meldes

Din IT-ansvarlige tager opgaven

Jeres sikkerhedshåndbog skal fortælle om retningslinjer – og have en procedure for, hvad der skal gøres i tilfælde af svigt

a·data
software til sundheden

Husk

- Makulér altid materiale med CPR numre/personhenførbare oplysninger uden ophold
- Undgå at bruge mails til at udveksle personhenførbare oplysninger
- Hvis nødvendigt skal de sendes i krypterede vedhæftninger
    - **Slet hurtigst muligt**
- Undlad at udveksle/diskutere personhenførbare oplysninger med kollegaer

a·data
software til sundheden

Logning

- Min log på sundhed.dk
- Retssager
- Ansvarlighed

a·data
software til sundheden

Hvem kan hjælpe

De bedste til det er

Dit tandlægesystem

De kender din klinik – de leverer de fleste af jeres IT-ydelser – de er bedst klædt på til det.

a·data
software til sundheden