Cloud Computing kontrakter

Vejledning om juridiske, kommercielle og tekniske forhold i aftaler om Cloud Computing (2. Udgave)

DANSKE ADVOKATER

dansk·it

Cloud Computing kontrakter

Vejledning om juridiske, kommercielle og tekniske forhold i aftaler om Cloud Computing

 Udgivelse: januar 2016 (2. udgave)

Forfattere:
Niels Chr. Ellegaard, certificeret it-advokat, Plesner
Per Andersen, forhenværende direktør, DANSK IT
Steen Andersen, it-direktør, Nilfisk
Steen Hermansen, digitaliseringschef, Danske Advokater

Layout:
DANSK IT

Kontakt:
Danske IT-advokater
Vesterbrogade 32
DK 1620 København V
Tlf: +45 3343 7000
forening@danskeadvokater.dk
www.itadvokater.dk

DANSK IT
Bredgade 25a
DK 1260 København K
Tlf: +45 3311 1560
dit@dit.dk
www.dit.dk

Indhold

1. Indledning

Cloud computing er for alvor kommet på dagsordenen hos de fleste virksomheder og it-leverandører i Danmark og i udlandet. Mange har dog stadig betænkeligheder ved cloud computing og har vanskeligt ved at overskue konsekvenserne ved at anvende løsninger baseret på cloud computing i deres virksomhed.

Cloud computing er ikke ny teknologi, men en anden måde at anvende eksisterende teknologi på, hvor brugeren (”Kunden”) på væsentlige punkter overlader kontrollen til leverandøren af it-ydelsen (”Leverandøren”) og kommer ind i en standardiseret og færdigpakketeret verden af ”services”. Kundens formål med at overlade denne kontrol til Leverandøren er at opnå de fordele i form af fleksibilitet, skalerbarhed, stabilitet og omkostningsbesparelser, som cloud computing i mange tilfælde vil give.

Formålet med vejledningen er at give Kunden en forholdsvis let og overskuelig vejledning i forhold til de spørgsmål, der bør stilles, og overvejelser, der bør gøres, før Kunden går ind i en løsning baseret på cloud computing (”Cloudløsningen”).

Det særlige ved cloud computing er, at juridiske, kommercielle og tekniske forhold vanskeligt kan skilles ad. Om en konkret Cloudløsning er det rette valg for Kunden, afhænger derfor ikke blot af en teknisk vurdering af Cloudløsningen, men også af juridiske, finansielle og strategiske overvejelser.

Vejledningen tager ikke stilling til, om cloud computing er en bedre eller ringere løsning for Kunden i forhold til alternativerne. Der kan i forhold til cloud computing peges på mange risici, men disse skal altid sammenholdes med fordelene. Endvidere vil mange af de risici, der redegøres for i vejledningen, genfindes i almindelig outsourcing og inden for traditionel it. Kunden bør derfor ikke fravælge en Cloudløsning alene på grundlag af identificerede risici, hvis disse risici også eksisterer i forhold til de alternative løsninger, som måtte findes. Vejledningen er med andre ord en checkliste og et ”inspirationskatalog” for Kunder, der ønsker at tage en Cloudløsning i brug.

Vejledningen retter sig først og fremmest til dem, som skal indgå og bruge kontrakten vedrørende Cloudløsningen (”Kontrakten”), og er skrevet ud fra et ønske om, at den skal kunne læses og bruges af både jurister og ikke-jurister. Vejledningen kan

ikke træde i stedet for konkret rådgivning, men det er hensigten, at vejledningen skal kunne give Kunden et grundlag for selv at gøre sig sine overvejelser og fokusere på de rigtige spørgsmål.

Vejledningen er blevet til i et samarbejde mellem DANSK IT og Danske IT-advokater, og arbejdsgruppen har bestået af Certificeret IT-advokat fra Danske IT Advokater Niels Chr. Ellegaard (Plesner), forhenværende Direktør i DANSK IT Per Andersen, IT-direktør i Nilfisk-Advance Steen Andersen og Digitaliseringschef i Danske Advokater Steen Hermansen.

Vejledningen blev første gang publiceret i september 2014, og denne anden udgave indeholder en række opdateringer, herunder i forhold til ændringer i bogførings-loven og inden for persondataretten. Endvidere er vejledningen udbygget med et afsnit om kontraktstyring og uddybning af afsnittet om sikkerhed.

2. Hvad er cloud computing?

Der findes ikke en generelt anvendelig og alment accepteret definition af, hvad cloud computing er. De fleste anvender dog cloud computing som et begreb for it-løsninger, der leveres som tjenester i stedet for produkter. Cloudløsninger er normalt kendetegnet ved, at

- De tilgås direkte via internettet
- Servicen betales efter forbrug
- Forbruget kan reguleres op og ned i Kontraktens løbetid, og
- Tjenesten leveres fra Leverandørens platform af puljede computerressourcer

I hvilket omfang nævnte kendetegn gælder for den konkrete it-løsning, afhænger dels af den tekniske løsning og dels af Kontrakten.

Normalt inddeles Cloudløsninger i tre kategorier:

- Software as a service (SaaS): Hvor Leverandøren stiller en tjeneste til rådighed i form af applikationer, som bliver hostet, drevet og vedligeholdt af Leverandøren
- Platform as a service (PaaS): Hvor Leverandøren som en tjeneste stiller en webbaseret platform til rådighed som en tjeneste for Kunden. Platformen indeholder basissoftware, som gør det muligt for Kunden at lægge sine egne applikationer på platformen
- Infrastructure as a service (IaaS): Grundlæggende infrastrukturtjenester stilles til rådighed med henblik på, at Kunden kan installere egen basissoftware og applikationer

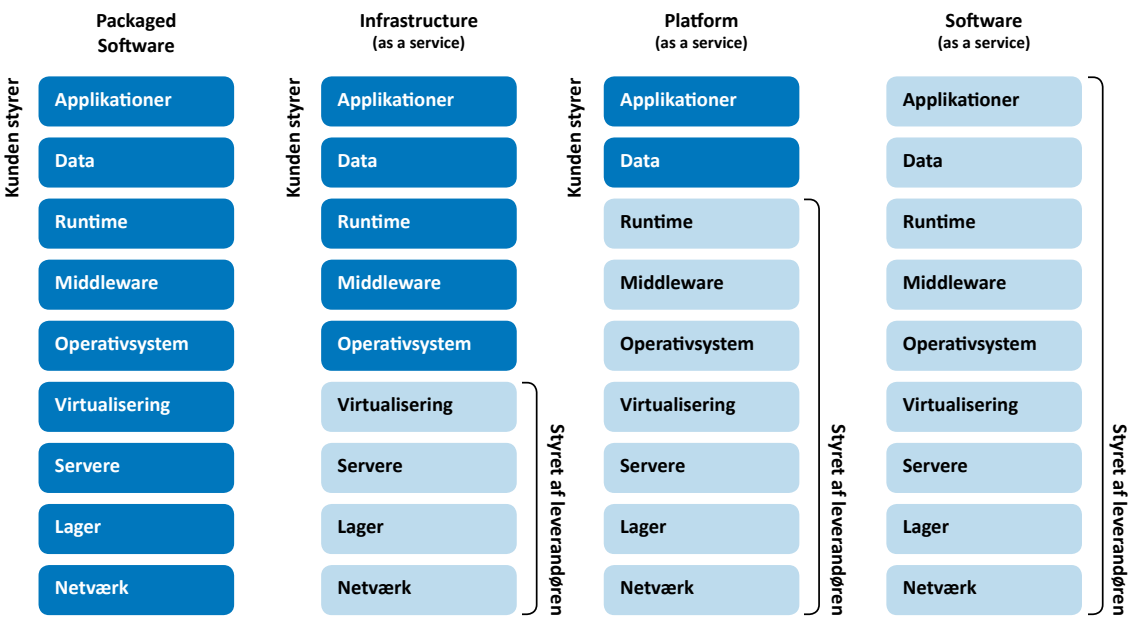
Anvendelsen (”deployment”) af cloud ses i en række forskellige varianter i form af:

- Public cloud: Tjenstesterne leveres fra en offentlig tilgængelig infrastruktur (åbent netværk) med fælles standardiserede platform og infrastruktur
- Private cloud: Tjenesterne leveres fra en ikke-offentlig tilgængelig infrastruktur (lukket netværk) med platform og infrastruktur tilpasset den enkelte Kunde
- Community cloud: Tjenesterne leveres fra en infrastruktur, som er tilgængelig for en bestemt gruppe (community) med platform og infrastruktur tilpasset gruppen

Kombineres disse anvendelsesmodeller, tales der om hybridmodeller.

Normalt vil det være sådan, at jo højere oppe i "stakken" man kommer, jo mindre kontrol vil man have med Cloudløsningen. Det vil sige, at en IaaS-løsning giver en større grad af kontrol og frihed end en SaaS-løsning, da Kunden i IaaS selv kan styre og kontrollere styresystemer og applikationer.

Cloud services:



3. Hvordan adskiller cloud sig fra andre it-ydelser?

I princippet er der ikke forskel mellem en Cloudløsning (SaaS) med en applikation solgt som software as a service og en løsning, hvor Kunden selv køber applikationen og driver denne på sin egen hardware og tilkøber vedligeholdelse og support.

For at Kunden kan komponere sin egen it-ydelse, skal Kunden således normalt:

- købe en softwarelicens
- implementere og tilpasse den købte software
- installere og drive applikationen,
- foretaget vedligeholdelse og videreudvikling, og
- købe support hos leverandørerne

I en Cloudløsning leveres hele pakken som en færdig og forædlet tjenesteydelse fra Leverandøren, og Kunden har ikke som sådan indflydelse eller kontrol over produktionen.

For at Leverandøren kan levere denne færdigpakketerede tjeneste (service) til Kunden, er det nødvendigt i væsentligt omfang at acceptere de standardløsninger og valg, som Leverandøren har gjort på vegne af alle de Kunder, der benytter Cloudløsningen.

Der vil i de fleste Cloudløsninger være mulighed for at foretage parameter-opsætninger og i et vist omfang foretage tilpasninger, som anvendes sammen med løsningen via en grænseflade (API). I det væsentlige må Kunden dog regne med, at det er en standardløsning, der købes, og at der derfor ikke kan foretages særlige tilpasninger i forhold til Kunden, hvilket gælder både i forhold til selve løsningen, men også i forhold til servicemål og support, der stilles til rådighed.

Den afgørende forskel mellem cloud computing og traditionelle it-ydelser er således, at de ydelser, som Kunden normalt selv skal kombinere, leveres som en tjenesteydelse (service) i form af en samlet færdig pakke.

4. Grundlæggende overvejelser

4.1 Fordele ved cloud computing

De væsentligste fordele, der normalt kan opnås ved anvendelse af Cloud-løsninger, er

- begrænsede eller ingen tekniske kapital- og opstartsomkostninger (se dog om implementeringen af Cloudløsningen nedenfor)
- betaling i henhold til forbrug
- fleksibilitet i forhold til op- og nedskalering af computerressourcer
- mulighed for varierende aftalelængder
- mulighed for at operere med "tynde klienter"
- mulighed for full-service løsninger og servicemål, hvor hele løsningens performance er inkluderet
- mulighed for anvendelse af Leverandørens skalafordele (det vil sige anvendelse af Leverandørens serverkapacitet)
- løbende softwareopdateringer uden ekstraomkostninger
- andre sædvanlige outsourcingfordele (sikkerhed for oppetid, tilgængelighed, back up, nødberedskab mv.)
- miljømæssige fordele (CO_2 reduktion ved at pulje it-løsninger i store datacentre)

4.2 Ulemper ved cloudløsninger

Som modstykke til de nævnte fordele ved cloud computing skal Kunden samtidig forholde sig til de ulemper, som er ved anvendelse af cloud computing:

- risiko for at de lave opstartsomkostninger bliver "spist" af løbende omkostninger ved køb af abonnement over en længere periode
- tab af kontrol i forhold til udvikling og softwareændringer
- tab af kontrol i forhold til drift
- ingen mulighed for at "stå af toget" (der skal betales løbende - Kunden er nødt til at have abonnementet)
- sårbarhed i forhold til at den samlede løsning skal leveres af én Leverandør ("lock-in")
- trafikomkostninger i forhold til transport af data
- sårbarhed og afhængighed i forhold til at være online (have internetadgang)
- sikkerhedsrisici i forhold til uvedkommendes adgang til Cloud-løsningen
- vanskeligheder i forhold til integration med andre applikationer og systemer
- begrænsede muligheder for tilpasninger
- risiko for manglende adgang til egne data ved ophør og overførsel af disse til Kunden selv eller ny Leverandør (Hvor sikker kan Kunden være på at kunne få rådighed over sine data, når Kontrakten ophører), og
- regulatoriske/compliance risici i forhold til behandling af personoplysninger i Cloudløsningen, se nærmere herom i afsnit 12 og 13 nedenfor.

4.3 Kundens indledende selvevaluering af behov og risici

For at Kunden kan forholde sig til det samlede billede af fordele og ulemper ved anvendelse af en Cloudløsning, bør Kunden i forhold til den Cloudløsning, som Kunden overvejer at tage i anvendelse, som minimum stille følgende spørgsmål:

Understøttelse af forretningen

- I hvor stor udstrækning er det fra Kundens side acceptabelt, at forretningsprocesserne tilpasses softwaren og ikke omvendt?

Krav til serviceniveau (afsnit 10 og 11)

- Er det system, som Cloudløsningen erstatter (eller den nye funktion Cloudløsningen opfylder), kritisk for Kundens virksomhed (vil Kunden uafhængigt af Cloudløsningen rimeligvis kunne videreføre sin virksomhed)?
- Harmonerer servicemål i forhold til oppetid og tilgængelighed med de servicemål, som Kunden anvender for de øvrige systemer/applikationer?

IT-arkitektur og integration (afsnit 8 og 9)

- Hvordan passer Cloudløsningen ind i Kundens eksisterende systemlandskab?
- Kan Cloudløsningen integreres med andre centrale systemer og applikationer hos Kunden?
- Hvor vigtigt er det for Kunden, at Cloudløsningen kan tilpasses Kundens andre applikationer og systemer (er standard tilstrækkelig)?

Økonomisk kalkule (afsnit 6, 7 og 16)

- Hvad er økonomien på kort, mellemlang og lang sigt ved at tage en traditionel løsning i brug sammenlignet med omkostningerne ved køb af Cloudløsningen (vil det kunne svare sig at købe løsningen som en Cloudløsning, eller bliver de umiddelbare fordele "spist op" af de løbende omkostninger ved Cloudløsningen)?
- Er der væsentlige implementeringsomkostninger forbundet med at tage Cloudløsningen i anvendelse, herunder i forhold til integration med anden software og forandring af forretningsprocesser?

Sikkerhed og compliance (afsnit 12 og 13 samt bilag 1)

- Er Leverandørens sikkerhedsniveau tilfredsstillende (er det tilfredsstillende både i forhold til adgangskontrol, databehandling samt nød- og katastrofeberedskab)?

- I hvilke lande skal data opbevares eller tilgås fra?
- Har Kunden behov for at kunne dokumentere opfyldelse af særlige regulatoriske krav eller compliancevilkår i forhold til behandling af data?

Exit (afsnit 14-17)
- Hvordan kommer Kunden ud af Cloudløsningen?
- Er der bindinger, der skaber lock-in?
- Har Kunden behov for særlige rettigheder til software efter ophør af Kontrakten?

Kontraktstyring (afsnit 18)
- Hvordan administreres Kontrakten?

4.4 Detaljeret evaluering af Cloudløsningen

Når Kunden har foretaget den indledende selvevaluering af egne behov og en overordnet risikovurdering, bør Kunden tage stilling til, om Kunden ønsker at gå ind i en dybere undersøgelse af Cloudløsningens fordele og ulemper.

Det afgørende er, at Kunden i sin tilgang får stillet de rigtige spørgsmål i rette tid således, at det undgås, at der enten ikke investeres unødig tid og ressourcer i undersøgelse af en Cloudløsning, som alligevel ikke vil opfylde Kundens behov, eller at Kunden først for sent bliver opmærksom på Kundens egne behov og krav til risici, ikke er afstemt med det, som Leverandøren af Cloudløsningen kan tilbyde.

I den følgende del af vejledningen vil de enkelte elementer i Cloudløsningen blive gennemgået i forhold til de mere deltaljerede overvejelser, som man som Kunde bør gøre sig, hvis man vil tage en Cloudløsning i anvendelse.

5. Typer af cloudkontrakter

5.1 Kan Kontrakten forhandles?

En stor del af de Cloudløsninger, som kan købes i dag, leveres på grundlag af standardvilkår, som ikke eller kun vanskeligt kan forhandles med Leverandøren. Baggrunden herfor er, at Leverandørens forretningsmodel er baseret på salg af rene standardprodukter, og dels at produktet grundlæggende er nødt til at være ens for alle Kunder, da Leverandøren ellers ikke vil opnå de stordriftsfordele, der er forbundet med at levere it-løsningen som en Cloudløsning. Der findes dog også Cloudløsninger, som kan købes efter tilpassede vilkår, og hvis den volumen, som Kunden vil købe, er tilstrækkelig stor, vil visse af vilkårene også kunne forhandles.

Det første, Kunden derfor bør undersøge, er, om Kontrakten kan gøres til genstand for forhandling, eller om Kunden er nødt til at tage Kontrakten, som den er.

5.2 Er kontraktgrundlaget modent?

Ved vurdering af Kontrakten er det samtidig vigtigt, at Kunden undersøger, om kontraktgrundlaget er tilstrækkeligt gennemarbejdet. Der er i markedet i dag en lang række Leverandører, som enten er nye i markedet, eller er ved at konvertere fra en traditionel it-leverancemodel til en cloudbaseret leverancemodel. Er der tale om sådanne umodne Leverandører, skal Kunden dels være opmærksom på, om Leverandøren rent faktisk kan levere en tilfredsstillende ydelse, hvis procedurerne ikke er beskrevet tilstrækkeligt præcist, og dels skal Kunden sikre sig, at der forhandles et konsistent og tilfredsstillende sæt vilkår.

5.3 Hvad gør man, hvis Kontrakten ikke kan forhandles

Hvis det må konstateres, at Kontrakten ikke kan forhandles, består Kundens opgave i at foretage en vurdering af, om det tilbudte produkt udover at leve op til Kundens tekniske krav også lever op til de krav, som Kunden har stillet i forhold til risici, og til de regulatoriske krav til Kontraktens indhold. En sådan vurdering kan enten føre til, at Kunden skal afstå fra at indgå Kontrakten, fordi risikoen er for stor/manglende compliance, eller at risikoen er håndterbar sammenholdt med investeringens størrelse og betydningen af de involverede data.

5.4 Internationale kontrakter

En stor del af Leverandørerne af Cloudløsninger vil ikke være hjemmehørende i Danmark, og Cloudløsninger er netop kendetegnet ved at have et internationalt salgspotentiale. Det gør samtidig, at Kontrakten ofte er undergivet udenlandsk ret, og at udenlandske domstole eller voldgifter er indsat som de retsinstanser, der skal afgøre eventuelle tvister.

Som i alle andre kontraktforhold bør Kunden også have øje for, om en reel håndhævelse af Kontrakten er (økonomisk) mulig, herunder i forhold til kontraktværdien af Kontrakten.

6. Cloudløsningens implementering

6.1 Omfanget af den nødvendige implementering

De fleste Kunder (om ikke alle) er opmærksomme på, at traditionelle it-løsninger skal implementeres for at kunne anvendes i virksomheden. Det samme gælder Cloudløsninger, og det er derfor vigtigt, at Kunden får analyseret, hvilket omfang Cloudløsningens implementering vil have i det konkrete tilfælde.

Indledningsvist er det væsentligt at få afdækket, om Cloudløsningen understøtter de processer, som Kunden ønsker løst, ved at tage Cloudløsningen i anvendelse. Hvis der er et "gap", mellem det Cloudløsningen kan tilbyde og de funktioner og processer, som Kunden har behov for at få dækket, er det første spørgsmål, om det i det hele taget er muligt at udvikle særlig funktionalitet, der kan dække et sådant gap, herunder om denne funktionalitet kan etableres i regi af Leverandøren.

Kunden bør også i den forbindelse, uanset om Cloudløsningen opfylder samtlige af Kundens behov, undersøge fleksibiliteten i Cloudløsningen i forhold til at kunne indgå i Kundens udviklingsplaner, hvis behovene hos Kunden ændrer sig.

Når behovsopfyldelsen er afklaret, bør de samlede omkostninger ved implementering, herunder i forhold til parameteropsætning, træning og integration med Kundens andre it-løsninger vurderes med henblik på at vurdere den samlede økonomi i anskaffelsen.

6.2 Hvordan håndteres implementeringsrisikoen

En særlig problemstilling er, hvem der skal påtage sig implementeringsrisikoen. I traditionelle it-projekter eller udviklingsprojekter vil Leverandøren normalt have implementeringsrisikoen, således at Leverandøren først anses for at have leveret, når det tilpassede standardsystem er accepteret af Kunden.

De fleste cloudkontrakter indeholder ikke en sådan fordeling af risikoen. Omvendt vil Cloudløsningen i mange tilfælde kunne opsiges med meget kort varsel, hvilket giver Kunden den fornødne frihed til at komme ud af Kontrakten, hvis implementeringen ikke kan gennemføres til Kundens tilfredshed.

Kunden skal også ved udarbejdelsen af sin business case være opmærksom på, at nogle Leverandører - ligesom ved licenskøb - kræver, at adgang til Cloudløsningen er erhvervet allerede for tidspunktet for påbegyndelse af implementeringen. Kunden kommer dermed til at betale for Cloudløsningen, selvom den ikke er i produktion hos Kunden.

Hvis Kontrakten er genstand for forhandling, bør Kunden søge enten at opnå en aftale om betaling efter forbrug (eksempelvis betaling for testbrugere) eller at udskyde tidspunktet for betaling for anvendelse af Cloudløsningen, indtil implementeringen er gennemført, og i øvrigt sikre sig, at Kunden ikke er bundet af Kontrakten, hvis implementeringen ikke lykkedes.

6.3 Særligt om ansvarsfordelingen

Hvis implementering gennemføres af en anden end Leverandøren af selve Cloudløsningen, er det ligesom i traditionelle it-projekter vigtigt at forholde sig til implementeringsrisikoen.

Uanset at selve Kontrakten for Cloudløsningen ikke kan forhandles, vil implementeringsaftalen normalt både kunne og skulle forhandles, og Kunden bør her sikre sig, at der er en rimelig risikofordeling mellem Kunden og den part, der påtager sig implementering.

7. Afregningsmekanismer ved brug af Cloudløsningen

7.1 Licensmæssige aspekter

Det særlige ved cloud computing er, at der er tale om en tjeneste (service), hvor Kunden får adgang til en it-løsning, som drives og vedligeholdes af Leverandøren. Betaling for brug kan derfor bedst sammenlignes med et abonnement ("subscription"), og er en løbende betaling for adgang til Cloudløsningen.

Da det er selve adgangen, man betaler for, er der teknisk set ikke tale om en licensaftale. Selve adgangen til at bruge den it-ydelse, som leveres, som en del af Cloudløsningen, indebærer imidlertid en form for licens for Kunden. Grundlæggende kan Cloudløsningen afregnes efter (i) antallet af brugere, (ii) forbrug, (iii) kapacitet, (iv) transaktioner, (v) tilgængelig funktionalitet eller en kombination af disse. Kunden bør forstå afregningsmodellen og prismekanismerne for Cloudløsningen. Typisk har Leverandørerne hver deres unikke måde at afregne efter, og Kunden bør derfor sikre sig, at det er klart, hvad Leverandøren forstår ved forbrug, brugere eller lignende under Kontrakten.

Uanset om der afregnes efter antal brugere, forbrug eller en kombination heraf, skal Kunden sikre sig, at der vil være adgang for alle relevante brugere hos Kunden. Det gælder både ansatte, men også indlejede konsulenter og tredjemandsleverandører (leverandører som leverer andre it-ydelser til Kunden).

Er der tale om brugerbaseret afregning, bør det ligesom ved licensaftaler undersøges, om afregning sker i forhold til samtidige eller unikke brugere. Kunden bør også sikre sig, at afregninger er overskuelige og kan valideres, hvilket kan efterprøves ved at få et eksempel på afregning. Det anbefales, at Kunden får indbygget spærremekanismer eller alarmer i forhold til forbrugsbaseret afregning med henblik på at undgå negative overraskelser.

7.2 Rettigheder til Cloudløsningen efter ophør

I modsætning til traditionelle it-løsninger, hvor Kunden køber en evigtvarende licens til software, har Kunden som udgangspunkt ingen rettigheder til brug af software, når Kontrakten vedrørende Cloudløsningen ophører. Dette er som regel ikke et problem, men Kunden skal gennemtænke, om der er behov for
at beholde adgang til systemet efter ophør af ordinær brug med henblik på opbevaring og tilgang til arkivdata. Endvidere kan der være behov for adgang til løsningen, indtil en migrering til en anden løsning er endeligt gennemført, hvilket også bør sikres via Kontrakten.

7.3 Andre relevante forhold – hvad er ikke med?

I tillæg til betaling for adgang til Cloudløsningen kan der være et behov for tilkøb af supplerende produkter i form af support og lignende, som ikke nødvendigvis indgår i selve Cloudløsningen.

Yderligere er det ofte sådan, at Leverandøren har en række forskellige versioner af Cloudløsningen eller en modulbaseret struktur, som indebærer, at Kunden kan tilkøbe yderligere funktionalitet. Da Cloudløsningen som en del af ydelsen løbende opdateres og opgraderes, er det væsentligt for Kunden at afklare, i hvilket omfang tilkøb af moduler eller funktionalitet vil blive nødvendigt, og hvad det i givet fald vil koste. Dette kan ske ved at bede om en udtømmende prisliste over samtlige af Leverandørens ydelser.

Leverandøren vil (og kan ej heller) redegøre for, hvordan det fremtidige ydelseskatalog vil se ud, herunder om der senere vil blive tilbudt funktionalitet eller ydelser, som bliver tilkøb og dermed er uden for Cloudløsningen. Det Kunden imidlertid bør sikre er, at Leverandøren ikke ændrer sit ydelsesudbud på en sådan måde, at den eksisterende funktionalitet i Cloudløsningen ”udhules” ved at opgraderinger af dele af løsningen efterfølgende tilbydes som særskilt betalbare moduler. Leverandøren vil på sin side have behov for en stor grad af frihed til at designe sit produktudbud

til at møde konkurrencen og behovet i markedet, men de fleste Leverandører vil tilbyde, at Cloudløsningens funktionalitet ikke vil blive forringet i Kontraktens løbetid.

Kunden bør sikre sig, at der kun betales for sådanne tilkøbte ekstraprodukter, så længe selve hovedydelsen, nemlig adgang til Cloudløsningen, er tilgængelig.

8. Snitflader/grænseflader mellem Cloudløsningen og andre applikationer/software

8.1 Behovet for integrationer

Et væsentligt aspekt ved Cloudløsningen er, at de data, der behandles, i mange tilfælde skal kunne bruges i andre applikationer eller sammenhænge. Behovet for integrationer er helt afhængig af, hvilken Cloudløsning der er tale om.

Er der tale om en IaaS-løsning, vil Kunden i langt højere grad selv kunne forestå integrationer, hvorimod integrationer fra en SaaS-løsning vil skulle basere sig på den pågældende Cloudløsning. Spørgsmålet om integrationer er vanskeligt, da det ikke blot kan afklares ud fra et øjebliksbillede (det vil sige, hvad har Kunden brug for på indkøbstidspunktet). Kunden bør også tænke langsigtet i forhold til at sikre, at behovet for eventuelle fremtidige integrationer kan opfyldes.

Derfor bør Kunden som minimum sikre sig, at Leverandøren tilbyder standard API'er til integration med de af Kundens øvrige applikationer, der skal eller potentielt kan tænkes at skulle integreres til. Hvis det ikke er tilfældet, og hvis der er mulighed for at forhandle Kontrakten, bør det indskrives, at Leverandøren er forpligtet til at udvikle de manglende API'er og/eller sørge for, at løsningen giver mulighed for ved brug af standard interfaces at gennemføre integration med andre applikationer, herunder andre Cloudløsninger. Alternativt bør Kunden sikre sig, at der i markedet findes 3. parts integrationsprodukter, der giver mulighed for standardintegrationer mellem den påtænkte SaaS løsning og andre udbredte Cloudløsninger i markedet og de af Kundens applikationer, som Cloudløsningen kan tænkes at skulle integreres til.

8.2 Hvad bør man teknisk sikre sig?

Typisk vil Kunden have behov for at undersøgende følgende spørgsmål:

- Er der i Cloudløsningen browserunderstøttelse af de browsere, som Kunden anvender, og vil anvende i fremtiden?
- Er der begrænsninger i forhold til det hardware, som Cloudløsningen kan tilgås fra?
- Er der med Cloudløsningen integration til sædvanlige tredjepartsprodukter såsom NemID?
- Kræver Cloudløsningen anvendelse af applikationer på terminalen (device), som anvendes af Kundens brugere til at tilgå Cloudløsningen?
- Kan der etableres AD-integration med single sign on (enten direkte eller via tredjepartsprodukter)?
- Er der ressourcekrav i forhold til de terminaler (devices), som benyttes til at tilgå Cloudløsningen?
- Vil der kunne skabes den fornødne hastighed på integrationer til andre systemer (skal de fornys for at skabe tilstrækkelig hastighed)?
- Hvilke former for API'er til udvikling af kundespecifikke løsninger stilles til rådighed ?
- Hvilke standard integrationsmuligheder stilles til rådighed?

9. Ændringer i ydelsen

Da det, som Kunden typisk køber, er adgangen til en standardløsning, er spørgsmålet om ændringer væsentligt. Grundlæggende kan spørgsmålet deles op i to:

1. I hvilket omfang kan jeg som kunde kræve ændringer, og
2. I hvilket omfang skal jeg som kunde tåle ændringer.

Mange Kontrakter med Leverandører er meget åbne i forhold til ændringsadgang, og giver Leverandøren adgang til at foretage ændringer med kort varsel eller af og til uden varsel. Kunden bør derfor nøje overveje, i hvilket omfang ændringer i Cloudløsningen ville kunne få indflydelse på andre af Kundens applikationer og systemer, og om selve Cloudløsningen er så vigtig for Kunden, at Kunden ligefrem skal kunne modsætte sig ændringer i Cloudløsningen.

I forhold til det første spørgsmål, om Kunden kan kræve ændringer, kan et sådant behov være foranlediget af, at Kunden får tilkøbt nye applikationer eller systemer, og/eller at opgradering af Cloudløsning er nødvendig for at kunne drive Kundens andre applikationer. Eksempelvis kan det i en IaaS eller PaaS Cloudløsning være en forudsætning, at basissoftware i Cloudløsningen er opgraderet til en nyere version, for at Kundens applikationer kan opgraderes til en højere version. Det kan derfor være tilsvarende vigtigt at sikre sig, at Kunden kan kræve ændringer i Cloudløsningen.

I det omfang der ikke efter Kontrakten kan kræves ændringer, eller Kunden ikke kan forhandle sig frem til en sådan mulighed, bør Kunden vurdere Cloudløsningen ud fra, om den fremstår tilstrækkelig robust, og om Leverandøren kan forventes at ville bevæge Cloudløsningen i den retning, som Kunden har behov for. Principielt ville spørgsmålet om ændringer ikke være af væsentlig betydning, hvis der ikke var "lock-in" eller exitbarrierer, da Kunden i tilfælde af manglende imødekommelse af Kundens behov ville kunne skifte til en anden Leverandør. Da der imidlertid netop ofte er sådanne "lock-in" effekter og vanskeligheder ved en exit, er dette forhold stadig af væsentlig betydning at få afdækket for Kunden.

10. Servicemål (SLA)

10.1 Betydningen af servicemål i Cloudløsninger

Servicemål spiller en central rolle i forhold til Cloudløsningen, da det netop er adgangen til løsningen, som er selve produktet. Man kan gå så vidt som at sige, at produktet er lig med servicemålet i den forstand, at tjenesten (i form af adgangen til service) ikke er bedre end de servicemål, der leveres. Kunden bør derfor fokusere på, hvilke servicemål, der garanteres eller stilles i udsigt fra Leverandørens side særligt i forhold til tilgængelighed og svartid, herunder i forhold til geografiske forhold.

Udover oppetid, tilgængelighed og svartid for selve Cloudløsningen er det også relevant at undersøge servicemål for blandt andet support og vedligeholdelse. Hvor hurtigt tilbyder Leverandøren at igangsætte udbedring af fejl, lover Leverandøren fejlrettelse eller workaround inden for en bestemt tidsperiode og lover Leverandøren at svare på supporthenvendelser indenfor en angivet tidsfrist?

Ikke alle Cloudløsninger tilbydes med garanterede servicemål, og i de fleste tilfælde vil de juridiske konsekvenser fastlagt i Kontrakten i forhold til manglende overholdelse af servicemål være begrænsede. Endvidere vil servicemål ofte kunne ændres af Leverandøren i Kontraktens løbetid, se afsnit 9 og 16.3 om ændringer i henholdsvis ydelsen og Kontrakten. Kunden er derfor nødsaget til i realiteten selv at påtage sig risikoen, medmindre der i markedet tilbydes mulighed for at købe ydelsen gennem en forhandler, der er villig til at garantere servicemål med tilhørende juridiske konsekvenser, som er tilfredsstillende for Kunden.

Hvis Kunden ikke kan afdække den juridiske risiko for Cloudløsningens tilgængelighed og svartid i Kontrakten, er Kunden henvist til at undersøge Leverandørens historiske performance, afprøve Cloudløsningen ved pilotprojekter eller ikke-kritiske applikationer eller begrænse anvendelse af Cloudløsningen til sådanne, sikre at der kan migreres relativt hurtigt og risikofrit til en alternativ løsning og lignende tiltag.

10.2 Måling

Det er ligeledes vigtigt at være opmærksom på, hvorledes oppetid, tilgængelighed og svartid måles fra Leverandørens side, og hvordan dette kan verificeres:

- Måler Leverandøren forskellige steder i verden, eller måles der kun ud af et konkret datacenter/land?
- Hvilket udstyr anvender Leverandøren til at måle med, herunder enhed (device), browser, version og anvendt tredjepartssoftware?

Der kan være forskelle på, hvad der opleves i Leverandørens ende, og hvad Kunden oplever, da ydelsen typisk aftages via internettet, hvor kapacitet, kvalitet og forsinkelser påvirker oplevelsen.

Endvidere er mange servicemål betingede og undtager særlige situationer fra måleperioden eller opererer med lange måleperioder, som udvander værdien af servicemålet. Et eksempel herpå er, at andre kunders adfærd, eksempelvis ved afvikling af store uannoncerede jobs, påvirker oplevelsen kortvarigt, uden at det kan ses i de offentliggjorte målinger af servicemål.

10.3 Konsekvenser ved manglende opfyldelse af servicemål

Ofte vil Leverandører af Cloudløsninger lade manglende opfyldelse af servicemålene udløse en form for reduktion i vederlaget, hvilket kan sammenlignes med enten en bod eller et forholdsmæssigt afslag i ydelsen. Det er også ofte sådan, at denne reduktion i vederlaget angives at være den eneste sanktion og konsekvens af manglende opfyldelse af servicemål. Kunden skal derfor være meget opmærksom på, hvad konsekvenserne af i øvrigt tilfredsstillede servicemål er i Kontrakten, og om Kunden kan leve med en begrænset beskyttelse ved ikke at have adgang til at kræve erstatning for manglende adgang til Cloudløsningen. Kunden bør også vurdere, om det vil være praktisk muligt at håndhæve sanktionen. Det kan eksempelvis være problematisk, hvis Kontrakten er undergivet domstole i udlandet.

I det omfang Kontrakten ikke er genstand for forhandling, er Kunden overladt til at foretage en risikovurdering af Leverandøren, herunder baseret på Leverandørens historik, jf. ovenfor.

10.4 Anbefaling i forhold til servicemål

Undersøg nøje hvilke servicemål (om nogen) der garanteres for Cloudløsningen i forhold til oppetid, tilgængelighed og svartid, og hvordan performance måles. Bed om oplysninger om Leverandørens historiske performance. Undersøg også hvilke servicemål der er for support og vedligeholdelse, og i øvrigt hvilke sanktioner der er ved Leverandørens manglende overholdelse af servicemål. Hvis de juridiske konsekvenser er begrænsede og ikke kan forhandles, må Kunden forlade sig på Leverandørens historik, afprøve Cloudløsningen indtil Kunden føler sig tilstrækkelig komfortabel med den og i øvrigt sikre sig, at en exit kan foretages sikkert, hurtigt og effektivt uden væsentlige omkostninger.

11. Erstatningsansvar og ansvarsbegrænsninger

11.1 Baggrunden for Leverandørens ansvarsbegrænsninger

De fleste Cloudløsninger er i deres udgangspunkt tænkt som masseprodukter, og Leverandørerne har derfor i deres standardvilkår i Kontrakten indføjet ansvarsbegrænsninger, som i meget væsentligt grad begrænser Leverandørens ansvar for ydelsen. Leverandørernes baggrund for at gøre dette er typisk begrundet i, at der i prisen for tjenesterne ikke er indregnet en risikopræmie for Kundernes tab ved brug af tjenesterne, og at det, som Kunderne køber, ikke er en "forsikring" mod skade. Problemstillingen svarer til den, som kendes fra outsourcing- og udviklings/implementeringskontrakter, men for Cloudløsninger gør der sig det særlige gældende, at Leverandørerne i endnu højere grad har begrænset muligheden for at kræve erstatning.

11.2 Indholdet af ansvarsbegrænsninger

Ansvarsbegrænsningerne er forskellige for de enkelte Leverandører, men har typisk følgende indhold:

- Kunden kan ikke kræve erstatning for indirekte tab, som normalt defineres som driftstab, tabt fortjeneste, tab af goodwill og lignende
- Det samlede erstatningsansvar er beløbsmaksimeret svarende til den faktiske betaling eller betaling for en nærmere bestemt periode (eksempelvis 12 måneders vederlag)

Typisk vil det være anført, at begrænsningerne ikke gælder ved grov uagtsomhed eller forsæt fra Leverandørens side

11.3 Konsekvensen af ansvarsbegrænsninger

Ansvarsbegrænsningerne er typisk enten meget vanskelige at forhandle eller ikke mulige at ændre. Juridisk set står Kunden derfor typisk i den situation, at Kunden afgiver kontrol, men at det juridiske ansvar (erstatningsansvar) ikke følger med i fuldt omfang, og Kunden må derfor beslutte, om Cloudløsningen er så robust, at Kunden kan acceptere den juridiske risiko, der ligger i anvendelse af Cloudløsningen.

En god måde at anskue situationen på er at gennemtænke et scenarie, hvor Kunden selv har kontrol over de ydelser, som Cloudløsningen leverer, sammenholdt med en situation, hvor Leverandøren har kontrollen. I de fleste tilfælde vil Kunden have den samme forsikringsdækning (eller mangel på samme) i forhold til dækning af driftstab mv. Den afgørende forskel bliver derfor, om Kunden, hvis Kunden selv var i kontrol, kunne have afværget de begivenheder, som afstedkommer tabet, eller eventuelt kunne have gjort det hurtigere og mere effektivt end Leverandøren. Dette skal så sammenholdes med omkostningerne ved et sådant beredskab. Det afgørende bliver således, om Leverandøren kan bevise, at Leverandørens beredskab er lige så godt, som det Kunden selv etablerer, hvis Kunden selv havde drevet Cloudløsningen.

I kontrakter vedrørende Cloudløsninger ses typisk også bestemmelser om, at betaling af bod for manglende overholdelse af servicemål er den eneste juridiske sanktion, og at der derfor slet ikke kan gøres et erstatningsansvar gældende, udover de aftalte bodsbeløb.

Hvis Kunden som følge af ansvarsbegrænsninger er overladt den juridiske risiko, er Kunden henvist til at undersøge Leverandørens historiske performance, afprøve Cloudløsningen ved pilotprojekter eller ikke-kritiske applikationer, begrænse anvendelse af Cloudløsningen til ikke-kritiske applikationer, sikre at der kan migreres relativt hurtigt og risikofrit til en alternativ løsning og lignende tiltag.

Kunden bør gennemgå og afdække ansvarsbegrænsningerne og foretage en risikovurdering, som dels går på, hvordan Kunden ville være stillet, hvis Kunden selv havde drevet Cloudløsningen, sammenholdt med hvis denne drives af Leverandøren. Kunden bør derefter vurdere, om Leverandørens beredskab er passende i forhold til den risiko, Kunden ønsker at løbe, og om prisen for ydelsen for Kunden afspejler det forhold, at Kunden ikke får dækning for de risici, som Kunden løber ved at tage Cloudløsningen i anvendelse.

12. Håndtering af data og persondata

12.1 Indledning

Et af de centrale spørgsmål ved anvendelse af Cloudløsninger har historisk været og er stadig spørgsmålet om behandling af data, herunder ikke mindst persondata.

Problemstillingerne vedrørende behandling af data adskiller sig ikke væsentligt fra de problemstillinger, som kendes fra behandling af data i et outsourcingforhold. Der er derfor ikke som udgangspunkt persondataretlige grunde til at fravælge cloud computing til fordel for anden form for outsourcing. I persondatalovens forstand er Kunden typisk dataansvarlig, og Leverandøren bliver dermed databehandler for Kunden som dataansvarlig. Behandler Kunden i forvejen data for andre (og er dermed selv databehandler), bliver Leverandøren underdatabehandler for Kunden.

Anvendelse af databehandlere stiller en række krav til Kunden, som blandt andet har pligt til at sikre sig, at det i Kontrakten anføres, at Leverandøren alene handler efter instruks fra den dataansvarlige, og at der træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbrug eller i øvrigt behandles i strid med persondataloven (persondatalovens § 41, stk. 3). Der henvises i øvrigt til afsnit 13 nedenfor vedrørende sikkerhed.

Persondatalovens § 41, stk. 3:

> *"Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere."*

Er der tale om "følsomme" oplysninger som defineret i lovens § 7 (oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold), kan der være behov for iagttagelse af særlige sikkerhedsforanstaltninger.

Anvendes Cloudløsningen til at behandle persondata, skal Kunden vurdere, om Kontrakten indeholder en forpligtelse for Leverandøren til at etablere og opretholde de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Kunden må således vurdere, om sikkerheden i løsningen er tilstrækkelig god og ligger inden for rammerne af den risikovurdering og risikohåndtering, som Kunden selv anlægger ved sin egen behandling af persondata.

Er Kunden selv databehandler for en anden dataansvarlig, skal Kunden sikre, at de krav, som den dataansvarlige har stillet over for Kunden, også opfyldes ved Cloudløsningen. Der kan også være pligt til at indhente tilladelse fra Kunden til at bruge en underdatabehandler.

12.2 Den kommende persondataforordning

Kunden bør sikre sig i Kontrakten, at Leverandøren vil tilpasse sine ydelser og Kontrakten til at imødekomme de krav, som den nye persondataforordning vil kræve af parterne. Kunden bør i den forbindelse opnå klarhed over, om disse ændringer vil blive gennemført uden at dette medfører prisændringer eller ændring af andre vilkår af betydning for Kunden.

12.3 Særligt om bogføringsdata

Mange SaaS-løsninger indeholder funktioner, der opbevarer og behandler bogføringsdata. Bogføringsdata er omfattet af bogføringsloven, som stiller en række generelle og specifikke krav til bogføringen, således skal bogføringen blandt andet tilrettelægges og udføres således, at regnskabsmaterialet ikke ødelægges, bortskaffes eller forvanskes, ligesom det skal sikres mod fejl og misbrug (bogføringslovens § 6). På samme måde som med behandling af persondata bør Kunden undersøge, om der er truffet de fornødne foranstaltninger, som opfylder de generelle specifikke krav, der er i bogføringsloven, hvis der i Cloudløsningen behandles bogføringsdata, se bogføringslovens § 12, som nu gælder for såvel opbevaring i som uden for Danmark.

Efter § 12 i bogføringsloven gælder det, at regnskabsmaterialet skal opbevares på en sådan måde, at det uden vanskeligheder kan gøres tilgængeligt i Danmark for offentlige myndigheder mv., som har ret til at kræve indsigt i materialet.

Regnskabsmaterialet kan således i medfør af bogføringslovens § 12, stk. 2, opbevares i elektronisk form i udlandet (eller i Danmark), hvis den bogføringspligtige

1) Opbevarer materialet i overensstemmelse med bogføringsloven
2) Til enhver tid kan fremskaffe det i Danmark
3) Opbevarer eventuelle beskrivelser af benyttede systemer mv. (systembeskrivelser) og eventuelle adgangskoder i Danmark
4) Sørger for at regnskabsmaterialet udskrives eller stilles til rådighed i et anerkendt filformat.

I forhold til systembeskrivelser vil det være tilstrækkeligt at opbevare standardbeskrivelser, hvis der anvendes standardsystemer. I forhold til udskrift og filformat er det afgørende, at de offentlige myndigheder kan benytte materialet i deres kontrol- og efterforskningsarbejde.

Kunden bør ved anvendelse af Cloudløsninger, der benyttes til opbevaring af bogføringsmateriale, sikre sig, at Leverandøren i Kontrakten påtager sig at sørge for at Tjenesterne af Kunden kan anvendes i overensstemmelse med ovennævnte krav (uanset om bogføringsdata opbevares i udlandet).

12.4 Sektorspecifikke krav

Mange brancher er underlagt sektorspecifikke krav i forhold til behandling af data. Det gælder eksempelvis den finansielle sektor, som er forpligtet til at sikre, at data behandles efter vedtagne politikker og retningslinjer udarbejdet i henhold til lov om finansiel virksomhed. Tilsvarende gælder sundhedsloven for institutioner, virksomheder og personer, som agerer inden for sundhedsvæsenet, hvor Kunden skal sikre sig, at sådanne sektorspecifikke krav til databehandling også opfyldes.

12.5 Opbevaring og behandling af data i udlandet

12.5.1 Persondata

En væsentlig del af rationalet i anvendelse af Cloudløsninger er, at der etableres store datacentre, som benyttes til opbevaring af data for Kunderne under de enkelte Cloudløsninger. I Cloudløsninger baseret på public cloud vil det ofte være sådan, at data opbevares forskellige steder.

I forhold til behandling af persondata er det sådan, at behandling kan ske inden for EU/EØS, uden at dette kræver iagttagelse af særlige forhold. Det skyldes, at der via EU er vedtaget fælles regler for behandling af persondata, som sikrer en fælles minimumstandard for behandling af personoplysninger. Overføres persondata til lande uden for EU (eksempelvis USA eller Indien), er der - medmindre landet er godkendt som "sikkert tredjeland" - tale om overførsel til "usikre tredjelande". Overførsel til usikre tredjelande kræver efter persondatalovens regler, at der tilvejebringes et særligt grundlag (eksempelvis samtykke eller aftaleopfyldelse), eller at der ydes tilstrækkelige garantier til beskyttelse af de registreres rettigheder, hvilket bl.a. kan sikres ved standardkontrakter baseret på de såkaldte "EU model Clauses" eller ved brug af virksomhedens egne bindende virksomhedsregler ("Binding Corporate Rules"). I visse tilfælde skal der også indhentes tilladelse til en tredjelandsoverførsel hos Datatilsynet.

I forhold til USA er den særlige "Safe Harbour" ordning blevet kendt ugyldig af EU-domstolen i oktober 2015. En række leverandører, som har anvendt "safe

Harbour" ordningen har derfor ændret grundlaget for behandling af persondata eller er ved at omstille sig.

Persondataloven kræver, at Kunden ved, hvor persondata behandles. Dette kan give udfordringer i Cloudløsninger, hvor Leverandøren har mange datacentre spredt på flere forskellige geografiske lokationer og benytter dem efter eget valg til at opbevare Kundens persondata. En måde at løse problemstillingen på er derfor at bede Leverandøren om at give en lokationsgaranti ("location guarantee") eller oplysning om hvilke datacentre, der anvendes til behandling af Kundens data. Fjernadgang til en database sidestilles med en overladelse/ videregivelse af oplysningerne og adgang for personer i eksempelvis et servicecenter i Indien vil derfor kræve et særligt grundlag, hvis persondata kan tilgås fra servicecentret. Hvis EU-standardkontrakterne ("Model Clauses") anvendes uden ændringer, kræves der ikke tilladelse fra Datatilsynet. Foretages der imidlertid selv mindre ændringer i standardkontraktens bestemmelser, vil en sådan tilladelse skulle indhentes, hvilket vil indebære en væsentlig forsinkelse.

12.5.2 Bogføringsdata

I modsætning til tidligere er det nu ikke længere et krav, at bogføringsdata skal behandles i Danmark, medmindre der er indhentet tilladelse til behandling uden for Danmark. Se om kravene ovenfor i punkt 12.3.

12.5.3 Anbefaling

Kunden - og/eller dennes rådgiver - bør undersøge, hvor data fysisk opbevares og behandles. Hvis det drejer sig om persondata og behandlingen sker uden for EU/ EØS, skal Kunden sikre sig, at der i det fornødne grundlag hertil (f.eks. Model Clauses/Binding Corporate Rules). Er der tale om bogføringsdata, vil det være nødvendigt at opfylde kravene i bogføringslovens §12 uanset om bogføringsdata opbevares i eller uden for Danmark. Kunden bør i alle henseender søge at få afdækket konkret, i hvilke datacentre behandlingen sker. Ligeledes vil der efter omstændighederne være behov for at indhente tilladelse til en overførsel af persondata fra Datatilsynet.

13. Sikkerhed

13.1 Indledning

Et afgørende parameter i forhold til anvendelse af Cloudløsningen er, om Leverandørens sikkerhedsforanstaltninger og beredskab er fornødent, passende og tilstrækkeligt, herunder i forhold til Kundens egne risikovurderinger og de krav der stilles i henhold til gældende lovgivning. Dette krav må forventes at blive tillagt yderligere betydning under den nye persondataforordning.

De fleste leverandører vil have etableret sikkerhedskontroller, som baserer sig på ISO-standarder eller lignende, herunder eksempelvis ISO 27001 standarden. Denne standard er ikke udarbejdet med Cloudløsninger for øje, og der er derfor udviklet en "overbygning" (ISO 27018), der tilpasser kontrollerne i ISO 27001 til Cloudløsninger.

Hvis Leverandøren er ISO-certificeret betyder det, at en uafhængig tredjemand, som har ret til at certificere under den relevante ISO-standard, har undersøgt Leverandørens kontroller og processer og har fundet at de lever op til ISO-standarden.

En cerificering gives imidlertid altid med et nærmere bestemt omfang (scope) for øje, og Kunden bør derfor altid undersøge det såkaldte "statement of applicability" for certificeringen, hvis Kunden vil lægge ISO-certificeringen til grund.

Leverandørerne vil typisk kunne fremlægge revisionserklæringer og certifikater i forhold til overholdelse af sikkerhedskrav, eksempelvis erklæring efter standarderne ISAE 3402 eller SSAE 16. De nævnte standarder er generelle retningslinjer, som anvendes af revisorer og andre, der afgiver erklæringer vedrørende "assurance". Standarderne siger således ikke noget om, hvilke krav Kunden skal overholde, men derimod om, hvilken fremgangsmåde den der afgiver erklæringen (revisor eller lignende) vil følge og hvilke vilkår erklæringen er afgivet under.

Kunden bør ved Kontraktens indgåelse kræve at få fremlagt disse erklæringer og i øvrigt sikre sig i Kontrakten, at der løbende (eksempelvis en gang om året) gives Kunden kopi af erklæringerne. Kunden vil kunne bruge disse i sin egen it-revision og bør i den forbindelse sikre sig, at fremlæggelse af erklæringer så vidt muligt er koordineret med Kundens egen revision. Kunden bør i Kontrakten sikre sig, at der gives meddelelse ved "incidents", hvor sikkerheden er blevet brudt eller truet.

Kunden bør efter omstændighederne også se Leverandørens "disaster recovery" plan og sammenholde den med sin egen, således at de er koordinerede.

Som bilag 1 til vejledningen er til inspiration medtaget en liste over generelle sikkerhedskrav, som Kunden bør undersøge. Listen er således ikke udtømmende og undersøgelsen bør altid afstemmes med kritikalitet og Kundens egne (virksomhedsspecifikke) krav.

13.2 Kundens egne undersøgelser af sikkerheden, herunder ved audit

Da der ved anvendelse af Cloudløsninger typisk er tale om delte miljøer, vil det ofte give vanskeligheder for Kunden at kunne foretage en egentlig inspektion eller audit af Leverandørens faciliteter, men i medfør af persondataretten er det et krav, at der i et eller andet omfang er ret til dette. I større aftaler og/eller ved anvendelse af Cloudløsninger til brug for væsentlige, kritiske applikationer, vil Kunden kunne foretage videregående undersøgelser (en form for "due diligence") og kræve supplerende oplysninger og dokumentation fremlagt i forhold til de sikkerhedskrav, Kunden måtte stille, navnlig i forhold til beskyttelse af opbevaret data i Cloudløsningen. Sikkerhed dækker som minimum over følgende forhold:

- Sikkerhed for, at kun de rette får adgang til Kundens data
- Sikkerhed for, at løsningen er tilgængelig
- Sikkerhed for, at Kunden kan få sine data tilbage ved exit

Da der typisk ikke kan opnås en egentlig juridisk og tilstrækkelig sikkerhed for juridisk opfyldelse (erstatningsansvar) fra Leverandørens side, er Kundens undersøgelse og risikovurdering i forhold til Cloudløsningens sikkerhed af central betydning. Kunden må derfor tage stilling til, om resultatet af de foretagne undersøgelser er tilfredsstillende i forhold til Kundens risikovurdering og de gældende lovkrav (persondataloven mv.).

13.3 Virksomhedsspecifikke krav til sikkerhed

Lige som der i relation til spørgsmålet om behandling af data (navnlig persondata), kan der i den enkelte virksomhed være særlige krav til sikkerhed, som skal opfyldes i henhold til vedtagne sikkerhedspolitikker, -standarder og -procedurer. Sådanne politikker mv. kan være baserede på lovkrav, hvilket eksempelvis er tilfældet for finansielle virksomheder.

Kunden bør inden indgåelse af Kontrakten få verificeret opfyldelse af sådanne sikkerhedskrav, herunder eksempelvis i forhold til adgangsforhold (særligt administratorrettigheder) såvel elektronisk som fysisk baseret på egne obligatoriske sikkerhedskrav.

14. Exit

14.1 Indledning

Et centralt aspekt ved en Cloudløsning er, i hvilket omfang og på hvilken måde det vil være muligt at forlade Cloudløsningen og lade den erstatte af en ny løsning hos en anden Leverandør eller via en traditionel it-løsning, som Kunden selv driver.

Lige så vigtigt det er at sikre sig, hvorledes indtræden i Cloudløsningen kan ske (implementering, se afsnit 6 ovenfor), lige så vigtigt er det ved kontraktindgåelse at sikre sig, at man også kan komme ud af Cloudløsningen på sikker og effektiv vis og få sine data tilbage.

Kunden bør undersøge og få dokumenteret, hvorledes en exit kan foregå, herunder ved konkret beskrivelse af, hvordan data tilbageleveres ved ophør. Kunden bør også sikre sig, at der ydes support fra Leverandørens side i forhold til exit.

14.2 Adgang til data efter ophør

Det særlige ved cloud computing er, at der gives en adgang til løsningen, så længe Kontrakten varer. Der er med andre ord ikke mulighed for at fortsætte brugen af Cloudløsningen og få tilgang til data lagret i Cloudløsningen, når Kontrakten ophører.

Kunden bør forholde sig til, hvorledes de opbevarede data kan behandles, når Kontrakten er udløbet. I visse situationer vil det være muligt for Kunden at forhandle en løsning, hvor der opretholdes en begrænset adgang til Cloudløsningen, således at data fortsat kan opbevares som en form for arkivløsning.

15. Lock-in effekter ved brug af Cloudløsninger

Ved lock-in effekter forstås, at Kunden enten juridisk, teknisk eller kommercielt bindes til Leverandøren på en sådan måde, at det enten er umuligt eller vanskeligt for Kunden at skifte til anvendelse af en anden Cloudløsning med samme funktion eller hjemtage funktionen. Lock-in er ikke et fænomen, der kun gælder i forhold til cloud computing, og Kunden bør undersøge, i hvilket omfang der vil være tilsvarende lock-in effekter ved valg af alternativer til cloud computing. Typiske lock-in effekter kan blandt andet være:

- Der er ikke andre leverandører, der udbyder tjenester med den samme funktionalitet som Leverandøren (manglende substitution)
- Kunden har investeret store ressourcer internt og eksternt i forhold til at implementere Cloudløsningen (investering)
- Overgang til en ny Cloudløsning vil kræve en større implementeringsindsats (implementeringsbarrierer)
- Kunden har etableret integrationer mellem Cloudløsningen og sine andre systemer, som ikke kan anvendes ved overgang til en ny Cloudløsning eller ved hjemtagelse (afhængigheder til andre systemer)
- Data kan ikke udlæses i et anvendeligt format eller kan ikke udlæses på en sådan måde, at de er anvendelige i en ny løsning (datamigreringsbarrierer)
- Kunden er bundet af længerevarende bindingsperioder eller opsigelsesvarsler i Kontrakten (Kontraktbinding)
- Kunden opnår ikke brugsret eller ophavsret til integrationer eller anden kode udviklet særligt til Kunden behov og formål (proprietære barrierer)

Kunden bør forud for indgåelse af Kontrakten undersøge, om Kunden ved anvendelse af Cloudløsningen vil blive låst, enten økonomisk, teknisk eller juridisk på en sådan måde, at Kunden mister handlefrihed, hvis eksempelvis Cloudløsningen ikke udvikles efter Kundens ønsker, eller hvis Leverandøren forhøjer prisen væsentligt.

Kunden kan til en vis grad sikre sig mod lock-in effekter i Kontrakten. Dette kan blandt andet ske ved at indskrive krav om adgang til data ved ophør i formater, som passer til Kunden, og de alternative løsninger, som Kunden kan forvente anvendt i stedet for Cloudløsningen eller sikre brugsret eller ejendomsret til specialudviklet kode. Kunden kan endvidere sikre sig kommercielt ved at undersøge, om der er et modent marked for løsninger inden for det felt, Cloudløsningen skal virke, således at der er reelle alternativer i markedet.

16. Varighed af Kontrakter

16.1 Uopsigelighedsperiode fra Leverandøren og Kundens side

Det grundlæggende princip ved anvendelse af cloud computing er betaling ud fra forbrug. Dette ændrer dog ikke på, at mange Leverandører opererer med uopsigelighedsperioder (bindingsperioder) og længerevarende opsigelsesvarsler. Uopsigelighedsvilkår kan være betingelsen for at opnå gunstige priser. Typisk er der relativt korte opsigelsesvarsler i Kontrakter om cloud computing, men dette afhænger af den konkrete Kontrakt. Uanset om der ikke er nogen bindingsperiode og/eller korte opsigelsesvarsler, bør Kunden forholde sig til de lock-in effekter, der er beskrevet i afsnit 15 ovenfor, og som kan være til hinder for, at Kunden i praksis (af økonomiske eller tekniske grunde) vil kunne komme ud af Kontrakten.

Kunden kan på sin side have et behov for at opnå leveringssikkerhed i en længere periode, hvis Kunden har foretaget en investering i det indledende forløb ved at implementere Cloudløsningen, eller der vil være væsentlige omkostninger forbundet med at migrere til en anden løsning. Kunden bør derfor - hvis Kontrakten er genstand for forhandling - sikre sig en uopsigelighedsperiode på nogle år (typisk 2-4 år) samt en ensidig ret til at kunne forlænge varigheden af Kontrakten. Alternativt vil Kunden ikke have sikkerhed for at kunne genvinde de investeringer, som er foretaget ved implementeringen. En uopsigelighedsperiode fra Leverandørens side er således en sikring af, at forretningsgrundlaget for Cloudløsningen (business casen) hænger sammen for Kunden. Endvidere sikres Kunden mod kommercielt pres i en genforhandlingssituation, hvis Kunden har en ensidig ret til at forlænge Kontrakten.

I det omfang Kontrakten ikke kan forhandles (og Kunden dermed ikke kan sikre sig en uopsigelighedsperiode fra Leverandørens side), er Kunden nødsaget til at forlade sig på, at Leverandøren vil fastholde produktet i markedet, og at Kunden selv bærer risikoen for sin investering.

16.2 Ophævelsesmulighed ved misligholdelse

Uafhængigt af vilkårene for opsigelse er vilkårene for ophævelse ved væsentlig misligholdelse. Spørgsmålet om ophævelse er ikke væsentligt i Kontrakter om Cloudløsninger, hvis de er baseret på udbud af "on demand" tjenester, som Kunden blot kan ophøre med at bruge med kort eller intet varsel.

Er der derimod tale om kontrakter med længerevarende bindingsperioder, vil det have betydning, at Kunden kan bringe Kontrakten til ophør ved væsentlig misligholdelse. Kunden bør således uanset aftalte opsigelsesvarsler og uopsigelighedsperioder altid kunne komme ud af Kontrakten ved Leverandørens væsentlige misligholdelse uden varsel eller med et kortere varsel. Typisk er det beskrevet i Kontrakten, hvad der udgør væsentlig misligholdelse. Er vilkårene for ophævelse ikke rimelige, og er Kontrakten genstand for forhandling, bør Kunden søge at sikre, at der en ret til at ophæve Kontrakten ved udgang af en afhjælpningsperiode, hvis Leverandøren ikke inden udgangen af denne periode har afhjulpet mangler eller forsinkelse. Kunden bør også sikre sig, at Kunden kan ophæve med et vist varsel, som Kunden selv fastsætter, da det normalt er urealistisk, at Kunden kan skifte til en anden løsning straks efter ophævelsen i særdeleshed hvis den begivenhed, der giver anledning til ophævelsen, er en pludselig indtrådt begivenhed.

16.3 Ændringer i vilkår, herunder prisændringer

Ændringer i Kontrakten vil, medmindre andet er aftalt, kræve, at begge parter er enige heri. Det vil sige, at Leverandøren ikke kan ændre i priser, servicemål eller i selve Cloudløsningen, medmindre dette aftales med Kunden.

Da Leverandøren typisk har behov for et vist manøvrerum, vil Leverandøren ofte kræve en ret til at kunne foretage ændringer i ydelsen, men også ofte i selve Kontrakten, herunder i servicemål (SLA). Ændringer i servicemål er et godt eksempel, da det både rammer selve ydelsen, og de vilkår den leveres på.

Ret til at foretage prisændringer er noget, som bør være reguleret i Kontrakten. I denne sammenhæng bør det tillige indgå ved vurdering af lock-in effekterne, som er beskrevet i afsnit 15 ovenfor.

Hvis Kontrakten ikke kan gøres til genstand for forhandling, vil Kunden også på dette punkt være overladt til at foretage en risikovurdering i forhold til risikoen for at blive mødt med negative ændringer.

Kunden bør undersøge, i hvilket omfang der er en ret for Leverandøren til at foretage ændringer i ydelsen, priser og/eller aftalevilkårene, omfanget af denne ret og det varsel, der gælder for at gennemføre ændringer.

16.4 Konkurs og rekonstruktion

Ved indgåelse af Kontrakten bør Kunden også forholde sig til risikoen for, at Leverandøren går konkurs eller tages under rekonstruktion (modpartsrisiko). Disse scenarier kan fra Kundens side ses som en form for tvungen exit, og Kunden bør derfor forholde sig til dette som en del af exitovervejelserne.

Der kan i forbindelse med konkurs eller rekonstruktion opstå særlige problemstillinger vedrørende adgang til data, og Kunden bør derfor undersøge, hvilke muligheder Kunden har for at kunne hjemtage sine data, hvis Leverandøren af den ene eller anden grund ikke kan eller vil medvirke med ophørsassistance til Kunden under en konkurs eller en rekonstruktionssituation. En mulig løsning på denne problemstilling er at foretage backup, således at data sikres via en tredjepart, men dette indebærer yderligere omkostninger og arbejde for Kunden, og giver ikke nødvendigvis i alle situationer den nødvendige sikkerhed for adgang til opdaterede data.

I praksis vil det ofte være sådan, at konkursboet eller rekonstruktionen meget hurtigt får solgt Kontrakterne til en ny Leverandør, som således kan videreføre Cloudløsningen. Dette kræver dog, at der er en køber, som vil indtræde, og der er således ikke nogen kommerciel sikkerhed for, at dette vil være tilfældet.

16.5 Særligt om persondata ved ophør

For så vidt angår spørgsmålet om databehandlerens adgang til at behandle persondata i en Cloudløsning efter aftaleophør, er det vigtigt at være opmærksom på persondatalovens regler. Det følger således af persondatalovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Denne bestemmelse indebærer således, at såfremt en dataansvarlig meddeler en databehandler instruks om, at persondata, der behandles på vegne af den dataansvarlige, f.eks. skal slettes, har databehandleren en lovfæstet pligt til at efterkomme denne instruks. Denne pligt kan ikke underlægges bestemmelser i parternes indbyrdes aftale, hvorfor databehandleren skal efterkomme en sådan instruks, uanset hvad der måtte følge af aftalegrundlaget mellem den dataansvarlige og databehandleren.

Det bemærkes, at overtrædelse af bestemmelsen i persondatalovens § 41, stk. 1, er strafbelagt.

Aftalen bør derfor indeholde en eksplicit bestemmelse om, at Leverandøren uden undtagelse skal efterkomme alle instruktioner fra Kunden vedrørende data, herunder en instruks om at slette eller udlevere data.

17. Rettigheder til software/applikationer

17.1 Ejendomsret til data

I langt de fleste Kontrakter vedrørende Cloudløsninger fremgår det, at Kunden har den fulde ejendomsret til sine egne data. Hvis ikke dette fremgår direkte af Kontrakten, bør Kunden søge at få dette angivet. Dette kan være vigtigt i forhold til at sikre, at Leverandøren ikke anvender Kundens data til andre formål end at levere ydelserne under Cloudløsningen. Hvis data omfatter persondata, skal man være opmærksom på, at det er et grundlæggende krav under persondataloven, at Leverandøren alene må anvende data til at levere ydelserne.

17.2 Ejendomsret til software/Cloudløsningen

Det særlige ved cloud computing er, at der ikke som ved traditionelle it-produkter opnås en evigtvarende brugsret til software, men derimod en tidsbegrænset adgang til at benytte en tjeneste, som baserer sig på software. Det vil sige, at når Kontrakten ophører, har Kunden ikke yderligere ret til at bruge den underliggende software, som anvendes til at levere ydelserne. Som led i implementering af Cloudløsningen kan der være udviklet særlig funktionalitet til Kunden, herunder til brug for grænseflader til andre systemer (API'er). Kunden bør i Kontrakten sikre sig, at Kunden får adgang til sådan specialudviklet software.

18. Leverandør- og kontraktstyring

Brugen af cloud computing ændrer ikke ved de grundlæggende krav til leverandørstyring. Der skal fra begge parter gøres en indsats for at holde relationen vedlige relationen, og denne skal løbende evalueres. Virksomheden bør sikre sig, at leverandørstyringen også omfatter leverandører af Cloudløsninger, herunder ikke mindst SaaS løsninger.

Anskaffelse af en Cloudløsning indebærer outsourcing af en række opgaver til Leverandøren - opgaver, som tidligere har været varetaget af Kunden selv ved traditionel IT-anvendelse. Det gælder eksempelvis i forhold til beslutning om og gennemførelse af opdatering og opgradering af software og applikationer. Samtidig stiller anvendelsen af Cloudløsninger, og det deraf følgende tab af kontrol for Kunden, krav om strategisk årvågenhed fra Kundens side.

Som led i anvendelsen af Cloudløsninger, bør Kunden således overveje, hvorledes Kunden bedst strukturerer sin styring af samarbejdet og Kontrakterne med Leverandørerne af Cloudløsninger. I den forbindelse bør Kunden som minimum tage stilling til hvem hos Kunden, der skal have ansvaret for følgende opgaver:

1. **Strategiske spørgsmål**
   - Er Cloudløsningen egnet til at imødekomme Kundens forretningsmæssige behov på kort, mellemlangt og lang sigt?
   - Leverandøren som samarbejdspartner (overvågning af modpartsrisiko)?
   - Hvilke alternativer er der i markedet til de anvendte Cloudløsninger?
   - Hvilke barrierer og Lock-in effekter vil der være ved at skifte til et skifte til en alternativ løsning?

2. **Kundens IT-landskab**
   - Hvordan passer den enkelte Cloudløsning ind i forhold til Kundens øvrige IT-anvendelse, herunder i forhold til andre eventuelle outsourcing-leverandører?
   - Understøtter Cloudløsningen integration med øvrige løsninger på kort, mellemlang og lang sigt?

3. **Sikkerhed og compliance**
   - Opfylder Cloudløsningen Leverandørens egne sikkerhedskrav og Kundens krav til sikkerhed, persondatalovgivningens krav samt krav i medfør af

sektorspecifik lovgivning?
- Hvordan håndteres og rapporteres brud på sikkerhedend?

4. Support og performance
- Hvem autoriserer og uddanner brugere til Cloudløsningen (brugerstyring)?
- Er "superbrugerne" personer fra forretningen eller IT-funktionen og håndterer disse "superbrugere" tillige supportrelationen til Leverandøren?
- Hvem undersøger og rapporterer fra Kundens side fejl og mangler ved Tjenesterne og følger op på afhjælpning?
- Hvem kontrollerer, om Cloudløsningen har en tilfredsstillende performance og overholder aftalte servicemål (tilgængelighed og svartid)?

5. Forbrugsstyring og økonomi
- Hvem sikrer, at Kundens køb af "abonnementer" (brugere) og/eller volumen er tilpasset Kundens behov på kort, mellemlang og lang sigt?
- Hvem sikrer, at der sker korrekt afregning fra Leverandørens side?

En række af de nævnte opgaver og spørgsmål ligger ikke naturligt i Kundens allerede etablerede funktioner og håndteringen af opgaverne vil muligvis skulle ske i et samarbejde mellem flere af virksomhedens funktioner (eksempelvis mellem IT-funktionen, indkøb og de relevante dele af forretningen). IT-funktionens rolle i forhold traditionel IT-anvendelse har typiske været teknisk orienteret. Ved Cloudløsninger er der derimod behov for et ændret fokus; væk fra det tekniske til et fokus på, om Kunden får det som er aftalt og forventes (egentlig kontraktstyring) og strategi (er Cloudløsningen og samarbejdspartneren den rigtige og hvad er alternativerne). Disse kompetencer er ikke nødvendigvis til stede i forvejen, og Kunden bør derfor sikre, at de eksisterende personer i IT-funktionen tilegner sig disse kompetencer eller erstattes af personer, der har dem.

Kunder der anvender Cloudløsninger i større omfang bør tilrettelægge og koordinere opgavevaretagelsen i lyset af at Cloudløsninger kræver mindre fokus på tekniske forhold og større fokus på kontraktstyring og strategi.

Bilag 1: Checkliste sikkerhed

1. Kend dine behov

Forudsætningen for meningsfyldt at kunne vurdere, om leverandørens sikkerheds-setup er tilstrækkeligt, er, at virksomhedens krav til sikkerhed er klart defineret, da det er disse krav, sikkerheden skal måles op imod.
Da kravene til sikkerhed kan variere afhængigt af, hvilke systemer og data, der er tale om, bør virksomhedens sikkerhedskrav være konkrete i forhold til de systemer og data, der afvikles/opbevares i cloud-løsningen. På den ene side er det vigtigt at sikre, at der er en tilstrækkelig beskyttelse, men på den anden side er der ingen grund til at betale for en sikkerhed, der væsentligt overstiger behovet. Ideelt set bør virksomheden have klassificeret sine systemer og data og styre sikkerheden ud fra denne klassificering. Da sikkerhedskravene følger klassificeringen vil det - for virksomheder, der har foretaget en sådan klassificering - være relativt let at fastlægge sikkerhedskravene over for leverandøren.

2. Fokus på "hvad" frem for "hvordan"

Det afgørende for virksomheden er, at der er den nødvendige sikkerhed; men leverandøren bør i videst muligt omfang gives friheden til at beslutte, hvordan denne sikkerhed tilvejebringes.
Et af kendetegnene ved cloud computing er, at det bygger på en høj grad af standardisering. Derfor vil det formentlig være både dyrt og besværligt at formå leverandøren til at justere dennes interne processer, og så længe man som kunde samlet set opnår det nødvendige sikkerhedsniveau, vil det formentlig være både nemmere og billigere at lade leverandøren styre, hvordan denne sikkerhed opnås.

3. Få styr på grænsefladerne

Leverandøren vil som udgangspunkt have særdeles begrænset - og ofte slet ingen - viden om kundens forretning, og følgelig kan sikkerheden ikke være målrettet kundens forretning.
Det er derfor vigtigt at være bevidst om, hvad det helt præcist er, leverancen omfatter, og hvilke forudsætninger den bygger på. Sådanne forudsætninger kunne eksempelvis være, at kunden skal give leverandøren særskilte oplysninger om, hvilke typer af data, der opbevares, eller at kunden selv er ansvarlig for at konfigurere og vedligeholde visse parametre i systemet.

Ligeledes er det - ud fra naturen af Tjenesterne - naturligt at antage, at Leverandøren stiller information til rådighed, så Kunden kan opnå den ønskede sikkerhed; men at det kræver en aktiv indsats fra kundens side. Eksempelvis kan Leverandøren godt stille log-filer til rådighed, og Leverandøren kan også meningsfyldt gennemgå disse for visse tekniske hændelser; men det er kun Kunden, der meningsfyldt kan gennemgå sådanne logs i forhold til brugernes anvendelse af systemet.
Endelig bør det afklares, hvordan kritiske processer hos Leverandøren "passer" med Virksomhedens egne processer, eksempelvis for incident management og beredskab. Netop for sådanne processer vil Leverandørens processer - og outputtet herfra - være forudsætningen for ens egne processer. En forståelse af grænsefladen er derfor nødvendig for at sikre, at forudsætningerne for ens egne processers effektivitet er opfyldt. Dette kan i praksis give anledning til justering af egne processer, jf. afsnittet umiddelbart herunder.

4. Overvej justering af interne processer

Som omtalt ovenfor bygger Cloudløsninger på en høj grad af standardisering, og det vil derfor som udgangspunkt være vanskeligt at få leverandøren til at ændre processer.
Hvis Kunden konstaterer, at Leverandørens sikkerhed ikke lever fuldt op til ens egne krav, bør det overvejes, om man kan justere egne processer for at kompensere for manglen. Dette vil oftest være nemmere og billigere end at forsøge at formå Leverandøren til at ændre sit setup, og bedre end at fravælge en Cloudløsning som ellers ville være en fordel for forretningen.

5. Foretag vurdering af leverandørens sikkerhed inden løsningen tages i brug

Cloudløsninger bygger som nævnt på en høj grad af standardisering - og når først løsningen er etableret, er det endnu vanskeligere at få noget ændret. Som kunde bør man derfor foretage en vurdering af sikkerheden allerede inden løsningen tages i brug - det vil i øvrigt også være nødvendigt for at leve op til bl.a. persondatalovens bestemmelser om brug af databehandlere.

6. Databehandleraftaler

Hvis løsningen anvendes til behandling af persondata, vil leverandøren i persondatalovens forstand være databehandler. Som databehandler må Leverandøren alene handle efter instruks fra den dataansvarlige (det antages dog implicit at være en del af instruksen, at Leverandøren skal sørge for, at Cloudløsningen fungerer, og Leverandøren vil derfor være berettiget til at foretage de handlinger, der er nødvendige herfor).
I mange tilfælde vil det ikke være muligt at få Leverandøren til at acceptere en specifik databehandleraftale - i sådanne tilfælde må man som kunde sikre sig, at Kontrakten indeholder de bestemmelser, der som minimum skal indgå i en databehandleraftale. Se punkt 12.

7. Hvor er mine data

Persondata må ikke - med mindre der foreligger særligt grundlag - eksporteres til lande uden for EØS med mindre disse lande sikrer et tilstrækkeligt sikkerhedsniveau, eller der i øvrigt er truffet foranstaltninger til at sikre, at den konkrete behandling er underlagt passende sikkerhedsforanstaltninger.
Da det forhold, at data er tilgængelige fra et tredjeland, medfører, at data i persondatalovens forstand anses for at være eksporteret til pågældende tredjeland, skal man som kunde ikke blot være opmærksom på, hvor Leverandørens servere fysisk er placeret, men også hvor driftspersonalet befinder sig.

8. I hvilket omfang har leverandøren adgang til mine data

Det kan - på grund af legale eller forretningsmæssige krav til fortrolighed - være nødvendigt at sikre sig, at leverandøren ikke kan tilgå (læse) ens data.
Da Leverandørens medarbejdere som udgangspunkt vil have privilegeret adgang til systemer og data, vil en begrænsning af Leverandørens adgang ofte skulle ske ved at kryptere data.

Dette kan i sig selv give anledning til sikkerhedsmæssige overvejelser (risikoen for at data går tabt, hvis der opstår fejl i forbindelse med selve krypteringen), men hvis man vælger at kryptere data, skal man sikre sig, at Leverandøren ikke har adgang til krypteringsnøglen, da krypteringen i så fald ikke vil yde nogen beskyttelse i forhold til Leverandørens medarbejdere.

9. Kontrol af leverandørens sikkerhed

De fleste leverandører søger at undgå, at enkeltkunder foretager egne inspektioner af leverandørens sikkerhed, og da dette ofte vil være relativt ressourcekrævende for begge parter, vil det som regel være en fordel at basere sig på certifikater og erklæringer, hvor uafhængige tredjeparter udtaler sig om leverandørens sikkerhed. Det kunne f.eks. være ISO certificeringer eller revisorattesterede rapporter (ISAE 3000, ISAE 3402 eller tilsvarende - alt afhængigt af formålet og erklæringsområdet).

Da det som udgangspunkt er Leverandøren, der vælger, hvilke dele af den samlede løsning, der skal være omfattet af et certifikat eller en rapport, er det vigtigt, at Kunden undersøger, hvad den pågældende erklæring helt præcist dækker, og om dette er tilstrækkeligt i forhold til egne behov.

Derudover bør man forholde sig til, om typen af erklæring giver en tilstrækkelig sikkerhed i forhold til ens behov som kunde - eksempelvis om certifikatet/erklæringen alene forholder sig til, om der er etableret sikkerhedsforanstaltninger, eller om der også gives sikkerhed for, at de pågældende sikkerhedsforanstaltninger i en given periode har fungeret konsekvent og som tilsigtet.

10. Løbende governance

En årlig erklæring fra Leverandøren er både godt og nødvendigt - men ikke nødvendigvis tilstrækkeligt. Visse svigt i det interne kontrolsystem kan have uforholdsmæssigt store konsekvenser for kunden, og det vil derfor være problematisk, hvis Kunden ikke bliver opmærksom på dette før det fremgår af en erklæring, der måske først modtages et år efter hændelsen.

Kunden bør derfor identificere de interne kontroller, der anses for særligt væsentlige, og kræve af leverandøren, at blive orienteret uden ugrundet ophold, såfremt leverandøren konstaterer et svigt i en af disse kontroller. Derudover bør Kunden have en intern proces for håndtering af sådanne hændelser, således at man i videst muligt omfang kan afbøde eller begrænse de negative effekter.

Cloud Computing kontrakter

Vejledning om juridiske, kommercielle og tekniske forhold i aftaler om Cloud Computing

Cloud computing er for alvor kommet på dagsordenen hos de fleste virksomheder og it-leverandører i Danmark og i udlandet. Mange har dog stadig betænkeligheder ved cloud computing og har vanskeligt ved at overskue konsekvenserne ved at anvende løsninger baseret på cloud computing i deres virksomhed.

Cloud computing er ikke ny teknologi, men en anden måde at anvende eksisterende teknologi på, hvor brugere på væsentlige punkter overlader kontrollen til leverandøren af it-ydelsen og kommer ind i en standardiseret og færdigpakketeret verden af "services". Kundens formål med at overlade denne kontrol til Leverandøren er at opnå de fordele i form af fleksibilitet, skalerbarhed, stabilitet og omkostningsbesparelser, som cloud computing i mange tilfælde vil give.

Formålet med vejledningen er at give Kunden en forholdsvis let og overskuelig vejledning i forhold til de spørgsmål, der bør stilles, og overvejelser, der bør gøres, før Kunden går ind i en løsning baseret på cloud computing.