Personoplysninger

- **Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)**

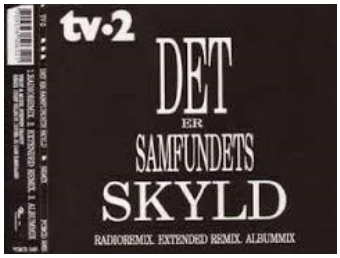
- **Vi bør have kontrol over vores personoplysninger.**
- **Det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig**

Jens Hørlück

- Cand. Oecon
- 1975-82 Landbrugets EDB Center
- 1982-2009: Adjunkt/lektor ved AU - Institut for Økonomi.
- 2009: Projektleder ved Aarhus Universitet IT
- 2014: Pension

- Undervisning og forskning i "IT for økonomer"
  - Informationsanalyse
  - IT økonomi
  - Projektledelse – især IT projekter
  - IT infrastruktur
  - Persondata har været med siden registerloven (1979)

Jens Hørlück – mine holdninger



”Det er ~~samfundets~~ skyld”
Ledelsens

Jens Hørlück – mine holdninger

- **Det er ledelsens ansvar**
- **Desværre har ledelsen ofte holdninger som:**
  - **”IT er teknik”**
  - **”Hvor svært kan det være”**

KMD's pladsanvisningssystem har været utæt i 12 år.

Nu: Brud på persondatalovens §41 stk. 3. → **FY**

Forordning:

- Kommunernes ansvar, at persondata behandles korrekt
  - Bødestraf til kommunerne - Måske
  - Kommunerne skal på forhånd dokumentere, at de har sikret sig og har aftalerne på plads
  - Mulighed for regres ???
- KMD kendte hullet i lang tid
  - Bødestraf til databehandler (op til 2% af omsætning)
  - Skal anmeldes indenfor 72 timer – ellers særskilt bøde

E-mail

- En sagsbehandler sender personfølsomme oplysninger via E-mail til en person udenfor kommunens net.
- Klar overtrædelse, både af nugældende lov og af forordningen
  - Men fremover kan kommunen idømmes bøde. (Måske)
- Det er kommunens ansvar at ansatte kender reglerne og følger dem.

EU persondataforordning – gælder fra 25. maj 2018

- Erstatter EU's persondatadirektiv fra 1995
  - Direktiv: omsættes til nationale love
  - Danmark: Persondataloven fra 2000
  - Stor forskel på national lovgivning – og praksis - i EU / EØS
- Forordning: direkte virkning i alle EU/EØS lande
- Direktivet fra 1995 forældet
  - Mail, Web, Cloud, mobil teknologi….
  - "Alle" er på
  - Internationalisering af databehandling
  - Store globale IT virksomheder
  - ….

General Data Protection Regulation (GDPR) – 88 sider

Præambel Formål og indledende betragtninger (173 punkter – 30 sider)	Kapitel I Generelle bestemmelser Art. 1-4	Kapitel II Principper Art. 5-11
Kapitel III Den registreredes rettigheder Art. 12-23	Kapitel IV Dataansvarlig og databehandler Art. 24-43	Kapitel V Overførelse af personoplysninger til tredjelande Art. 44-50
Kapitel VI Uafhængige tilsynsmyndigheder Art. 51-59	Kapitel VII Samarbejde og sammenhæng Art. 60-76	Kapitel VIII Retsmidler, ansvar og sanktioner Art. 77-84
Kapitel IX Bestemmelser vedrørende specifikke behandlingssituationer Art. 85-91	Kapitel X Delegerede retsakter Art. 92-93	Kapitel XI Afsluttende bestemmelser Art. 94-99

EU persondataforordning – gælder fra 25. maj 2018

- Dansk særlovgivning vedr.
  - Undersøgelser i strafferetlige sager
  - Statens sikkerhed
- Specielle særregler (meget få)
  - Mulighed for bødestraf til offentlige myndigheder
    - Lovforslaget siger nej
    - Flertal i folketinget for et ja
  - CPR nummers specielle stilling fastholdes

Stramninger

	Persondata loven	Forordningen
Ident	Identificerede oplysninger	Identificerbare oplysninger
Reaktionstid indsigt	- **snarest** - hvis ikke inden 4 uger, skal der gives besked - Ingen absolut grænse	- **uden unødig forsinkelse**. - senest en måned efter - I meget komplekse sager max 2 måneder
Reaktionstid - Rettelser - Sletning	- **Snarest** - God forvaltningsskik	**- uden unødig forsinkelse**
Gebyr ved indsigt	Kan kræves – max 200 kr	Gratis

Persondata - ændringer

	Persondata loven	
Almindelige oplysninger	Personnavn • Adresse • E-mail	
Semi følsomme	Strafbare forhold Sociale problemer Andre rent private end følsomme oplysninger	
Følsomme	Race eller etnisk baggrund • Politisk, religiøs eller filosofisk overbevisning • Fagforeningsmæssige tilhørsforhold • Oplysninger om helbred eller seksuelle forhold	
Cpr nummer	Aldrig offentliggørelse uden samtykke	

Persondata - ændringer

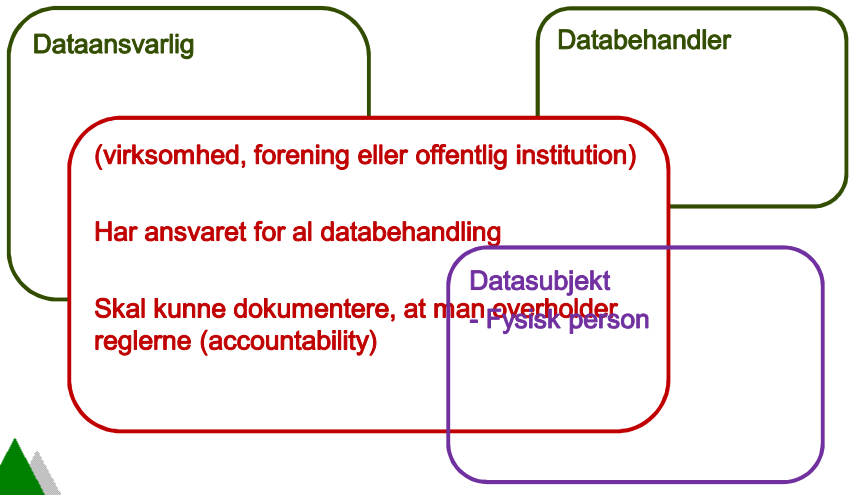
	Persondataforordning	Behandling
Almindelige oplysninger	Personnavn Adresse E-mail +oplysninger, der ikke er nedenfor	Alm. behandlingskrav
Rent private	Strafbare forhold Sociale problemer Andre rent private oplysninger	Forskel på private og offentlig behandling
Følsomme	Race eller etnisk baggrund Politisk, religiøs eller filosofisk overbevisning Fagforeningsmæssige tilhørsforhold Oplysninger om helbred eller seksuelle forhold Behandling af genetiske eller biometriske data med henblik på unik identifikation	Forbudt – medmindre - Led i lovbestemt behandling - Udtrykkeligt samtykke
Cpr nummer	*Aldrig offentliggørelse uden samtykke*	*Dansk særlovgivning herom*

Behandling er kun lovlig, hvis

- Den registrerede har givet samtykke til et eller flere specifikke formål.
- Nødvendig af hensyn til udførelse af en opgave, som er i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

- Nødvendig af hensyn til **opfyldelse af en kontrakt**, som den registrerede er part i.
- Nødvendig for at overholde en **retlig forpligtelse**, som påhviler den dataansvarlige.
- Nødvendig for at **beskytte den registrerede**s vitale interesser.
- Nødvendig for, at den dataansvarlige kan **forfølge en legitim interesse**, med mindre den registreredes interesser går forud

Roller i henhold til forordningen

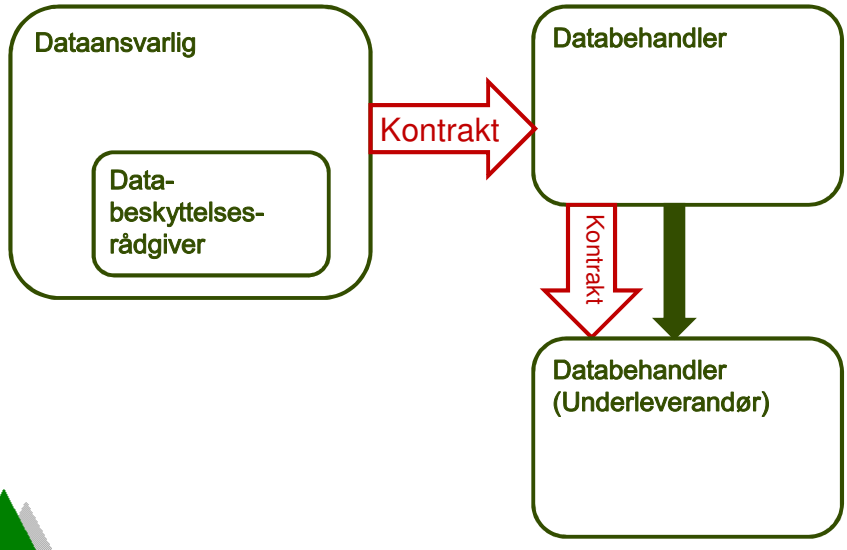


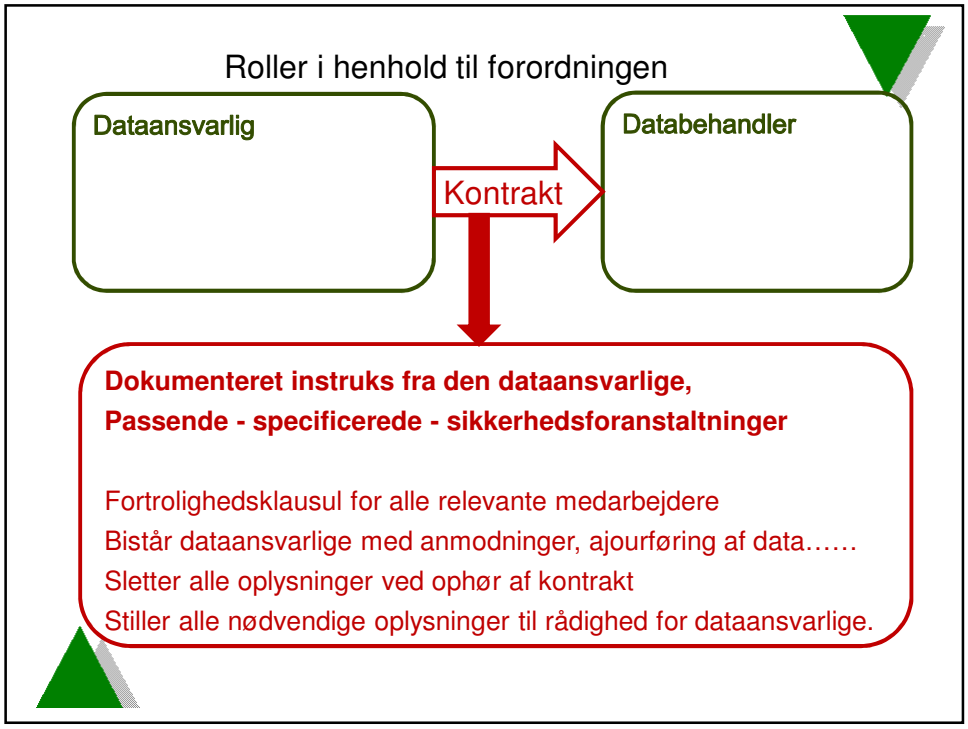
Roller i henhold til forordningen

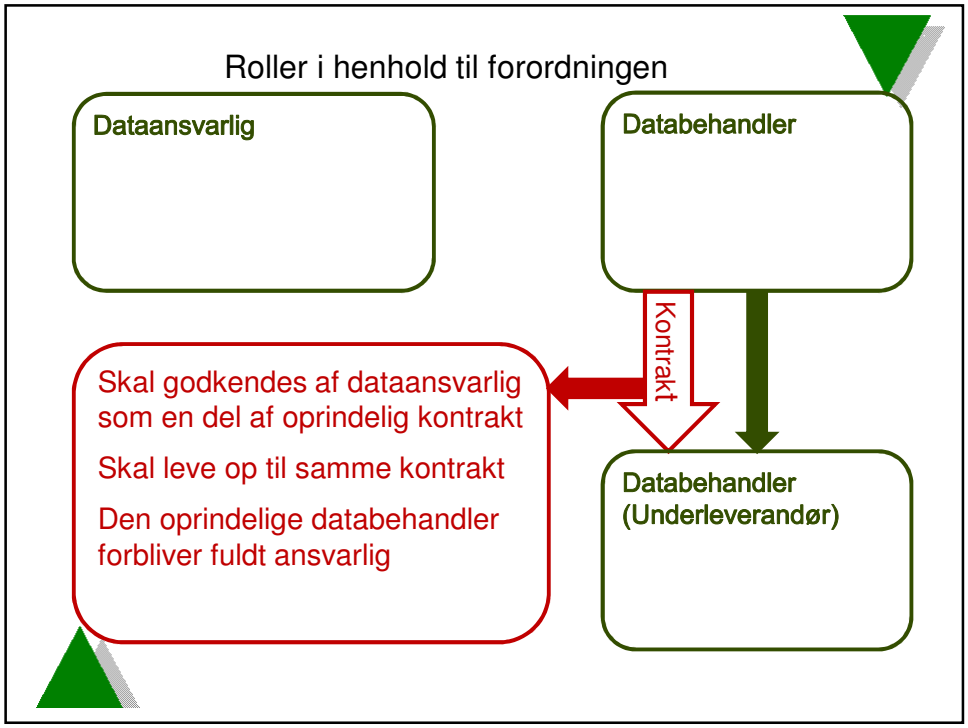
Dataansvarlige skal sikre at personoplysninger

- behandles lovligt, rimeligt og på en gennemsigtig måde,
- indsamles til udtrykkeligt angivne og legitime formål,
- er tilstrækkelige, relevante og begrænset til det nødvendige
- er korrekte og om nødvendigt ajourførte,
- kun opbevares, så længe det er nødvendigt i henhold til formålet
- behandles på en måde, der sikrer tilstrækkelig sikkerhed.

Roller i henhold til forordningen




Roller i henhold til forordningen
Dataansvarlig
Kontrakt
Databehandler
Dokumenteret instruks fra den dataansvarlige,
Passende - specificerede - sikkerhedsforanstaltninger
Fortrolighedsklausul for alle relevante medarbejdere
Bistår dataansvarlige med anmodninger, ajourføring af data……
Sletter alle oplysninger ved ophør af kontrakt
Stiller alle nødvendige oplysninger til rådighed for dataansvarlige.


Roller i henhold til forordningen
Dataansvarlig
Databehandler
Kontrakt
Skal godkendes af dataansvarlig
som en del af oprindelig kontrakt
Skal leve op til samme kontrakt
Den oprindelige databehandler
forbliver fuldt ansvarlig
Databehandler
(Underleverandør)

Roller i henhold til forordningen

Dataansvarlig

Data-beskyttelses-rådgiver

Skal findes i offentlige institutioner – kan være fælles

Skal findes i private virksomheder, hvor persondata er en del af kerneaktiviteten og som behandler i stort omfang

Skal være fagligt kvalificeret

Skal inddrages – tilstrækkeligt og rettidigt

Skal have tilstrækkeligt med ressourcer til at gennemføre sit arbejde

Roller i henhold til forordningen

Dataansvarliges ansvar

Databehandlers ansvar

Privacy by design og privacy by default

Pligt til at orientere Datatilsynet og i nogen tilfælde også de registrerede i tilfælde af datasikkerhedsbrister

- indenfor 72 timer

.

Compliance – pluk fra forordning

- Artikel 5.2: Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

- Artikel 24.1: Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

Compliance

- Hvilke personoplysninger behandler kommunen?
- På hvilket retligt grundlag behandler kommunen personoplysninger?
  - Hvis ikke der er et klart lovgrundlag:
    - Hvilken information giver kommunen de registrerede?
    - Hvordan opfylder kommunen de registreredes rettigheder?
    - Hvordan indhenter kommunen samtykke?
    - Hvordan med personoplysninger om børn?
- Hvad skal kommunen gøre ved brud på persondatasikkerheden?
- Har kommunen indtænkt databeskyttelse i jeres it-systemer?
- Hvem er ansvarlig for databeskyttelsesspørgsmål?
- Overfører kommunen oplysninger til udlandet?

Compliance - datamapping

Hvem indsamler personoplysninger	Hvilke typer PO og hvilke lovkrav er der til behandling	Hvor opbevares data?
Hvordan indsamles data?	Hvorfor indsamles data?	Særlige lovkrav?
Hvilken information er undergivet særkrav?	Hvem håndhæver regulatoriske krav og hvordan - sanktionsniveau?	Hvorfor er reglerne der?

Den registreredes rettigheder

- Oplysningspligt – fra databehandler
- Indsigtsret
- Ret til at korrigere og slette oplysninger
- Ret til at gøre indsigelse mod behandlingen
- Ret til at tilbagekalde sit samtykke til enhver tid
- Ret til at klage til Datatilsynet

Samtykke – skærpede krav

- Almindelige oplysninger**: Samtykke**
- Følsomme oplysninger: **Udtrykkeligt samtykke**

- Samtykke skal være specifikt og formålsbestemt
  - Kan ikke udvides uden nyt samtykke
- Samtykkeanmodningen skal adskilles tydeligt fra øvrigt indhold

- Skal kunne frafaldes lige så nemt som det gives
- Der skal informeres om, hvordan man kan frafalde sit samtykke, få slettet, ajourført sine oplysninger og få indsigt i sine data og gøre indsigelse over behandlingen.

- Gælder også samarbejdspartnere

Samtykke – skærpede krav

- Samtykke kan ikke udgøre lovligt behandlingsgrundlag, hvis der er en klar ubalance mellem datasubjektet og den dataansvarlige

- Samtykke må ikke kræves som betingelse for tillægsydelser, der ikke er nødvendige i forhold til en kontrakt.

- I forbindelse med børns (< 16 år) aktiviteter på f.eks. sociale medier skal samtykke indhentes hos den, der har forældre-myndigheden

- Ansvaret for dokumentationen påhviler databehandler

Ret til sletning – retten til at blive glemt

- Når oplysningerne er ikke længere nødvendige i forhold til formålet med indsamling og behandling,
- F.eks.
  - Tilbagekaldelse af samtykke
  - Manglende retligt grundlag
  - Personen modsætter sig databehandlingen og ingen tungtvejende legitime grunde til fortsat behandling
- Uden unødig forsinkelse.
- Gælder også samarbejdspartnere.

Overførsel af data til udenfor EU/EØS (”tredjelande”)

Som udgangspunkt forbudt - dog

- Dataoverførsel kan ske til tredjelande, hvis modtagerlandet yder et tilstrækkeligt sikkerhedsniveau for de overførte oplysninger, f.eks.
  - EU standard contractual clauses (model contracts)
    - Ikke krav om tilladelse fra Datatilsynet, medmindre ordlyden ændres
    - Yderligere bestemmelser – er som udgangspunkt ok, hvis de ikke er i strid med Model Clauses
- Binding Corporate Rules
  - Skal godkendes af Datatilsynet og evt. et andet EU tilsyn
- Sikre tredjelande, såsom Israel, Argentina, Canada, Schweiz
  - tilladelse kræves ift. følsomme oplysninger
- EU US privacy shield
  - Specielle regler
- Samtykke eller en af de andre undtagelser, f.eks. kontrakt- eller lovgrundlag