# Juridiske aspekter

## ved anskaffelse av skytjenester

Advokat Grete Funderud Stillum

DYNUG.NO - DYNAMICS Brukergruppe

Scandic Oslo Airport - 20.09.2017

BRÆKHUS

# Utgangspunkt

**Ønsker - mål:**

- **Fleksible funksjonelle, brukervennlige løsninger som er tilgjengelig på flere plattformer med integrasjoner mellom løsningene, med riktige datakvalitet**
- **Økt bruken av nye teknologiske muligheter, som automatisering, IoT, innhenting og analyse av store datamengder/BI, maskinlæring/AI mv**

**Løsning:**

- **De største mulighetene ligger i bruk av gode skytjenester, med riktig leveransemodell**
  - Skytjenesteleverandører
  - Langsiktige rådgivere med både teknologi og strategisk kompetanse som kjenner løsningene, bransjen og kunden
  - Egenkompetanse på strategi/forretningsmodell, samlet IT-landskapet og bestilling/innkjøp
  - Juridisk kompetanse for å sikre at tjenestene brukes lovlig og for å sikre hensiktsmessig avtaleregulering av roller, rettigheter og ansvar

# Rolle/ansvarsfordeling - Service description Dynamics for Operations 365 (v. 3 2017 )

## Service model

- Microsoft: Deploying, actively monitoring, and servicing
- Independent Software Vendors (ISV):  Specific solutions - AppSource
- Implementation Partner: Configuration with one or more ISV solutions and Customer-specific customizations
- Customer: Defines, develops, and tests any modifications using defined tools




BRÆKHUS
ADVOKATFIRMA

# Skytjenestenes sentrale egenskaper

- «All in one» leveranse tilgjengelig via internett
  - Standard applikasjon med hyppige obligatoriske (?) oppdateringer
  - Hardware med operativsystem, middelware og integrasjonsverktøy
  - Sikkerhet og drift
  - Leie/abonnement (ikke evigvarende bruksrett)
  - Eskalerbar
  - Overføring av data med lagring og prosessering på flere steder i Norge, EU, USA eller andre land
  - Mange skyhybrider (privat/public) og miks av sky og on premiss løsninger
- Tilknyttede tjenester
  - Forretnings-/strategirådgivning
  - Oppsett og konfigurering
  - Tilpasninger/modifikasjoner
  - Konvertering/datamigrering
  - Integrasjoner/grensesnitt med andre skytjenester og løsninger (on premiss mv)
  - Brukerstøtte og opplæring
  - Løpende bistand basert på type skytjeneste og egenkompetanse

# Lovverk og avtaler som regulerer leveransene fra leverandøren(e)

- **Ingen særlig lov eller forskrift**
- **Avtaleloven § 36 mot kvalifisert urimelige avtaler**
- **Noen krav i EUs personvernforordning (GDPR)**
- **Ulovfestet kontraktsrett, bransjepraksis og rettspraksis**
- **Indirekte lov-/forskriftskrav basert på kundens behov for bruk?**
- **Sentralt med avtaleregulering**
  - Skyleverandørenes standardkontrakter
    - Dekker sjelden implementering og rådgivning
  - Avtale om kjøp av SaaS-tjenester fra IKT Norge
  - Avtale om løpende tjenestekjøp (SSA-L) fra Difi
  - Skytjenesteavtalen fra Dataforeningen («integrasjonsavtale»)
  - Difis bistandsavtale (SSA-B) og oppdragsavtale (SSA-O) - IKT Norges konsulentavtale
  - Databehandleravtalemaler fra Datatilsynet og EU
  - **NB**: Forholdet mellom leverandørene, underleverandørene, tredjepartene og kundens egne bidrag

# Juss som regulerer bruken av skytjenester

- **Jussen kan medføre behov for å endre hvordan tjenesten var tenkt brukt, krav om dokumentasjon, nye retningslinjer mv**
- **Hvilke juridiske krav er aktuelle? Konkret vurdering avhengig av type virksomhet og type data, avtaleforpliktelser og virksomhetens policy**
- **Ansvaret ligger hos virksomheten - bruken**
- **De rettslige kravene bør identifiseres og gjenspeiles i kontrakten; f.eks bilag 1 og 2 som andre krav og løsningsbeskrivelser**
- **Aktiviteter i prosjektet som avklarer/detaljerer hvordan de rettslige kravene skal hensyntas, i workshops og test; f.eks bilag 3: Prosjektplan**
- **Eks:**
  - ERP: Alltid krav til behandling av regnskaps- og personopplysninger
  - Digitalisering av avtaleprosesser: Opplysningsplikt, signering, angrerett
  - IoT, innhenting og analyse av store datamengder: Personvernregler med krav til informasjon, samtykkeerklæring mv
  - Automatisering, maskinlæring/AI: Arbeidsrettslige regler om nedbemanning/ omorganisering

# Min. krav «vanlige virksomheter»* bør vurdere ved ERP skytjenester

- **Lovkrav til oppbevaringssted for regnskapsmateriale**
- **Lovkrav til behandling av personopplysninger**
- **Funksjonalitet**
- **Responstid, oppetid og tilgjengelighet**
- **Endringer i tjenesten, oppgraderinger mv**
- **Prising**
- **Sanksjoner**
- **Avvikling – «lock in effekt»**
- **Konkurs eller vesentlig mislighold**

* Flere krav for bl.a: Organ underlagt arkivloven, forvaltningsorgan og leverandører av sikkerhetsgradert anskaffelser til forvaltningsorgan, bank og finanssektoren, inkassoforetak, forsyningssektoren og alle som behandler helseopplysninger

# Regnskapsmateriale i skyen

- **Regnskapsmateriale må oppbevares i Norden, og være tilgjengelig i lesbar form og skal kunne skrives ut på papir fra terminal el i Norge i hele oppbevaringsperioden**
- **Oppbevaring utenfor Norge krever skriftlig melding til Skattedirektoratet**
- **Få unntak. Kan få tillatelse fra Skatteetaten – mest praktisk v/konsern**
- **Mulig løsning:**
  - Reglene blir endret? SAF-T vil dempe behovet, og dermed kravet?
  - Leverandørene etablerer skyer i Norden
  - Full kopi/backup i Norge/Norden senest 6 måneder etter bokføringsslutt som Skatteetaten får tilgang til via et miljø i Norge. Husk tilsvarende oppbevaringsplikt som «original»
- **Hjemmel: Bokføringsloven, bokførings-/ og oppbevaringsforskriften**

# Personvern

**Utgangspunkt:**

- Personopplysningsloven, personopplysningsforskriften og ekomloven
  EUs nye personvernforordning (GDPR) med forskrifter (mai 2018)
- Generelle regler som ikke bare gjelder skytjenester
- Kravene må gjennomføres før en ny tjeneste tas i bruk eller brukes på ny måte

**De viktigste personvernkravene ifht. skytjenester:**

1. Kartlegging, vurderinger og dokumentasjon av personvernforhold og sikkerhet
2. Informasjon til den registrerte
3. Databehandleravtale
4. Krav til løsningen: Innebygd personvern og dataportabilitet
5. Krav om personvernombud for enkelte virksomheter
6. Bortfall av melde- og konsesjonsplikt, men krav til forhåndsdrøftinger med Datatilsynet dersom behandlingen medfører høy risiko



BRÆKHUS
ADVOKATFIRMA

# Personopplysninger – kartlegging, vurdering og dokumentasjon

- **Kartleggingsarbeid med dokumentasjonskrav («protokoll») basert på virksomhetens størrelse og behandlings- omfang/risiko. Tilpasset mal, f.eks oppdelt pr. tjeneste/løsning**
- **Hvilke kategorier registrerte og personopplysninger virksomheten behandler og til hvilket formål**
- **Om det foreligger behandlingsgrunnlag**
  - Samtykke/avtale er normalt det mest praktiske grunnlaget
  - Krav til saklighet og relevans
  - Bruk i samsvar med det innhentede formålet
- **Om det er gis tilstrekkelig informasjon - personvernerklæring**
- **Om opplysningene er korrekte og oppdaterte – sletteplikt**
- **Om opplysningene utleveres, og i så fall til hvem og hvor (land)**



BRÆKHUS
ADVOKATFIRMA

# Personopplysninger – internkontroll og sikkerhetstiltak

- **Pol: Krav om internkontrollsystem med retningslinjer og dokumentert risikovurdering av tjenesten**
- **GDPR: Krav om egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar m/nødvendige retningslinjer. Økte krav ved behandlinger som «*vil medføre en høy risiko for fysiske personers rettigheter og friheter*»**
- **Elementer i en risikovurderingen**
  - Behov for konfidensialitet (sikre at kun autoriserte brukere har tilgang), integritet (hindre uautoriserte endringer og sporbarhet) og tilgjengelighet (sikre at dataene er tilgjengelig ved behov)
  - I forhold til sannsynlighet for at en hendelse inntrer og konsekvenser
  - Risiko varierer med datatype
- **Rutiner, retningslinjer/policyer, maler, arbeidsprosesser, som f.eks.**
  - Epostrutiner
  - Sletterutiner
  - Avvikshåndtering med meldeplikt til Datatilsynet og den berørte

# Personopplysninger – databehandleravtale

- **Leverandører av skytjenester er databehandlere**
- **Krav om avtale som regulerer behandling av kundens personopplysninger, også om skyen bare ligger i Norge**
- **Hovedinnhold etter GDPR**
  - Hensikten med og varigheten av behandlingen
  - Behandlingens formålet og art
  - Kategorier av registrerte og personopplysninger
  - Databehandlers begrensede rett til behandling av opplysningene, inkl. behandlingssted og rett overføring til tredje land og adgangen til å engasjere underleverandør
  - Konfidensialitets- og sikkerhetskrav med revisjonsrett
  - Plikt til å melde avvik
  - Sletting/tilbakelevering av personopplysninger etter opphør, etter kundens valg
  - Krav om innsyn og dokumentasjon
- **NB: Datatilsynets mal tilfredsstiller kravene for behandling i Norge/EU etter pol men ikke GDPR**

# Personopplysninger - behandlingssted

- **Behandlingsstedet medfører ikke ytterligere krav ved behandling kun i Norge, EU eller et særskilt godkjent land**
- **USA: Sertifiseringsordning - Privacy Shield erstatter Safe Harbor**
  **Liste over sertifiserte: https://www.privacyshield.gov/list**
- **Annet utleveringsgrunnlag:**
  - Standard EU databehandleravtale for overføring til 3. land - Antatt ny standardavtale etter GDPR
  - Bindende virksomhetsregler (BCR)
- **Pol: Varsling til Datatilsynet m/kopi av avtalen før overføringen skjer**
- **Microsofts vilkår (OST):**
  - Sted for databehandling er USA og andre land som Microsoft eller tilknyttende selskaper eller underleverandører har virksomhet
  - Standard EU avtale for overføring til 3. land er inntatt som del av vilkårene
  - Trust center: «*Customers can specify the region, or datacenter, where their customer data will be stored*"



BRÆKHUS
ADVOKATFIRMA

# Spesifikasjon/krav til funksjonalitet, tilgjengelighet, responstid, sikkerhet mv

- Kunden må vurdere sine krav og hvem som er nærmest til å bære risikoen
- Skytjenesteleverandøren leverer det samme til alle kunder, og "as is".
  - Gjennomgå vilkårene og SLAer m/kompensasjonskrav og forutsetning, tidspunkt for vedlikeholdsvindu og plikt til oppdragering.
- Implementeringspartner kan ta et avtalt definert ansvar:
  - Etter dialog med kunden og råd om valg tjeneste og implementering Hva er det rimelig og fornuftig at hvem tar ansvar for? Muligheter for overvåkning, feiloppfølgning, konfigurering og ev. tilpasninger? Spør etter leverandørens tjenestekatalog el!
- Broker/megler tar et definert ansvar:
  - Særlig aktuelt ved løsninger basert på flere skytjenester for mange kunder
- Prøveperiode: Først etter en (test)periode og verifisering, begynner standardtjenestens regler om binding og (full) betaling. Ev. kort exitfrist.

# Bruk av opplysninger, konfidensialitet og sikkerhet

- Leverandørenes rett til å bruke dine opplysninger
- Fysisk sikring
- Tilgangskontroll
- Drift (tilgjengelighet)
- Sikkerhetsdokumentasjon og revisjonsrapport
- Plikt til å bistå for at kunden skal kunne ivareta sitt ansvar
- Bør vurderes «selvstendig» - mer enn oppfyllelse av pol
  Ikke alltid personopplysningene er det mest konfidensielle
- NB: Sertifisering trenger ikke bety at systemet har høy sikkerhet, men kun at sikkerhetsbehovene er identifisert og følges opp slik virksomheten har definert

# Prising

**Skytjenesten:**

- **Viktig å forstå prismekanismene - lisensreglene**
- **Pris pr. bruker pr. måned? Kapasitet?**
  - Hvilke deler av tjenesten får hvilke type brukere tilgang til?
  - Endringer i bruk – opp og ned
  - Prises faktisk, estimert eller rapportert bruk?

**Implementering og forvaltning fra partner:**

- **Prising bør gjenspeile ansvaret og oppgavene**
- **Ulike prismekanismer for ulike oppgaver og hvem som styrer hva som skal gjøres**
- **Totalleverandør - Tjenestekatalog**

# Endringer

- **Endringer i tjenesten**
  - Kan kunden velge om / når man vil oppgradere?
  - Oppdateringer kan kreve endringer i integrasjoner og tilgrensede systemer, samt endringer i arbeidsprosesser og opplæring.
  - Hva skjer med ev. tilpasninger i sky-tjenesten – vil de fortsatt fungere?
  - Rett til varsel og utsettelse v/uhensiktsmessig tidspunkt?
  - Utviklingen går i feil retning/for lite utvikling på «dine områder». Kunden kan miste noe som var årsaken til valget av tjeneste
  - Microsofts vilkår pr. september 2017 tillater kommersielt rimelige endringer i tjenestene

- **Endringer i avtalebetingelsene**
  - Kontraktsvilkårene kan ofte endres ensidig fra leverandøren
  - Endringer bør min. varsles og kunne gi grunnlag for kort exit rett
  - Microsofts vilkår pr. september 2017 gir ikke ensidig endringsrett i abonnementsperioden for funksjoner  som var inkludert ved anskaffelsestidspunktet

# Avvikling - Lock-in effekt

- **Kunden bør avklare når og hvordan bytte av skytjeneste og partner kan skje**
  - Sml. evigvarende bruksrett til programmet som kunne brukes for oppslag i historiske data
- **Bindingsperiode – ev. hvor lenge?**
- **Tilgang til egne data**
  - Microsofts vilkår: Tilgang til og mulighet for å hente ut kundedata som er lagret i tjenesten så lenge abonnementet løper og 90 dager etter utløpet, hvoretter konto deaktiveres og kundedata slettes
- **Integrasjoner og tilpasninger**
  - Rettigheter for at andre kan overta videreutvikling og feilretting (og praktisk mulighet – kildekode og dokumentasjon)
- **Format og ev. andre tekniske utfordringer**
- **Partner bør ha plikt til å assistere ved leverandørbytte**
  - Frist? Omfang? Pris?

# Konkurs eller vesentlig mislighold

- Får du dataene dine tidsnok, og kan bruke dem uten «resten av tjenesten»?
- Viktige å tenke på alle leverandørene og hvem som leverer hva - Hvordan løsningen er satt opp og hvem du bør ha avtale med
- **Kan bedre situasjonen:**
  - Benytt retten til uthenting av kundedata jevnlig
  - Rett til å «overta» partners rolle overfor Microsoft / bytte partner
  - Sørg for oppdatert dokumentasjon av prosesser, konfigurasjon, oppsett mv som du har tilgang til for å kunne etablere løsningen på nytt
  - Dersom løsningen (også) ligger hos andre leverandører, kan det avtales krav om flytting til denne, forutsatt at det forankres hos alle parter
  - Morselskapsgaranti fra partner eller andre som har rettigheter til koden
  - Kildekodedeponering og dokumentasjon for det partner leverer

# Spørsmål - Innspill

Kontaktinformasjon:

Grete Funderud Stillum,
Partner – Advokat i Brækhus Advokatfirma

Telefon: + 47 99 09 07 10

E-post: stillum@braekhus.no

BRÆKHUS