Juridiske krav til skytjenester ISBG medlemsmøte 30.11.2016

Grete F. Stillum

Advokat og partner i Brækhus Dege Advokatfirma

www.bd.no

BRÆKHUS DEGE
ADVOKATFIRMA

Aktualitet – problemstilling

- Funksjonalitet, tekniske muligheter, økonomi .... (og jus)
- Hvilke juridiske krav og muligheter bør virksomheter ta hensyn til ved valget av skytjeneste og ved implementeringen?
  Særlig vekt på personvern
- Min bakgrunn:
  - Jurist i 1994 og «IT-advokat» fra 1997
  - Både kunde- og leverandørsiden, små og store prosjekter,
    i alle faser fra avtaleinngåelse, prosjektoppfølging, krisestadiet med reforhandling, samt krav om heving og erstatning
  - «Sky-tjenester» fra Telecomputings ASP-løsninger til dagens SaaS, PaaS og IaaS med hybrider og ulike former for koblinger/integrasjoner

Skytjenestenes sentrale egenskaper (public SaaS)

- «All in one» leveranse tilgjengelig via internett
  - Standard applikasjon med hyppige (?) automatiske (?) oppdateringer
  - Hardware med operativsystem, middelware og ev. integrasjonsverktøy
  - Sikkerhet og drift
  - Overføring med lagring og prosessering av data på flere steder, i Norge, EU eller tredje land, ofte delt med flere
  - Leie/abonnement (ikke evigvarende bruksrett)
  - Eskalerbarhet
  - Standard avtale uten (særlig) forhandlingsmulighet
- Tilleggstjenester som ofte leveres av andre
  - Oppsett og konfigurering
  - Konvertering/datamigrering
  - Integrasjoner/grensesnitt med andre systemer
  - Tilpasninger/modifikasjoner
  - Brukerstøtte og opplæring

Lovverk og avtaler som kan regulere leveransen fra leverandør

- Ingen særlig lov eller forskrift
- Avtaleloven § 36 mot kvalifisert urimelige avtaler
- Ulovfestet kontraktsrett, bransjepraksis og rettspraksis
- Noen krav til leverandørens plikter i EUs personvernforordning (2018)
- Sentralt med **avtaleregulering**
  - IKT Norge – Avtale om kjøp av SaaS-tjenester (no og eng)
  - Ingen SSA-avtalemal fra Difi spesielt for skytjenester
  - Veileder fra Dataforeningen
  - Flere sjekklister - skal også komme fra Difi
  - Leverandørene av SaaS har egne standardkontrakter, men «vektet» og sjelden fokus på implementeringen...
  - Databehandleravtalemaler fra Datatilsynet og EU

Juridiske krav til bruk av skytjenester

- Utgangspunkt - regelverk
  - Regulatoriske krav (lov- og forskriftskrav)
  - Bedriftens avtaleforpliktelser, intern akseptabel risikoprofil og policy
- Ulike hensyn
  - Sikre norske myndighets tilgang til opplysninger
  - Sikre at ikke andre virksomheter eller myndigheter får tilgang til opplysninger
  - Sikre at opplysninger ikke misbrukes
- Ulike krav og løsninger
  - Krav som begrenser bruken eller krever tekniske endringer/tillegg
    - Eks. lokasjonskrav og sikkerhetskrav
  - Krav til vurderinger og dokumentasjon
  - Krav til avtalebetingelser med leverandøren eller avtale/samtykke/informasjon med brukere (ansatte, kunder eller andre)
  - Krav til klarering eller melding

Vurderinger av juridiske krav ved valg av skytjeneste og implementering

- Ansvaret ligger hos virksomheten
  - Kan ikke overføres til leverandøren
  - Myndigheter godkjenner ikke en løsning / tjeneste som sådan
  - Sertifisering av leverandøren / tjenesten er ikke i seg selv nok
- Hva avgjør hvilke krav virksomheten må forholde deg til?
  - Type virksomhet
  - Hvilke typer/kategorier opplysninger tjenesten skal benyttes til
- **Konkret** kartlegging og vurderinger!
  - Bør gjøres og dokumenteres før valg av leverandør og tjeneste, og gjenspeiles i kontrakten
  - Kan medføre behov for å gjøre noen justeringer i hvordan tjenestene var tenkt brukt, endre/eller innføre noe retningslinjer, opplæring og kontroller

Aktuelt regelverk mv

- For «vanlige private virksomheter»
  - Personopplysningsloven med forskrift og ekomloven
  - Bokføringsloven med forskrifter
  - Avtaleforpliktelser ifht. konfidensialitet mv
  - Interne krav / policy
    - Eksponering av kundeopplysninger og andre bedriftshjemligheter
    - Krav om balanserte avtaler, leverandørbindinger mv

- For særlig virksomheter (og leverandører til disse)
  - Organ underlagt arkivloven
  - Forvaltningsorgan og leverandører av sikkerhetsgradert anskaffelser til forvaltningsorgan (sikkerhetsloven)
  - Bank og finanssektoren (IKT-forskriften, finanstilsynsloven)
  - Inkassoforetak
  - Forsyningssektoren
  - Helseopplysninger (helseregisterloven og helsepersonelloven)

Kartleggingsresultat: Hva en «vanlig» virksomhet min. vurdere ved bruk av en skytjeneste

- Kravene til oppbevaring av regnskapsmateriale
- Flere krav til personopplysninger
- Behov for eierskap til opplysningene og begrensninger i leverandørens bruk av disse
- Sikkerhetskrav
- Spesifikasjon/krav
- Responstid, oppetid og tilgjengelighet
- Endringer i tjenesten, oppgraderinger mv
- Prising ved endret utnyttelse
- Sanksjoner
- Avvikling – «lock in effekt»
- Konkurs eller vesentlig mislighold

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.
- Hjemmel: Bokføringsloven, bokføringsforskriften og oppbevaringsforskriften.
- Få unntak. Kan få tillatelse fra Skatteetaten – konsern
- Mulig løsning:
  - Leverandørene etablerer skyer i Norden
  - Kopi i Norge/Norden med tilsv. oppbevaringsplikt «en gang i året» etter at årsregnskapet er avlagt, inkl. applikasjonen
  - Reglene blir endret? SAF-T vil dempe behovet, og dermed kravet?

Personopplysninger – nærmere kartlegging

- **Hvilke typer personopplysninger ønsker du å behandle og hvordan?**
- **Personopplysninger**: Alle opplysninger og vurderinger som direkte eller indirekte kan knyttes til en enkeltperson. Eks. navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder, fingeravtrykk, fødselsnummer mv. Ikke cookies (?)
- **Sensitiv personopplysninger**: Opplysninger om rase, straffe-, helse-, seksuelle forhold, fagforeningsmedlemskap.
- **Behandling**: Enhver bruk av personopplysninger, slik som innsamling, lagring, sammenstilling, overføring, utlevering mv.
- **Behandlingsansvarlig**: Den som bestemmer formålet med behandlingen av personopplysningene og hvilke hjelpemidler som skal brukes
- **Databehandler**: Den som behandler personopplysningene på vegne av den behandlingsansvarlige

Personopplysninger – behandlingsgrunnlag

- **Vurder om du har behandlingsgrunnlag eller må skaffe det**
- Samtykke/avtale vil normalt være det praktiske grunnlaget
  - Frivilling, uttrykkelig og informert
  - Særlig om ansatte:
    - Viktig å gi informasjon om hvordan tjenesten fungerer og utarbeide interne retningslinjer for bruk
    - Regler som begrenser innsyn i ansattes e-post og personlige område i virksomhetens datanettverk og elektroniske kommunikasjonsmedier
- Bruk i samsvar med det innhentede formålet
- Krav til saklighet og relevans
- Korrekte og oppdaterte opplysninger - sletteplikt
- Ofte behov for å endre informasjonen / samtykket ved nye tjenester
- Dokumenteres skriftlig

Personopplysninger - risikovurdering

- Krav om **din dokumenterte vurdering** av at informasjonssikkerheten er tilfredsstillende m/risikovurdering basert på aktuelle data – **del av virksomhetens internkontrollsystem**
- Bra om leverandøren er sertifisert, men ikke tilstrekkelig

- Vurderingen:
- Hva er akseptabel risiko ifht 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)
- Risiko vurderes i forhold til **sannsynlighet** for at en hendelse inntrer og **konsekvenser** at det skjer
- Risiko varierer ifht **datatype** , og derfor må de data som leverandøren sannsynligvis vil behandle identifiseres
- Dokumentere vurderingene **skriftlig**
- Gjør ev. endringer i rutiner, maler, arbeidsprosesser
- Revisjoner ved endringer i tjenesten eller endringer i bruken

Eksempel: Risikovurdering – Office 365

#	**Uønskede Hendelser**	**Kategori** Konfidensialitet/ Integritet/ Tilgjengelighet	**Sannsynlighet** 1: Sjeldnere enn hvert 3. år 2: Hvert 2.-3. år 3: Hvert år 4: Flere ganger hvert år	**Konsekvens** 1: Ingen viktige konsekvenser 2: Små konsekvenser 3: Middels store konsekvenser 4: Store konsekvenser	**Risiko** Sannsynlighet x Konsekvens
1	Uvedkommende får urettmessig tilgang (interne og eksterne)	Konfidensialitet	2	2	4
2	Bruker deler brukernavn og passord med andre	Konfidensialitet	3	2	6
3	Tjenesten er utilgjengelig i opptil 1 dag	Tilgjengelighet	1	1	1
4	Tjenesten er utilgjenglig i mer enn 1 dag	Tilgjengelighet	1	2	2
5	Tap av data	Integritet	1	3	3
6	Utilsiktet endring av opplysninger	Integritet	2	1	2
7	Tilsiktet, ondsinnet endring av opplysninger	Integritet	1	3	3
8	Sensitive opplysninger sendes på epost (ukryptert)	Konfidensialitet	3	3	9
9	Leverandøren endrer tjenesten	Tilgjengelighet	1	3	3
10	Data på avveie ved migrering fra dagens løsning	Konfidensialitet	1	3	3

Personopplysninger - behandlingssted

- **Vurder hvor du skal/kan behandle personopplysningene**
- Husk at behandling ikke bare er lagring, og at du må vurdere både leverandør og underleverandør. Hvor befinner ansatte seg?
- EU likestilles med Norge ifht. behandling av personopplysninger
- Noen EU godkjente land: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- USA: Privacy Shield erstatter Safe Harbor
  Liste over sertifiserte: https://www.privacyshield.gov/list
- Ellers kreves overføringsgrunnlag
  - Mest praksis:
    Inngå en standard EU kontrakt for overføring til 3.land m/varslingsplikt til DT
    Ingen endringer i malen er tillatt og nødvendig å fylle ut to vedlegg med bl.a. type data og konkret om sikkerhet

Personopplysninger - databehandleravtale

- Regulere behandlingen av personopplysninger - Virksomheten skal ha kontroll over egne data
- Formålet med behandlingen
- Hvilke type data som leverandøren har tilgang til / skal behandle
- Databehandlers plikter:
  - DB skal bare behandle dataene som ledd i oppfyllelse av sine kontraktsforpliktelser, og følge de rutiner og instrukser som kunden til enhver tid bestemmer.
  - DB skal oppfylle krav til sikkerhet, dokumentasjon, revisjon og avviksmelding iht. pol §§ 13-15 og pof kap 2
- Hvor dataene behandles. Regler v/lokasjonsbytte.
- Navn på underleverandør(er). Underleverandørbytte.
- Bestemmelser om varighet og opphør, inkl. håndtering ved opphør

Melde-/konsesjonsplikt til Datatilsynet

- Utgangspunkt:
  - Meldeplikt 30 dager før behandlingen starter via elektronisk skjema
  - Konsesjonskrav for sensitive personopplysninger som ikke er avgitt uoppfordret
- Mange unntak, for eksempel:
  - «Ordinær» egen behandling av opplysninger om ansatte, kunder, abonnent og leverandører for å oppfylle en avtale
  - Meldeplikt dersom du skal sende reklame til egne kunder
  - Meldeplikt for bruk av «fysisk» sporingsteknologi
- Mer info og link til meldeskjema: https://www.datatilsynet.no/personvern/Melding-og-konsesjon/

Eierskap og bruk av opplysningene, sikkerhet

- Bør også vurderes selvstendig - mer enn en oppfyllelse av personopplysningsloven (ikke alltid at personopplysningene er de mest verdifulle / sensitive)
- Fysisk sikring
- Tilgangskontroll
- Drift (tilgjengelighet)
- Sikkerhetsdokumentasjon og revisjonsrapport
- Plikt til å bistå for at kunden skal kunne ivareta sitt ansvar
- NB: Sertifisering trenger ikke bety at systemet har høy sikkerhet, men kun at sikkerhetsbehovene er identifisert

Spesifikasjon/krav

- Kunden må vurdere sine krav mht. funksjonalitet, tilgjengelighet, responstid, sikkerhet mv
- Mulighet for konfigurering og ev. tilpasninger
- Standardavtalene pålegger sjelden ansvar for «mangler»
  - Det samme leveres til alle kundene og tjenesten leveres ”as is”
- Mulig (delvis) løsning på et ønske om ansvar for kundens definerte behov:
  - **Prøveperiode**: Først etter en (test)periode og verifisering, begynner standardtjenestens regler om binding og (full) betaling.
    Ev. rett til exit med kort frist.
  - **Implementeringspartner tar et definert ansvar**: Etter dialog med kunden og råd om valg tjeneste, leverandør og oppsett/bruk
  - **Broker/megler tar et definert ansvar:** Særlig aktuelt ved løsninger basert på mange tjenester for mange kunder

Responstid, oppetid og tilgjengelighet

- Normalt tilgjengelig 24/7/365 dersom du har internett, men overvåkningstiden kan være kortene og små brudd registreres ikke / gir ikke konsekvenser ...
- Finnes det **garantier** om responstid, oppetid og tilgjengelighet, ev. tidskrav for feilretting? Hvordan skal disse forstås? Når på døgnet? Over hvilken måleperiode? Hva er målepunktet? Hva er unntakene? Når er vedlikeholdsvindu? Varsel før planlagt nedetid? Mulighet til å påvirke?
- Hva er **konsekvensene** dersom garantiene ikke oppfylles? Ofte ingen refusjonskrav/ prisavslag. Likevel et incitament?
- **Kontroll** er ofte vanskelig. Ofte bare sanksjon om du melder. Rapporter er viktig.

Endringer

- Endringer i tjenesten
  - Har alle kundene hele tiden samme «versjonen», eller 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 – fungerer de fortsatt?
  - 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

- Endringer i avtalebetingelsene
  - Kontraktsvilkårene kan ofte endres ensidig fra leverandøren
  - Endringer bør varsles og kunne gi grunnlag for kort exit

Prising

- Rimeligere?
- Vanskelig å forstå mekanismene. Hva er enhetsprisen? Pr. bruker pr. måned pr. funksjon, ev. m/tillegg pr. lagringsenhet.
- Hvilke deler av tjenesten får de ulike brukerne tilgang til?
  Ofte for snevert i forhold til «den norske måten å jobbe på»
- Endringer i bruk, omfang mv - eskalerbarhet begge veier?
- Like regler ved økt og redusert omfang? Prises faktisk eller estimert, ev. rapportert bruk?
- Vanskelig å sammenligne de ulike leverandørene?

Sanksjoner

- Hva gir leverandøren rett til å stenge kunden ute fra tjenesten - ofte mye, herunder ikke vesentlig betalingsmislighold
- Hva gir kunden exit rett - ofte lite
  Ønske: Definerte endringer, inkl. pålegg fra Datatilsynet og andre myndigheter som ikke etterkommes.
  Alternativt: Kort oppsigelse
- Hvilke økonomiske tap kan kunden kreve erstattet – ofte ingen aktuelle tap, utover ev. en liten nedetidskompensasjon. Heller ikke for tap av data/rekonstruksjon, ev. ansvar etter back-up. OK?
- Mulig å få skadesløsholdelse for tap pga manglende oppfyllelse av lovpålagte krav?
- Hva som er force majeure hendelser bør undersøkes fordi det kan si noe om graden av katastrofeberedskap

Avvikling - Lock-in effekt

- Ofte stor faktisk og juridisk leverandørmakt
- Ofte lang bindingsperiode
  - Mulig med ulik bindingstid (kortere for kunden)?
- Eierskap til dataene - hvordan kan kunden få tilgang til sine data
  - Hvilket format kan kundens data kreves utlevert på? Andre tekniske utfordringer? Frist?
  - Sml. trad. lisens hvor kunden ofte kan bruke gammel lisens for oppslag i historiske data
  - Leverandøren bør ha plikt til å assistere ved leverandørbytte. Krav til frist? Omfang? Pris?
- Sletting av data ved opphør:
  - Både viktig at data slettes betryggende, og at data ikke slettes for tidlig

Konkurs eller vesentlig mislighold

- Bostyrer har antatt utleveringsplikt for kundenes data ved konkurs hos en skytjenesteleverandør mot betaling, men får du de tidsnok...?
- Bedre? Avtalefest en rett til å få utlevert data på definert elektronisk format, som benyttes jevnlig
- Hvordan fortsette når «programdelen» blir borte?
  - Hvor vanskelig (tidkrevende) er det å få ny løsning/leverandør?
  - On premiss (begrenset) lisens, ev. i depot/escrow?
  - Ev. kildekodedeponering
- Ved IaaS/PaaS og hybridløsninger som ligger hos andre leverandører eller som andre tar back-up av
  - Mulighet for å avtalefeste at kunden kan kreve flytting eller utlevering av data, forutsatt at det forankres hos alle parter

Lovvalg og tvisteløsning

- Norsk rett, ofte mulig å få til!
- Tvisteløsningsorgan (hvor en tvist skal avgjøres og domstoltype)
  - For norske kunder, er Norge å foretrekke
  - I EU/EØS: Alminnelige domstoler er OK mht håndheving
  - Utenfor: Ofte behov for voldgift for at en dom skal kunne håndheves
- Det bør være samme lovvalg og tvisteløsningsorgan
  - Norske domstoler er best på norsk rett

Ny Personvernforordning i EU

- Godkjent av EU-rådet i mars 2016
- Hovedintensjonen er å etablere en felles forståelse av rettigheter og plikter for personvern i alle europeiske land
- Forordningen vil bli norsk lov via EØS-avtalen, antatt i **mai 2018**
- I hovedsak en videreføring av dagens personopplysningslov
- Økte sanksjoner for behandlingsansvarlig og nå også databehandler
  - Erstatningsansvar overfor den registrerte
    - Dersom forordningen ikke er overholdt
    - Handlinger i strid med instruks/avtale
  - Bøter opp til 20 millioner euro eller opp til 4 % av konsernets årlige globale omsetning

Personvernforordningen – hovedendringer

- Strengere krav til å dokumentere virksomheters internkontroll og datasikkerhet med risikovurderinger av personvernkonsekvenser
- Redusert melde-/konsesjonsplikt til Datatilsynet, men økt plikt til å melde sikkerhetsbrudd (72 timer)
- Økt krav til informasjon - Alle skal ha en forståelig personvernerklæring
- Mer utførlige regler om muligheten til å bruke data for andre formål og tydeligere regel om retten til å kreve sletting
- Innebygd personvern i løsninger med den mest personvernvennlige innstillingen som standard
- Innholdskrav til databehandleravtale
- Krav om personvernombud: Alle offentlige, og private virksomheter som behandler sensitive data eller overvåker borgere i stor skala
- Dataportabilitet: Borgere skal kunne ta med «sine data» til ny leverandør
- Også virksomheter som ikke er etablert i EU blir underlagt regelverket dersom de tilbyr varer eller tjenester i EU

BRÆKHUS DEGE ADVOKATFIRMA

Veiledere om skytjenester mv:

- Datatilsynet:
  http://www.datatilsynet.no/Global/04_veiledere/Cloud_computing_2014_oppdatert.pdf
  https://www.datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/
  http://www.datatilsynet.no/Global/04_veiledere/Risikovurdering_veileder.pdf
  https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-blir-nytt-med-forordningen/
  https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/
- Nordisk ministerråd:
  http://norden.diva-portal.org/smash/record.jsf?pid=diva2:701093&dswid=-5226
- EU Art. 29-gruppen: http://www.cil.cnrs.fr/CIL/IMG/pdf/wp196_en.pdf
- Dataforeningen: https://www.uninett.no/webfm_send/713
- Danske IT advokater og Dansk IT: http://itadvokater.dk/wp-content/uploads/2013/02/Vejledning-CloudComputing-final2.pdf
- Nasjonal strategi for bruk av skytjenester:
  https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

Spørsmål - innspill

Kontaktdetaljer:

Grete F. Stillum - Brækhus Dege Advokatfirma DA

Web: www.bd.no

Epost: gfs@bd.no

Mobil: 990 90 710

BRÆKHUS DEGE
ADVOKATFIRMA

Oslo:
Dronning Maudsgt. 10, 0250 Oslo
Tel. +47 23 23 90 90

Sandvika:
Rådmann Halmrasts vei 7, 1300 Sandvika
Tel. +47 67 21 69 00

Ski:
Jernbaneveien 4, 1400 Ski
Tel. +47 64 91 41 41