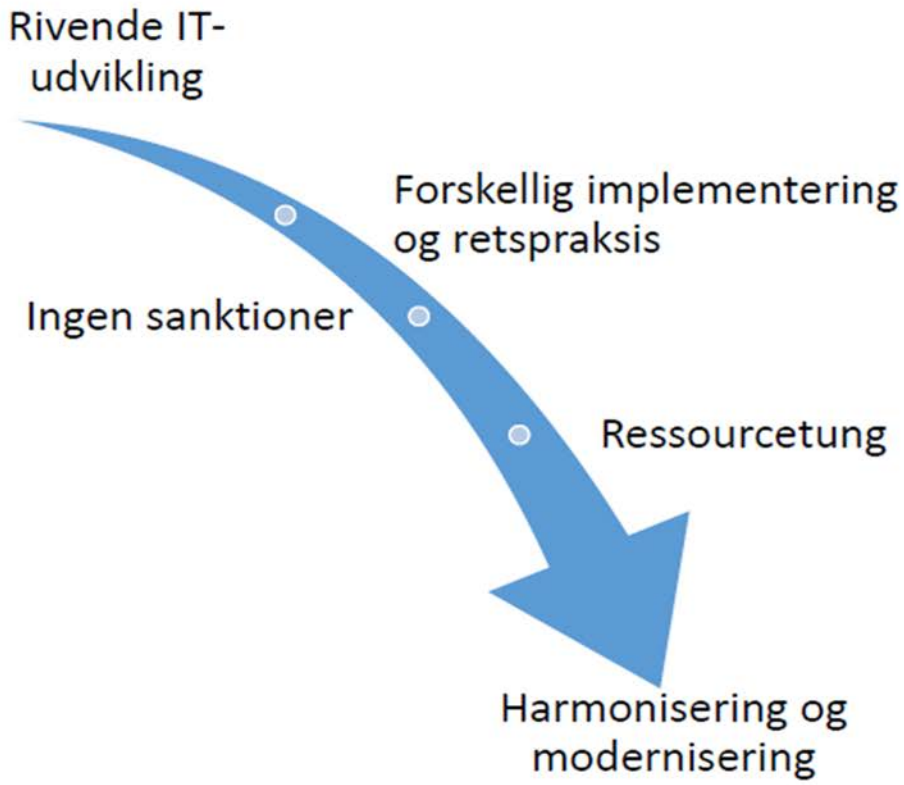
Datasikkerhed -beskyttelse af personoplysninger

HR- og fagchef, cand.jur. Isabel Brandt Jensen

Fokus

- Hvorfor persondatabeskyttelse?
- Persondataforordning fra EU
- Særlovgivning
- Hvad skal du huske?
- Persondataloven – grundlæggende betingelser
- Personaleadministration – HR
- Roller og ansvar
- Sikkerhedsbrist – bøder
- Udfordringer
- Vejledninger fra Datatilsynet og info på Tdlnet

Hvorfor persondatabeskyttelse ?



Hvorfor persondatabeskyttelse ?

Civilingeniør og sikkerhedsekspert: »YouSee-nedbrud ligner intern hacking«

Ifølge TDC har det krævet detaljeret viden om YouSees platform og opsætning at lægge kabeltv-netværket ned. Den formulering peger mod intern sabotage, lyder det fra teknisk direktør hos sikkerhedsfirma.

Jesper Stein Sandal @jespersandal Torsdag, 5. januar 2017 - 14:27 16

FØLG VERSON2

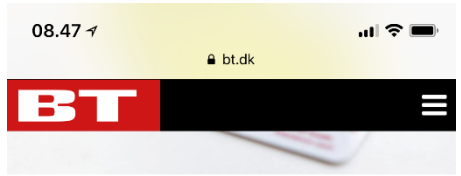
Fem millioner danske CPR-numre sendt til kinesere ved en fejl

Af Fannie Isabel Couderc Pramming og /ritzau/
20. juli 2016, 13:57 – **opdateret** 20. juli 2016, 16:21

En brev der indeholdt personfølsomme oplysninger blev ved en fejl

Datatilsynet fortalte Novo Nordisk om datalæk: Lagde testside online ved en fejl

Medicinalgiganten opdagede først læk af persondata fra 95.000 jobsøgende, da Datatilsynet henvendte sig.



Arkivfoto. **Foto: Jonas Skovbjerg Fogh**

BO POULSEN FØLG

To personer fra Odense har fået tilsendt en liste med 38 personers fulde navn, cpr-nummer, kundenummer og hvad de skylder kommunen for levering af ældremad.

Det skriver Fyens.dk.

»Det er er simpelthen så langt ude. Hvis det kan ske der, hvor kan det så ske?,« siger en kvinde, der mistede sin mor sidste år, til avisen. Fyens.dk har valgt at anonymisere kvindens identitet.

Kvinden modtog en regning fra kommunen for moderens gæld for ældremad - først i e-boksen og derefter i postkassen.

Og det var her, at listen med de personfølsomme oplysninger fulgte med.

Særlovgivning

- **Journalbekendtgørelsen § 15**. Læger, tandlæger, kiropraktorer, jordemødre, kliniske diætister, kliniske tandteknikere og tandplejere skal opbevare deres patientjournaler i mindst 10 år (opbevaringsperioden), jf. dog stk. 5.

Særlovgivning

- **Journalbekendtgørelsen § 18** Patientjournaler skal opbevares forsvarligt, og det skal sikres, at uvedkommende ikke har adgang til oplysningerne i patientjournalerne.
- Stk. 2. Ved anvendelse af papirjournaler skal der anvendes materialer og metoder, som er egnede til at sikre optegnelsernes holdbarhed.
- Stk. 3. Ved anvendelse af elektroniske patientjournaler skal det ved løbende sikkerhedskopiering sikres, at optegnelserne ikke tilintetgøres, fortabes eller forringes.
- Stk. 4. I lov om behandling af personoplysninger (persondataloven) § 41 er der fastsat regler om krav til datasikkerheden i forbindelse med behandling af personoplysninger.

Persondataforordning EU

- Endeligt vedtaget den 14. april 2016 i Europa-Parlamentet
- **Får virkning fra 25. maj 2018**
- Forordning, så direkte virkning i medlemsstaterne – dvs. ingen national implementeringslov
- Forventet øget harmonisering på tværs af EU – "ens" sanktionering
- MEN der åbnes op for nationale særregler på en lang række områder

Rådet for
Den Europæiske Union

UDKAST til forslag til lov om supplerende bestemmelser til forordning

- Databeskyttelsesforordningen og databeskyttelsesloven regulerer området for behandling af personoplysninger fra den 25. maj 2018.
- Persondataloven og sikkerhedsbekendtgørelsen (for offentlige myndigheder) bliver dermed ophævet.

Forordningens anvendelsesområde, jf. Art 2:

- Personoplysninger
- Automatisk databehandling (hel eller delvis)
- Ikke-automatisk databehandling i registre (struktureret samling af personoplysninger.

Compliance-tjek

På dansk – hvad skal du huske…

- Intern fortegnelse
- Dataflow*
- Konsekvensanalyse/Risikoanalyse*
- Dokumentation – beskrive lovhjemmel, procedurer
- HR-dokumentation
- Nødvendige tiltag? Handlingsplan.
- Vedligeholdelse

Hvilke persondata behandles?

- Undersøg og dokumenter
- Krav om intern fortegnelse over behandling af personoplysninger
- Hvor kommer data fra – dataflowanalyse
- Hvilke data deles og med hvem?
- Dataansvarlige skal implementere passende sikkerhedsforanstaltninger af teknisk og organisatorisk karakter for at sikre et sikkerhedsniveau, der er proportionelt med de risici, som er forbundet med persondatabehandlingen – husk risikoanalyse.

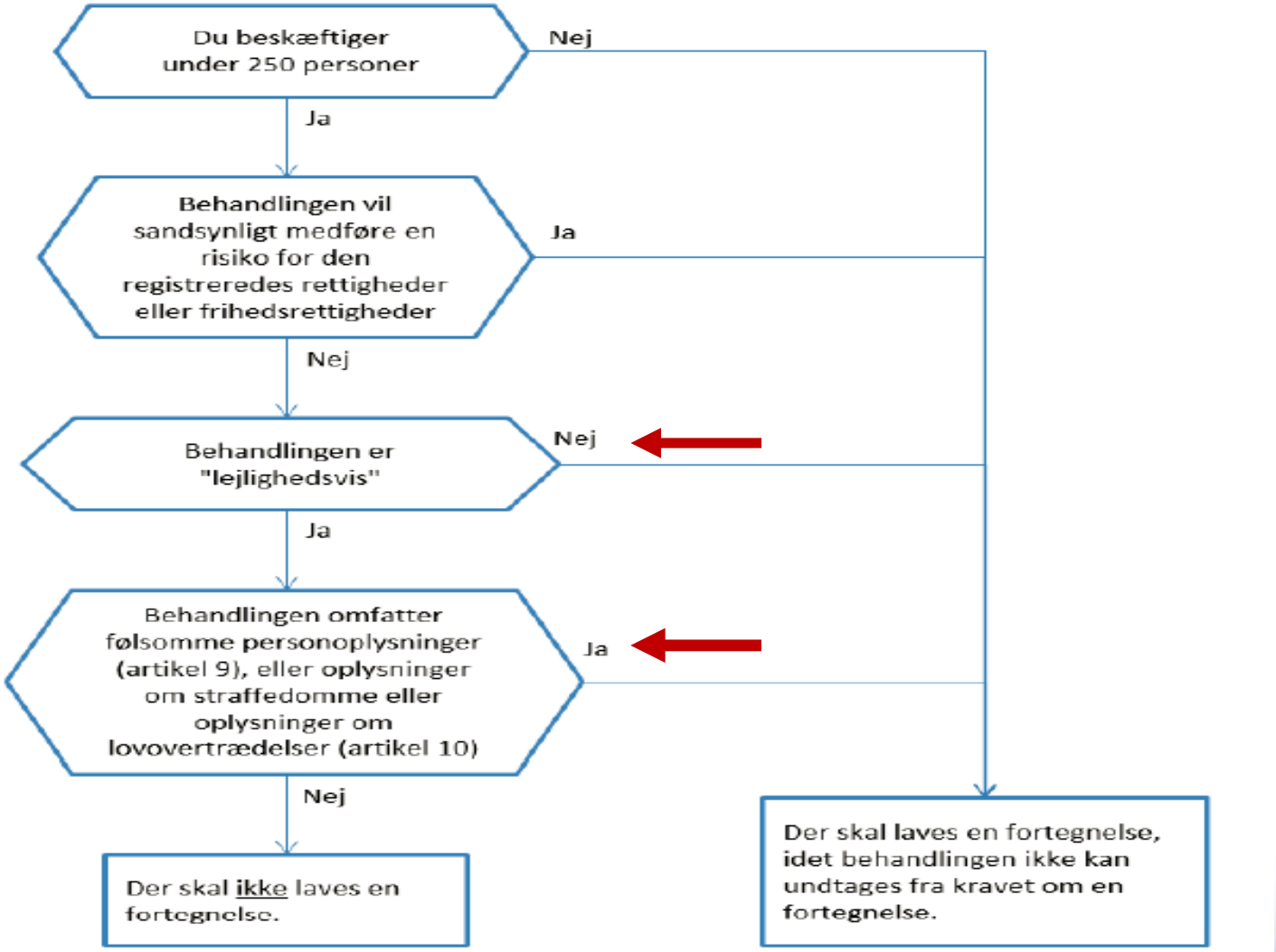
Intern fortegnelse over databehandlingsaktiviteter

- Fortegnelser skal foreligge skriftligt og elektronisk.
- Ikke udelukkende føre fortegnelsen i et fysisk dokument eller efter hukommelsen.
- Følg Datatilsynets vejledning om fortegnelser:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_fortegnelse__endelig___DOK461184_.PDF

- Fokus på at udvise ansvarlighed
- Dokumentation og overblik
- Al behandlingsaktivitet

Er du undtaget fra fortegnelseskravet?



Kilde:
Datatilsynet


Pilenes tykkelse = omfang/brug
Klinikkens dataflow
Tandklinikken
Hospitalsafdeling
Henvisning til kæbekirurg
Kommunal tandpleje
Kommunal sagsbehandler
Usikker mail og brev fra pt.
Patienter
Sikker mail EDI-portal
EDI-portal
Eboks erhverv
Sikker mail Brev
Tandlægeforeningen
Sikker mail
EDIfact std
Sikker mail Brev
Sikker mail Brev
Regionens afregning Sygeforsikringen Danmark
Patienter
Sikker mail Brev
Sikker mail EDI-portal USB/brev
Sikker mail
Tandteknikker
Sikker mail USB/brev
Forsikringsselskab
Klinisk tandteknikker
Anden klinik (journal overdragelse)
Regionen Klager

Organisatoriske foranstaltninger - dokumentation

- Persondataforordningen stiller krav om passende organisatoriske foranstaltninger.
- Dokumentation af dette for at kunne føre kontrol
- Politikker for god databehandling
- Procedurer til brug for god databehandling
- Beskrivelse af processer med udgangspunkt i god databehandling
- Interne processer til løbende evaluering af effektiviteten af ovenstående processer, politikker mv.
- Procesbeskrivelse for underretning om sikkerhedshændelser
- Forankring af ansvar for enkeltprocesser, generelle politikker mv.
- Kontroller, der sikrer, at processer, politikker, retningslinjer mv. er ajourførte og overholdes.

Tekniske foranstaltninger

- Politikker for anvendelse af kryptering, herunder type af kryptering
- Politikker for anvendelse af pseudonomisering, herunder type af pseudonymisering
- Politikker for sikring af adgangskontrol
- Procesbeskrivelser til sikring af anonymisering

Personoplysninger

- **Definition:** ”Enhver form for information om en identificeret eller identificerbar fysisk person”
- **Identificerbar:** ”fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en online-identifikator eller andet, der er særlige for personens fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet”

Fx: oplysninger om fysiske personer – hårfarve, bopæl, alder, arbejdsplads, genetiske oplysninger, billede, uddannelse, mv., oplysninger om kontaktpersoner hos samarbejdspartnere – fx e-mailadresse el. stilling.

Almindelige eller personfølsomme oplysninger ?

- Økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, Stilling, arbejdsområde, arbejdstelefon, stamoplysninger: Navn, adresse, fødselsdato, e-mail adr. væsentlige sociale problemer, andre rent private forhold, herunder ulykkestilfælde, bortvisning, personlighedstest etc.
- CPR-NUMMER § 11 stk. 2 i databeskyttelsesloven
- Race eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller om oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Hvornår må man behandle personoplysninger ?

- ✓Samtykke
- ✓Opfyldelse af kontrakt som den registrerede er part i eller gennemførsel af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af kontrakt
- ✓Retlig forpligtelse
- ✓Beskyttelse af vitale interesser
- ✓Nødvendig for at udføre opgave i samfundets interesse
- ✓Forfølge legitim interesse

Hvornår må man behandle følsomme personoplysninger ?

- HO = forbud
- U1: Arbejdsretlige forpligtelse, DBL § 7, stk. 2
- U2: Sundhedstjenester undergivet tavshedspligt DBL § 7, stk. 3

Samtykke

- Frivilligt – uden tvang og baseret på reelt og frit valg. Videre kan ”klar” skævhed mellem den registrerede og den dataansvarlige bevirke, at samtykke ikke er frivilligt, navnlig hvor den dataansvarlige er en offentlig myndighed, ligesom samtykke ikke er frivilligt, hvis afgivelse er en betingelse for opfyldelse af en kontrakt eller ydelse af en tjeneste,
- Specifikt – hvilke oplysninger og til hvad
- Informeret – hvem behandler og hvordan
- Utvetydigt (nogen gange udtrykkeligt) – der skal ikke være tvivl om afgivelse eller omfanget af et samtykke

Samtykke

- Ikke stiltiende eller indirekte - mulighed for udøvelse af kontrol gennem samtykke
- Ikke krav om skriftlighed, men den dataansvarlige har bevisbyrden, jf. Art 7, stk. 1, så praktisk – ved følsomme oplysninger nok også nødvendigt
- Den registrerede kan til enhver tid trække sit samtykke tilbage, jf. Art 7, stk. 3, OG man skal oplyse om denne mulighed i forbindelse med indhentelse af samtykke

Grundlæggende betingelser

- God databehandlingskik
- Kun til udtrykkeligt angivne og saglige formål
- Relevante, tilstrækkelige og aktuelle oplysninger
- Ajourføring
- Oplysninger arkiveres, slettet eller anonymiseres, når der ikke længere er behov for identifikation
- *Når opbevaringspligten efter* journalføringsbekendtgørelsen *ophører træder persondatalovens regler i kraft og sundhedspersonen skal derfor vurdere, om det er relevant og nødvendigt at opbevare journalen i længere tid.*

Persondataloven – personaleadministration

- 12 specifikke minimumskrav fra Datatilsynet for personaleadministration i overensstemmelse med persondatalovens gældende regler for datasikkerhed

https://www.datatilsynet.dk/erhverv/personaleadministration/krav-om-datasikkerhed-i-forbindelse-med-personaleadministration/

Særligt om behandling af oplysninger om medarbejdere

- Alle oplysninger kan behandles hvis samtykke
- Uden samtykke kan AG behandle de almindelige joboplysninger som er nødvendige for at administrere ansættelsen (navn, arbejdsområde, titel osv.)
- Adgangen til at behandle semifølsomme og følsomme oplysninger er snæver, hvis der ikke er et samtykke fra medarbejderen

Ved sikkerhedsbrist

- Er der som følge af et sikkerhedsbrist opstået en høj risiko for krænkelse af de registreredes rettigheder, har virksomheden som hovedregel en pligt til at anmelde dette til tilsynsmyndigheden uden unødig forsinkelse og om muligt senest 72 timer efter bruddet, ligesom de registrerede skal gives besked om sikkerhedsbristet uden ugrundet ophold.
- Hvis man vælger ikke at anmelde og underrette har Datatilsynet en række beføjelser.

Hvad er et sikkerhedsbrud ?

- Før du anmelder det skal du kunne identificere det.
- ”Hændeligt eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til PERSONOPLYSNINGER, der er omfattet af forordningens def. af et brud på persondatasikkerheden”.
- Se eksempler i Datatilsynets vejledning

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Hvad er konsekvenserne?

- Tab af kontrol over personoplysninger for den registrerede
- Identitetstyveri
- Finansielle tab
- Tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt
- Skade på omdømme

Anmeldelse og underretning ?

- *En klinik bliver udsat for ransomware, da en medarbejder trykker på et link i en e-mail, som er modtaget i klinikkens indbakke.*
- *Dette resulterer i, at al klinikkens data, herunder helbredsoplysninger om patienterne bliver krypteret og låst for klinikkens medarbejdere. Bagmændene kræver et større pengebeløb for at frigive oplysningerne.*
- *Klinikken har foretaget backup af sine systemer, men det er også lykkes bagmændene at kryptere disse.*
- *Klinikken har i deres systemer oplysninger om ca. 1200 aktive patienter og 600 ikke-aktive, herunder oplysninger om patienternes diagnoser.*

Bødernes størrelse

- Enkeltpersoner kan klage til datatilsynet eller indbringe en klage for domstolene
- Den dataansvarlige blive pålagt en bøde på op til 20 million euro eller op til 4 % af sin samlede årlige omsætning
- Bøde eller fængsel indtil 6 måneder, jf. DBL § 41

Roller og ansvar

Dataansvarlig er:

- Den fysiske eller juridiske person, der bestemmer til hvilke formål og med hvilke midler, behandlingen foretages
- Den dataansvarlige skal have en skriftlig aftale med sine databehandlere
- Har fortsat ansvaret for at få lavet databehandleraftale

Databehandler er:

- Den fysiske eller juridiske person, der behandler oplysninger på den dataansvarliges vegne
- Databehandleren må ikke
  - Benytte persondata til egne selvstændige formål
  - Kun hvad den dataansvarlige har bedt om

Udfordringer i dag - databehandleraftaler

- Indledende risikovurdering
- Kontraktforhandling – ingen reel afklaring af, hvilke data, der indgår, hvilke sikkerhedskrav, der skal være gældende mv.
- Intet eller mangelfuldt overblik over
  - underdatabehandlere
  - overførsler til tredjelande
  - overholdelse af sikkerhedskrav
  - databehandlerens brug af data til egne formål
- Kontrol ?
- Databehandler er ikke ”klar”

Patientjournaler
=
sundhedsoplysninger
=
høj risiko

Koder, antivirus,
backup, sikker mail

Risiko for tandlægen?

Risiko for pt.?

Udfordringer i dag - Back-Up

- Daglig sikkerhedskopi, backup
- Kontrol af data
- Verifikation af brugbare data
- Årlig kritisk restore?

Udfordringer i dag - Mail

Offentlige myndigheder: Mails skal sendes via sikker mail krypteret, hvis de indeholder personfølsomme eller semi-følsomme oplysninger.

Private: Ikke opsat samme regler MEN Datatilsynet anbefaler ovenstående følges.

Fra tandlægerne:

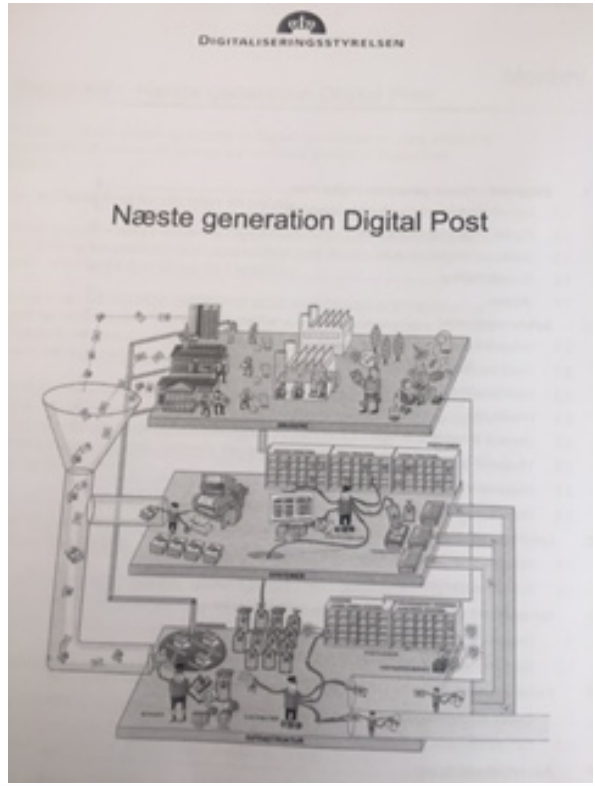
https://stps.dk/da/afgoerelser/afgoerelser-fra-styrelsen-for-patientsikkerhed/behandlingssager/2017/17sps09/

(overtrædelse af tavshedspligt)

Sikker mail

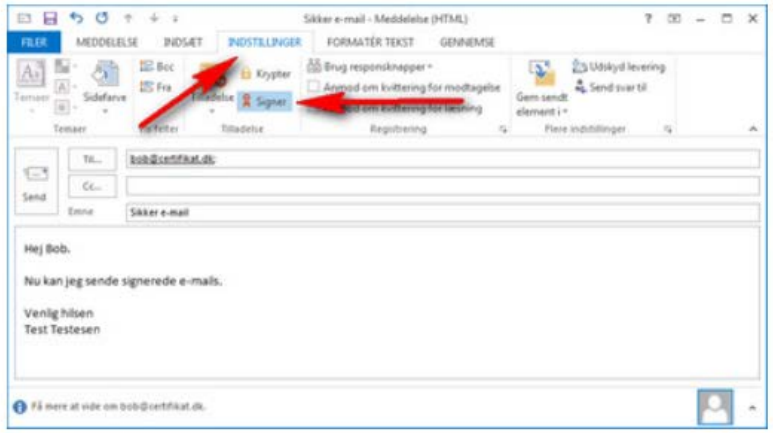
- (Privat) NemID er det samme log-in alle steder. Uanset om du vil bruge din netbank eller din kommunes online selvbetjening

- (Erhverv) NemID medarbejdersignatur - kan du identificere dig som medarbejder i en organisation eller virksomhed



Sikker mail

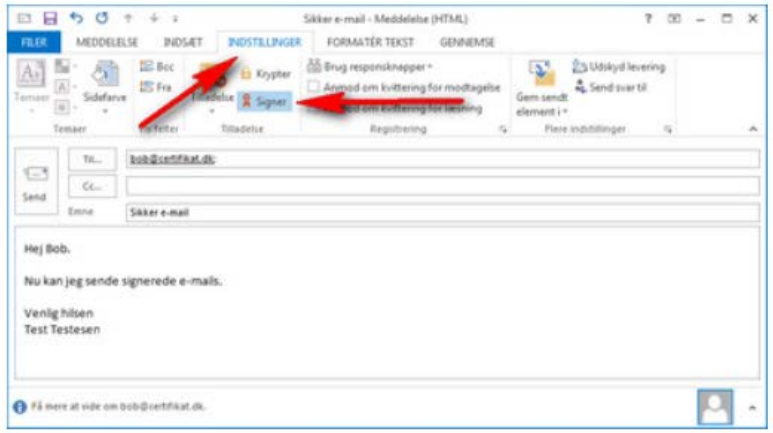
Signering



- Når modtageren skal være sikker på, at du er afsenderen
- En signering med dit NemID er modtagerens garanti for, at e-mailen er skrevet og sendt af dig
- Indholdet af meddelelsen er som standard ikke krypteret
- – og alle kan læse din e-mail
- https://www.nemid.nu/dk-da/support/brug_nemid/send_og_modtag_sikker_e-mail/opsaetning_af_e-mail-program/windows_8/outlook_2013/

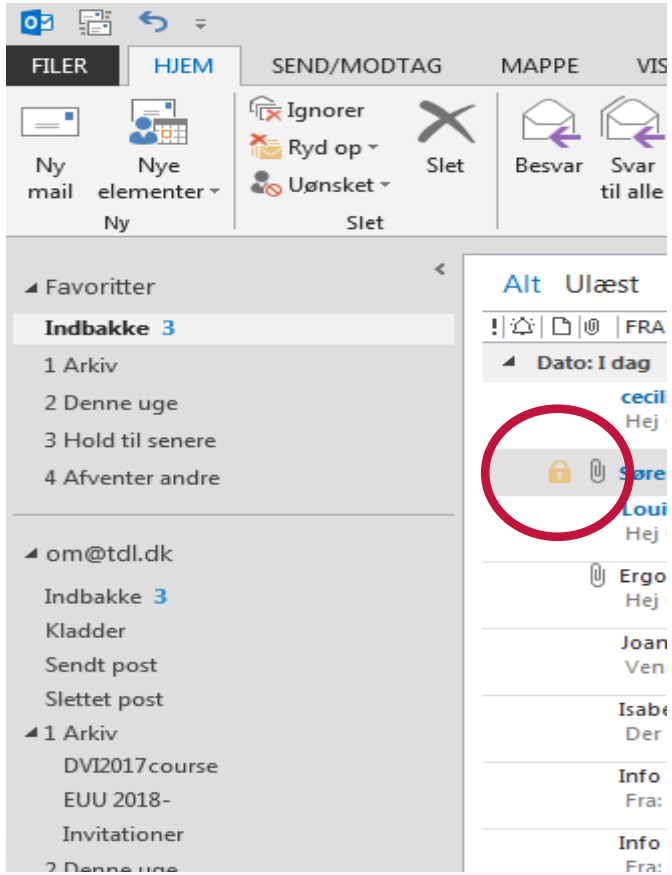
Sikker mail

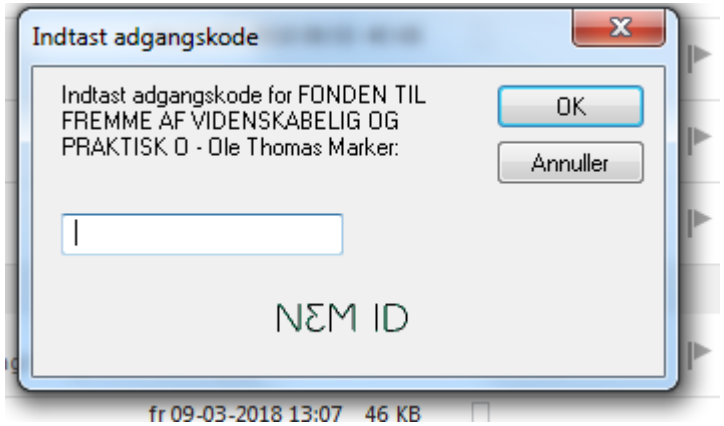
Kryptering

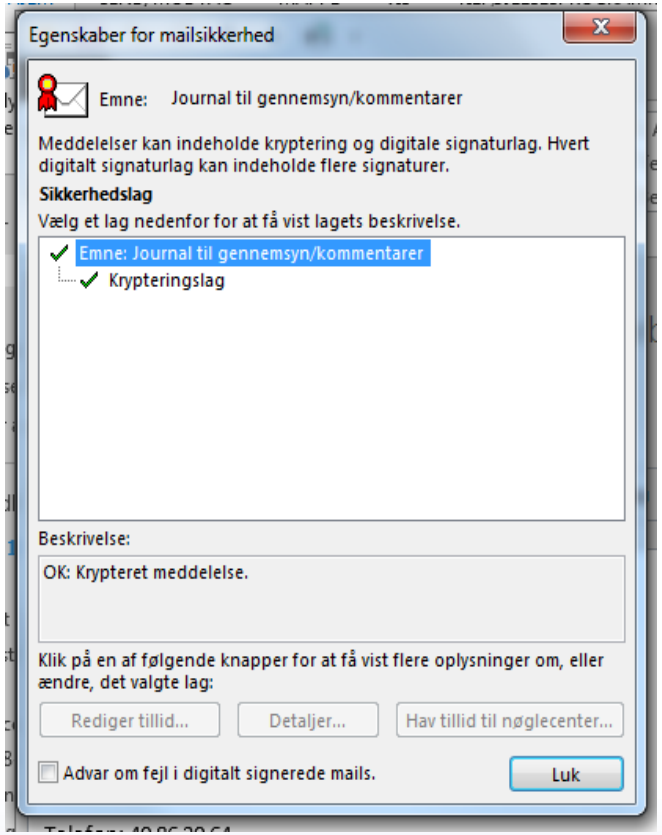


- Når ingen uvedkommende må læse din besked
- Certifikatet i modtagerens NemID bruges til at kryptere en e-mail, som kun modtageren skal kunne læse
- Når du modtager en signeret e-mail, kan du gemme afsenderens certifikat i din adressebog, så du senere kan sende en krypteret e-mail denne person

Kryptering


FILER
HJEM
SEND/MODTAG
MAPPE
Ny mail
Nye elementer
Ignorer
Ryd op
Uønsket
Slet
Besvar
Svar til alle
Ny
Slet
Favoritter
Indbakke 3
1 Arkiv
2 Denne uge
3 Hold til senere
4 Afventer andre
om@tdl.dk
Indbakke 3
Kladder
Sendt post
Slettet post
1 Arkiv
DVI2017course
EUU 2018-
Invitationer
Alt
Ulæst
Dato: I dag


Indtast adgangskode
Indtast adgangskode for FONDEN TIL FREMME AF VIDENSKABELIG OG PRAKTISK O - Ole Thomas Marker:
OK
Annuller
NEM ID
fr 09-03-2018 13:07 46 KB


Egenskaber for mailsikkerhed
Emne: Journal til gennemsyn/kommentarer
Meddelelser kan indeholde kryptering og digitale signaturlag. Hvert digitalt signaturlag kan indeholde flere signaturer.
Sikkerhedslag
Vælg et lag nedenfor for at få vist lagets beskrivelse.
Emne: Journal til gennemsyn/kommentarer
Krypteringslag
Beskrivelse:
OK: Krypteret meddelelse.
Klik på en af følgende knapper for at få vist flere oplysninger om, eller ændre, det valgte lag:
Rediger tillid...
Detaljer...
Hav tillid til nøglecenter...
Advar om fejl i digitalt signerede mails.
Luk

FAQ

Hvem kan man sende sikre mails til?

- En mail der ikke er krypteret, men kun er digitalt signeret kan læses af alle.
- En mail der er krypteret kan kun læses af den modtager, hvis nøgle er blevet anvendt til at kryptere mailen med.
- Det er således kun muligt at sende krypterede mails til modtagere, der har en krypteringsnøgle.
- Man kan finde og hente krypteringsnøgler:

https://service.nemid.nu/dk-da/support/soeg_certifikat/

For at sende journaler sikkert og korrekt?

- Sikker mail – Pdf format…
- Via journalsystemet til samme udbyder
- E-boks (offentlige)
- 3. part software – **ikke et krav**

DPO (databeskyttelsesrådgiver)

- Som udgangspunkt ikke krav om DPO for tandklinikker i privatpraksis.
- Offentlige myndigheder skal udpege en DPO

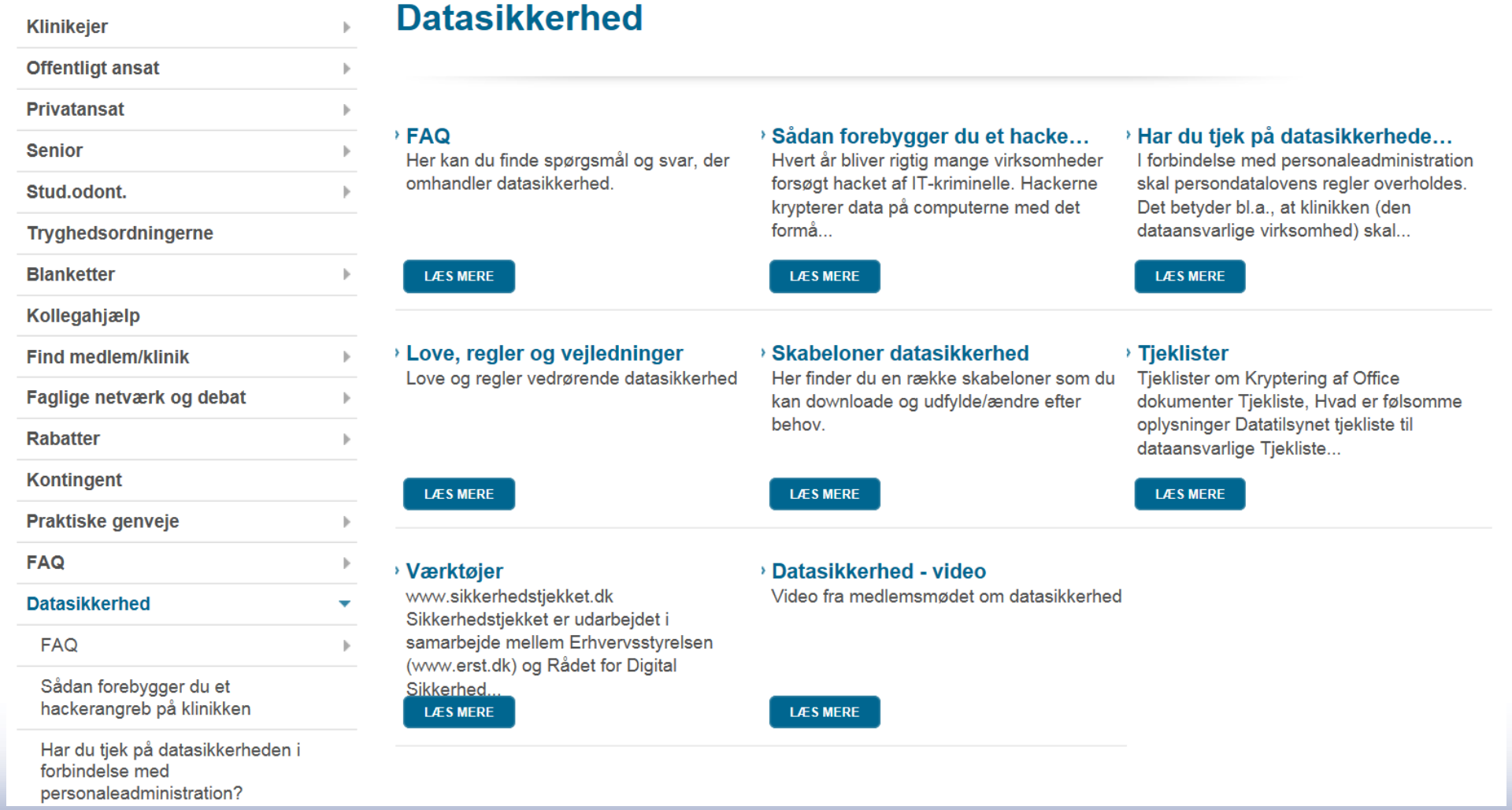
Følgende tre betingelser skal alle være opfyldt:

  - Behandling af personoplysninger skal være virksomhedens kerneaktivitet
  - Der skal behandles personoplysninger i et stort omfang
  - Behandlingsaktiviteten består i regelmæssig og systematisk overvågning af personer eller

- Behandlingen vedrører følsomme oplysninger eller oplysninger om strafbare forhold

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf

Brug Tdlnet.dk



Datatilsynet & Ministeriet (JM)

- Har udgivet en række spørgsmål svar:
- https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/Datatilsynets_FAQ.pdf
- Vejledninger fra JM, Datatilsynet og artikel 29 udvalget.
- www.dbreform.dk

Spørgsmål