Databeskyttelses-forordningen i Region Hovedstaden

Forretningsudvalgsmøde

8. maj 2018

Kort om mig

- Cand. Jur. 1996
- Videnskabsministeriet (bl.a. ministersekretær for Helge Sander)
- KPMG, It Advisory og Legal Services (senior legal manager)
- Labora Legal (advokatfuldmægtig og advokat)
- Region Hovedstaden, Center for It, Medico og Telefoni (chefkonsulent)
- Region Hovedstaden, Sekretariatet (DPO)

Persondatalovgivningen pr. 25. maj 2018

- Databeskyttelsesforordning og databeskyttelsesloven
- Erstatter eksisterende persondatalovgivning
- Erstatter sektorspecifik lovgivning (fx sundhedsloven)? Nej
- Ny lovgivning?

Hvorfor ny persondatalovgivning?

- Teknologisk udvikling og globalisering har skabt nye udfordringer ift beskyttelsen af personoplysninger - sikkerhedstrusler
- Indsamling og deling af personoplysninger er steget betydeligt
- Behov for en stærk og sammenhængende databeskyttelsesramme, som understøttes af effektiv retshåndhævelse
- Lovgivning fra 1996
- Facebook, Google – ”the right to be forgotten”
- Uensartet anvendelse og håndhævelse
- Øget fokus på privacy og værdien af data
- Øget fokus på data fra alle fronter – politikere, borgere, it-kriminelle

Trusler

- Hverdagens trusler:
  - Tekniske problemer
  - De ondsindede – hackere
  - Den menneskelige faktor – os selv

Hvad er nyt?

Nye tiltag

- Sammenhængsmekanisme
- Administrationen/tilsynet
- Ændring i mindset
- Bøder
- Databeskyttelsesrådgiver (DPO)
- Notifikationspligt

Skærpelser

- Øget dokumentationskrav (accountability)
- Risikobaseret tilgang
- Konsekvensanalyser
- Databeskyttelse – Privacy by Design /by Default (nævnes eksplicit)
- Rettigheder (”forgotten”)
- Øgede krav til databehandlere

DPO

- Data Protection Officer / Databeskyttelsesrådgiver
  - Rollen er lovmæssigt defineret
  - Har en central **rådgivnings- og overvågningsrolle** i regionen
  - Skal inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger - PbD mv.
  - Rapporterer (**underrette**) til øverste ledelsesniveau (Regionsrådet)
  - Kontaktpunkt for Datatilsynet
  - Skal være uafhængig/uvildig og må ikke modtage instrukser vedr. udførelsen af sine opgaver
  - Samarbejder tæt med CISO (Informationssikkerhed)

DPO-funktion i Region Hovedstaden

- DPO-funktion:
  - DPO + 2 medarbejdere
  - DPO-ambassadører/partnere
- Daglig funktion
  - 1 linje: Lokal rådgivning (lokale jurister eller medarbejdere med særlig viden om databeskyttelse)
  - 2 linje: DPO-ambassadører/partnere
  - 3 linje: DPO
  - 4 linje: Eksternt tilsyn

Fokuspunkter

- Internt
  - Databeskyttelse skal tænkes ind i de daglige sagsbehandlingsrutiner og **arbejdsprocesser** (ændring i mindset)
  - Generelt kompetenceløft
  - Klar ansvarsfordeling
  - Privacy by Design
  - Opfølgning og handling
- Eksternt
  - Mere - politisk - debat om databeskyttelse og anvendelse af persondata


Pssst...
husk de gode vaner.
Vi passer godt på borgernes personlige oplysninger

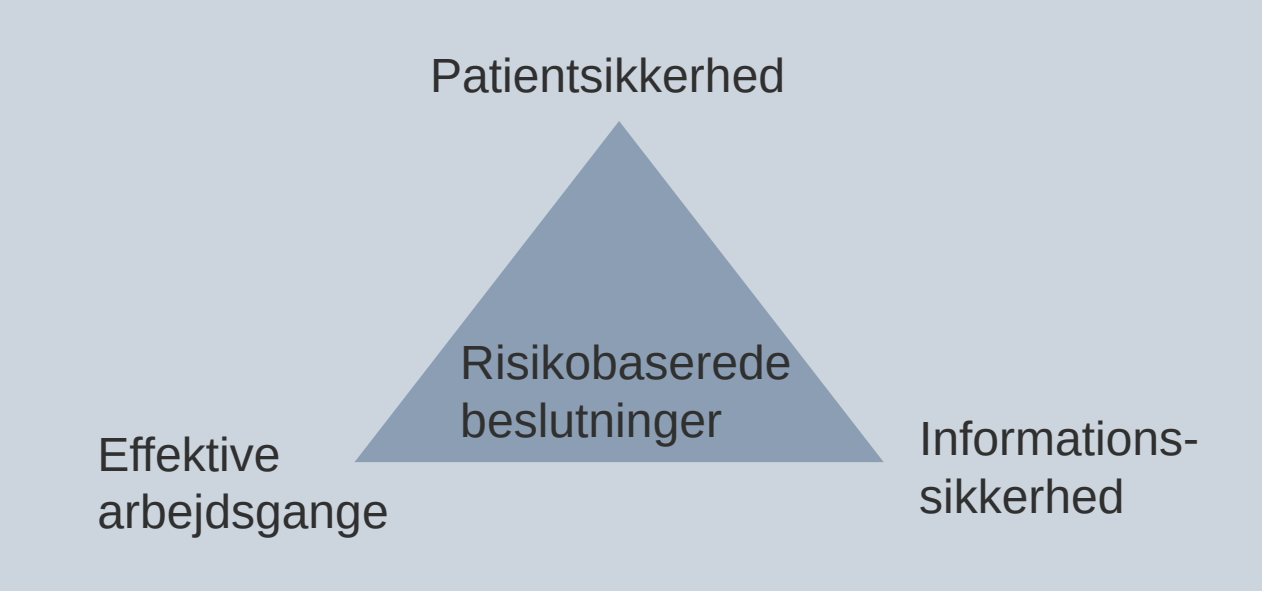
Implementeringen af forordningen

- Dokumentationskrav
  - Kortlægning, skabeloner, procedurer, vejledninger og politikker
- Data de rigtige steder - oprydning i opbevarede data
  - Drev og mailbokse
- Gennemgang af systemer
  - Risikovurdering og databehandleraftaler

Informationssikkerhed fremover

- At passe på patienten er også at passe på deres oplysninger – awareness
- Styrkelse af de tekniske sikkerhedsforanstaltninger – sikring mod angreb
- Årlig drøftelse af informationssikkerhed i Forretningsudvalget og Regionsrådet
  - Forelægges i tredje kvartal 2018

Dilemmaer – konkrete afvejninger



- Hent kun oplysninger om personer i regionens it-systemer, hvis du har et professionelt formål med det.
- Gem og opbevar følsomme personoplysninger om borgere, patienter og medarbejdere i de it-systemer, der er indrettet til det
- Opbevar ikke e-mails med fortrolige og følsomme personoplysninger i din postkasse i mere end 30 dage.
- Kommuniker ikke om borgere, patienter og medarbejdere på sociale medier, hvor regionen ikke har kontrol med data
- Brug aldrig uautoriserede fildelingstjenester og internet services som for eksempel Dropbox til arbejdsfiler med personoplysninger.
- Brug altid Digital Post til sikker og krypteret mail, når du sender beskeder med personoplysninger til modtagere uden for Region Hovedstaden
- Del aldrig dit personlige bruger-id og adgangskode med andre.
- Lås eller log af den computer, du arbejder ved, når du forlader den
- Vær diskret. Husk at anonymisere personoplysninger, hvis fx du anvender screendumps fra et it-system i en præsentation eller andet materiale.
- Vær opmærksom, når du håndterer dine e-mails: Klik ikke på links og åbn ikke vedhæftede filer i mistænkelige mails.

Spørgsmål