

# KROMANN REU



---

## CLOUD COMPUTING - REGULATORISKE UDFORDRINGER

Pia Kirstine Voldmester

KROMANN  
REUMERT

# OVERBLIK OVER REGELSÆTTENE

- Øjebliksbillede – tingenes tilstand ændres.....måske
- Husk: Forskel på offentlige myndigheder og private virksomheder
- Persondataloven – **personoplysninger**
- Bogføringsloven – **regnskabsmateriale**, private
- Regnskabsloven – regnskabsmateriale, offentlige
- Arkivloven – offentlige myndigheders arkiver

# BOGFØRINGSLOVEN OG REGNSKABSLOVEN

- Regnskabsmateriale skal opbevares i DK
- Opbevaring i udlandet kræver dispensation fra ESS
- Kan man få det til cloud opbevaring?
- Hvad vil ESS lægge vægt på?



# PERSONDATALOVEN – EN MYRIADE AF FORHINDRINGER?

- Overblik over udfordringerne:
  - Sikkerhed og risiko for brist
  - Kontrolmuligheder
  - Rådighed/adgang/sletning
  - Registreredes rettigheder
  - Andre barrierer?



# PERSONDATALOVEN – HVORNÅR GÆLDER LOVEN I FORHOLD TIL CLOUD?

- Al elektronisk behandling af personoplysninger er omfattet af persondataloven, når
  - Den dataansvarlige er etableret i Danmark -> alle danske virksomheder/myndigheder er omfattet af loven...uanset hvor i verden virksomheden får dataene behandlet og opbevaret.
  - Når dataansvarlige i lande uden for EU benytter hjælpemidler i DK eller indsamler oplysninger i DK.
  - Husk: Økonomidata, logistikdata mv. uden personoplysninger er *ikke* omfattet af PDL

# DEFINITIONER

- Personoplysning: oplysning om en identificeret eller *identificerbar* fysisk person
  - Meget bred definition, omfatter fx også medlems-, kunde-journalnumre mv., cpr-numre, foto, biometriske data og som hovedregel IP-adresser
- Dataansvarlig: Den der afgør til hvilket formål og med hvilke hjælpemidler personoplysninger må behandles (virksomheden/myndigheden)
- Databehandler: Den, der behandler oplysninger på den dataansvarliges vegne (cloud leverandøren)

# GRUNDLÆGGENDE KRAV

- Udvide god databehandlingskik
  - bl.a. betydning ved sikkerhedsbrud (information til de registrerede?)
- Pligt til løbende ajourføring/kontrol for at sikre, at der ikke behandles urigtige/vildledende oplysninger – hvordan gør man det i cloud løsninger?
- Opbevaring af oplysninger må kun ske, så længe det er nødvendigt (for at opfylde formålet) – pligt til **løbende ajourføring + slettepligt** - hvordan gør man det i cloud løsninger?

# NOGLE GRUNDLÆGGENDE PERSONDATARETLIGE KRAV

- Behandlingshjemmel
  - Forskellige regler for offentlige og private dataansvarlige og
  - Forskellige data-kategorier
    - Almindelige oplysninger
    - følsomme oplysninger og
    - Strafbare forhold, væsentlige sociale problemer og andre rent private forhold.
  - Oplysningspligt – skal man fortælle at man bruger cloud og hvem leverandøren er?
  - Indsigtsretten – hvordan udøves den?

# PERSONDATALOVENS SIKKERHEDSKRAV

- "Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven"
- Sikkerhedsbekendtgørelsen for offentlige myndigheder (autorisation og adgangskontrol (fysisk og elektronisk), inddata- og uddatamateriale, mv.
  - Bkg. 528 af 15. juni 2000 med tilhørende vejledning nr. 37 af 2. april 2001.
- Sikkerhedsbekendtgørelsen – gælder for offentlige myndigheder, meeeen.....den smitter af.
  - Datatilsynet har i flere sammenhænge anbefalet, at private virksomheder efterlever bekendtgørelsen

# HVAD INDEBÆRER PERSONDATALOVENS SIKKERHEDSKRAV?

- Fysisk adgangskontrol – aflåste serverrum, vagt mv.
- Teknisk adgangskontrol – brugernavn, passwords mv.
- Transmission (kryptering)
- Logning af adgangsforsøg
- Ingen uautoriseret adgang
  - heller ikke fra amerikanske myndigheder (!?)



# KRAV OM SKRIFTLIG AFTALE MED CLOUD LEVERANDØREN

- Databehandlere må kun behandle data efter instruks fra den dataansvarlige
- Når den dataansvarlige overlader en behandling (opbevaring) til en databehandler skal den dataansvarlige **sikre sig** at databehandleren kan træffe de tekniske og organisatoriske sikkerhedskrav og **påse**
  - Sikre sig -> instrukser
  - Påse -> kontroladgang (!!)
- Den dataansvarlige skal indgå en skriftlig databehandlingsaftale med databehandleren. Hvis den dataansvarlige er etableret i en anden medlemsstat: pligt til at iagttage egne, lokale sikkerhedskrav.

# OVERFØRSEL AF DATA TIL LANDE UDENFOR EU

- Kræver særskilt hjemmel
  - Sikre tredjelande (ok uden samtykke, men kræver Datatilsynets tilladelse ved overførsel af følsomme data)
    - USA: Safe Harbor
  - Samtykke
    - Er det praktisk?
    - Er det overhovedet gyldigt?
  - EU-modelkontrakter og tilladelse fra Datatilsynet
    - NB! Husk det begrænsede anvendelsesområde databehandler-kontrakten (fuldmagt kan være en løsning)
  - Binding corporate rules

# OVERFØRSEL AF DATA TIL LANDE UDENFOR EU

- Krigsreglen – særligt kritiske oplysninger
  - fx cpr-registret, skat, det centrale kriminalregister , ATP's PBS', TDCs landsdækkende systemer,
  - Mulighed for foranstaltninger til bortskaffelse eller tilintetgørelse i tilfælde af krig skal sikres
  - Tvivlsomt om cloud-løsninger kan anvendes
  - ....men det (lille) problem løses nok politisk

# DATATILSYNETS PRAKSIS – SAGEN OM ODENSE KOMMUNE

- Datatilsynets udtalelse af 3. februar 2011
  - Brug af Google Apps online kontorpakke til lærernes registrering af **(følsomme)** oplysninger om eleverne.
- De identificerede problemstillinger:
  - Overførsel af oplysninger til tredjelande
  - Behandlingssikkerhed generelt
  - Anvendelse af databehandler
  - Sletning
  - Transmission og login
  - Kontrol med afviste adgangsforsøg
  - Logning
- Konklusion: "...på en række punkter er [der] problemer i forhold til kravene i persondataloven"
- Men...ikke en fuldstændig afvisning af, at problemerne kan løses!

# ODENSE KOMMUNE-AFGØRELSEN, HVAD GIK GALT?

- Forarbejdet var ikke gjort ordentligt
- Formentlig slet ikke været nogen (reel) forhandling af krav til datahåndteringen, kontrol og auditering
- Nogle issues kan løses relativt enkelt
  - Modelkontrakter og fyldestgørende aftalegrundlag, fornødne sikkerhedsforanstaltninger/risk assessment, auditering mv.
- Andre er nok vanskeligere at løse:
  - Overblik over præcist hvor dataene befinder sig (mhp. at kunne sikre at de krævede sikkerhedstiltag efterleves).
  - Sletning af data
  - Udenlandske myndigheders adgang til data (fx USA Patriot Act)

# CLOUD – HVORDAN SIKRES AT LØSNINGEN ER LOVLIG (OG BLIVER VED MED AT VÆRE DET?)

- Behandlingen af persondata skal på dagsordenen under kontraktforhandlingen.
- Fokus på forarbejdet - risikovurderinger mv.
- Auditering under samarbejdet (det skal man faktisk!)
- HUSK: Anmeldelse til Datatilsynet/tilpasning af allerede foretagne anmeldelser.
  - Antagelse af ny databehandler, som ikke er anmeldt kan i værste fald indebære at tilsynet "lukker" løsningen!

# KROMANN REUMERT



CLOUD COMPUTING – KONTRAKTSFORHANDLING  
I SKYEN

Jan Ussing Andersen

KROMANN  
REUMERT

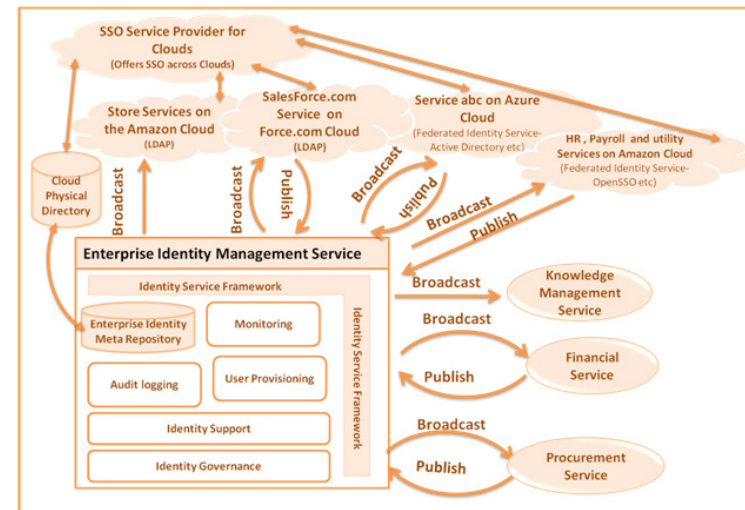
# CLOUD COMPUTING - AGENDA

- Forberedelsesfasen
- Cloud-kontraktens landskab
- Udvalgte kontraktemner – tips og faldgruber



# FORBEREDELSESFASEN

- Afklaring af egne behov
  - Business case og -benefits
  - Skal løsningen eller forretningen tilpasses
- Undersøgelse af leverandøren
  - Referencer mv.



# FORBEREDELSESFASEN

- Undersøgelse af ydelsen
  - Hvad får man egentligt?
  - Kan det lade sig gøre med eksisterende licenser/eksisterende setup?
- Undersøgelse af lovligheden – juridisk due diligence
  - Regulering og forbud
  - Open Source og copy-left
  - Jurisdiktion (bl.a. ift. Patentkrænkelser og US Patriot Act)

# KONTRAKTLANDSKABET

- Er der en kundestandard, der kan bruges?
  - Kendte standardkontrakter, f.eks. K01 (ikke uden meget væsentlige tilpasninger)
  - Driftskontrakter, outsourcingaftaler (tættere på)
  - Specialudviklede kontrakter
- Meget forskellige typer ydelser – behov for forskellige kontrakter
  - Storage, web-hosting, infrastruktur, applikationer, udviklingsværktøjer mv.
  - Enkeltstående cloud ydelser – eller en del af en større leverance

# KONTRAKTLANDSKABET

- Forhandlingsposition og -rum
  - Ændringer til ydelsen/ydelseshåndtering – meget begrænsede forhandlingsmuligheder
  - Forhandling af kontraktvilkår – lidt bedre muligheder, men alligevel svært – fokus er afgørende
  
- Klik-vilkår - dilemmaet

I accept the terms of use

Preview

# KONTRAKTEMNER - PROJEKTSTART



- Lovvalg og værneting
  - Risiko for at blive sagsøgt i udlandet
  - Domstole eller voldgift.
  
- Licensen i en ny kontekst
  - Ikke en IT-løsning men en abonnementsmodel
  - "overførsel" af gamle licenser
  - Sikre licens-rettigheder til brug i clouden – risiko for "licens-lock-in"

# KONTRAKTEMNER - SERVICEPERIODEN

- Levering af ydelsen
  - Ydelsesbeskrivelse – hvad leveres
  - Ændringer i ydelsen
    - Praktisk håndtering – notifikation, mv.
    - Begrænsninger i ændringer og/eller exit muligheder.
    - Hvad med special-tilpasninger/parameteropsætninger?
- Skalerbarhed
  - Tilgang til skalerbarhed (i begge retninger)
  - Betaling – beregning af forbrug



# KONTRAKTEMNER - SERVICEPERIODEN

- Leverancesikkerhed
  - Service Levels – operative og målbare krav til ydelsen
    - Mål (e.g. target levels) kontra reelle krav
    - Oppetid (availability) og svartider (response times)
    - Andet: support, skalerbahed, disaster recovery, datagenskabelse
  - Service Credits
    - Fees at risk – afskrækning eller erstatning?
  - Overvågning, rapportering og betaling/kreditering
  - Sole remedy-bestemmelser
  - Mulighed for ophævelse

# KONTRAKTEMNER - SERVICEPERIODEN

- Brug af data
  - Klar instruks
  - Leverandørens egen adgang til at bruge data (anonymt)
- Compliance – inc. datasikkerhed/håndtering
  - Krav om behandlingssted
  - Sikkerhedskrav og – standarder
  - Revisionskrav og – standarder



# KONTRAKTEMNER - SERVICEPERIODEN



- Betaling, tilbageholdsret mv.
  - Betalingsplaner og betalingsmodeller
  - Tilbageholdsret – forpligtelse til fortsat service
  
- Krav til version, aftestninger mv.
  - Først med sidste nyt, "first mover" risiko
  
- Snitflader med andre leverandører
  - Andre programleverandører, cloud-leverandører, udviklere
  - Netværksoperatøren

# KONTRAKTEMNER – ANSVAR

- Ansvarsbegrænsninger
  - Afskæring af tabstyper, herunder datatab
  - Beløbsbegrænsninger – typisk den løbende betaling
    - Misforhold ift. tab
    - Forsikringsdækning som alternativ
- Andre "relief events"
  - Force majeure, underleverandører, kundens forhold
- Ansvar for krænkelse af tredjemandsrettigheder
  - IaaS/PaaS – kundens ansvar over for leverandøren
  - Leverandørens ansvar for egen løsning

# KONTRAKTEMNER - OPHØR

- Hvordan undgår man lock-in
  - Forberedelse – sikre alternativer, benytte gængse standarder
  - Ingen juridiske hindringer for at benytte tredieparter
  - Regulering af dataformat og tilbageleveringsforpligtelser
  - Adgang til data - back-up hos trediepart
  - Deponering
- Exit-scenarier –hvis det hele går galt
  - Forpligtelse til deltagelse – termination assistance

# KONKLUSION



# STAY UPDATED

Tilmeld dig vores nyhedsbrev på [www.kromannreumert.com](http://www.kromannreumert.com)



KROMANN  
REUMERT