DIGITALISERINGSSTYRELSEN

CENTER FOR CYBERSIKKERHED

Vejledning i anvendelse af cloudservices

Version 1.1, juli 2020

2020

Version nr.	Dato	Udarbejdet/revideret af	Ændringer/bemærkninger
1	November 2019	Digitaliseringsstyrelsen og Center for Cybersikker-hed	
1.1	Juli 2020	Digitaliseringsstyrelsen og Center for Cybersikker-hed	Foretaget konsekvensrettelser efter dom om EU-U.S. Privacy Shield som overførsels-grundlag

Indhold

1. Indledning **5**

2. Introduktion til cloudservices **8**

3. Forretningsmæssige overvejelser **14**
3.1 Organisering og kompetencebehov 14
3.2 Agilitet og innovation 15
3.3 Skalering 16
3.4 Leverandørafhængighed 18
3.5 Økonomistyring 20

4. Juridiske overvejelser **24**
4.1 Særlige krav ved behandling af personoplysninger 24
4.2 Databehandleraftaler 25
4.3 Tredjelandsoverførsler 27
4.4 Konsekvensanalyse 29
4.5 Lokationskravet i databeskyttelsesloven 30
4.6 Databeskyttelse gennem design og standardindstillinger 30
4.7 Øvrig lovgivning 32

5. Sikkerhedsmæssige overvejelser **35**
5.1 Risikovurdering af cloudløsningen 36
5.2 Behandlingssikkerhed 37
5.3 Sikkerhed under behovsafklaringen 37
5.4 Sikkerhed i forbindelse med anskaffelsen 38
5.5 Sikkerhed under drift 39
5.6 Ophør eller skift i leverandørforhold 40
5.7 Håndtering af tvungne opdateringer 40
5.8 Uddannelse 41
5.9 Test og udvikling 42

6. Opsummering **44**

Indledning

1. Indledning

Anvendelsen af cloudservices kan i mange situationer være attraktiv for danske myndigheder til udvikling og drift af it-løsninger. Cloudservices tilbyder et hav af nye muligheder, og offentlige organisationer kan som udgangspunkt trygt anvende cloudløsninger til mange formål.

Som det er tilfældet for almindelig outsourcing, kan cloudservices tilbyde relevante løsninger for organisationer, som ønsker at mindske behovet for at have egen driftsorganisation ved i stedet at købe standardprodukter, som ikke kræver egne installationer. Indkøbet af cloudservices sker dog på andre vilkår, end der typisk ses ved almindelig outsourcing, da de kontraktmæssige forhold typisk ikke er til forhandling, men kunden til gengæld ikke bindes i længere tid. Cloudservices kan hér tilbyde en forenklet adgang til standardiserede digitale løsninger på mange platforme og enheder.

Cloudservices er også relevante for de myndigheder, som i højere grad ønsker at hjemtage ansvaret for dele af deres udvikling og som ønsker et udviklingsmiljø med den seneste teknologi, samt gode muligheder for fleksibilitet og skalerbarhed. For disse myndigheder kan cloudservices være med til at effektivisere udviklingsarbejdet og muliggøre hurtigere og mere agil udvikling, herunder ved eksempelvis at arbejde efter principperne i DevOps.

For at sikre det størst mulige udbytte af anvendelsen af cloudservices, og samtidig undgå de faldgruber, anvendelsen af cloudservices kan have, er det centralt, at myndigheder i valg af cloudservices og implementering heraf kommer rundt om en række centrale overvejelser.

Mange af de overvejelser man skal gøre sig, er ikke væsentligt anderledes end ved indkøb af en mere traditionel softwarepakke eller outsourcet ydelse. De har derfor en række sammenfald med generel leverandørstyring. Der er imidlertid nogle ansvarsmæssige, forretningsmæssige, juridiske og sikkerhedsmæssige forhold, som gør sig særligt gældende for cloudservices. Det skyldes de særlige service- og leverancemodeller, der kendetegner cloudservices, og som betyder, at man på nogle områder har mindre kontrol eller en anden type kontrol over sine data og systemer, end ved traditionel indkøb eller outsourcing. Dette betyder, at i forhold til en traditionel on-premise løsning fordeles det tekniske og operationelle ansvar og de deraf følgende risici på en anden måde imellem kunde og leverandør, uden at dette dog betyder, at kunden fraskrives alt ansvar herfor.

Formålet med denne vejledning er at understøtte ledelsesmæssige valg af strategi for organisationens fremtidige it-landskab, hvor cloudservices kan spille en rolle. Vejledningen beskriver de principielle problemstillinger, cloudservices introducerer og giver konkrete anvisninger til at vurdere anvendelsen af cloudservices.

Vejledningen er skrevet til offentlige organisationer, men kan også anvendes i private virksomheder.

Vejledningen er delt op i fire hovedsektioner:

- **Introduktion til cloudservices.** Cloudservices er et samlebegreb, der dækker over mange forskelligartede services. For sikkert at kunne navigere i anvendelsen af cloudservices, er det vigtigt at have kendskab til de grundlæggende modeller og deres respektive fordele og ulemper. I dette kapitel præsenteres de grundlæggende begreber.
- **Forretningsmæssige overvejelser.** Anvendelsen af cloudservices skal være baseret på forretningsbehov. Her ses på, hvilke forretningsbehov cloudservices kan være svaret på, og hvad det indebærer for organisationen.
- **Juridiske overvejelser.** Juridiske overvejelser om datasikkerheden, især ved behandling af personoplysninger, har afholdt mange fra at anvende cloudservices. I dette kapitel gennemgås de vigtigste opmærksomhedspunkter.
- **Informationssikkerhedsmæssige overvejelser.** Sidst beskriver vejledningen de særlige krav, cloudservices stiller til informationssikkerheden. Anvendelsen af cloudservices kan have indflydelse på, hvordan organisationen bedst opnår det ønskede informationssikkerhedsniveau, og hvordan det kontrolleres. Her gennemgås de særlige sikkerhedsaspekter, som cloudservices bringer med sig.

Afslutningsvis samles op på centrale pointer.

Vejledningen er skrevet, så det er muligt at læse om de specifikke emner hver for sig, men det anbefales at læse hele vejledningen for at sikre korrekt forståelse af de centrale begreber og problematikker.

Introduktion til cloud-services

2. Introduktion til cloudservices

"Cloudservices" er en fællesbetegnelse for meget forskellige services, der varierer i indhold, fleksibilitet for anvenderen og ansvarsfordeling imellem anvender og leverandør. Før man træffer beslutning om at anvende cloudservices, er det derfor vigtigt at forstå, hvad de forskellige variationer af cloudservices indebærer.

Helt overordnet er "cloud" en model til at tilvejebringe standardiserede ressourcer, der leveres som en service. Denne model består af fem centrale egenskaber, tre servicemodeller og fire leverancemodeller.[1]

Centrale egenskaber ved cloudservice-modeller:

De centrale egenskaber er fælles for alle cloudservice- og leverancemodeller.

- *On-demand selvbetjening.* En anvender kan efter behov selv tilvejebringe cloudressourcer, såsom servertid og lagring, uden at dette kræver menneskelig interaktion med hver enkelt leverandør.
- *Hurtig netværksadgang.* Ressourcer er tilgængelige via internettet og kan tilgås ved hjælp af standardmekanismer af forskellige typer enheder (fx mobiltelefoner, tablets, computere og servere).
- *Ressourcedeling.* Leverandørens ressourcekapacitet samles for at tjene flere anvendere samtidigt i en såkaldt multi-tenant model. Her udnytter cloudleverandøren variationen i hver enkelt anvenders behov til omkostningseffektivt og dynamisk at kunne servicere mange anvendere på én gang, uden at disse dog har adgang til hinandens applikationer eller data. Anvenderne har en følelse af lokalitetsuafhængighed, idet de generelt ikke har nogen kontrol over eller viden om den nøjagtige placering af de tilvejebragte ressourcer, men de kan typisk specificere placeringen af en ressource på et højere niveau (fx kontinent, land eller datacenter). Eksempler på ressourcer kan være grundlæggende lagring, processorkraft, hukommelse og netværksbåndbredde.
- *Hurtig elasticitet.* Ressourcekapacitet kan elastisk tilvejebringes og afgives, i nogle tilfælde automatisk, til hurtigt at skalere op eller ned i takt med anvenderens behov. For anvenderen synes de tilgængelige kapaciteter ofte at være ubegrænsede og kan tilvejebringes til enhver tid og i enhver mængde.
- *Målt service.* Forbruget af hver enkelt ressource overvåges og rapporteres, hvilket giver gennemsigtighed for både leverandøren og anvenderen af den anvendte ressource. Parametrene for målingerne er tilpasset typen af ressource (fx lagring, processorkraft, båndbredde og aktive brugerkonti).

[1] Beskrivelsen er baseret på definitionen af cloud computing fra det amerikanske institut for standardisering, National Institute of Standards and Technology (NIST). Mell, Peter og Timothy Grance, 2011: *The NIST Definition of Cloudservices Computing,* NIST Special Publication 800-145.

Servicemodeller:

Servicemodellerne beskriver indholdet af den ressource, man anvender.

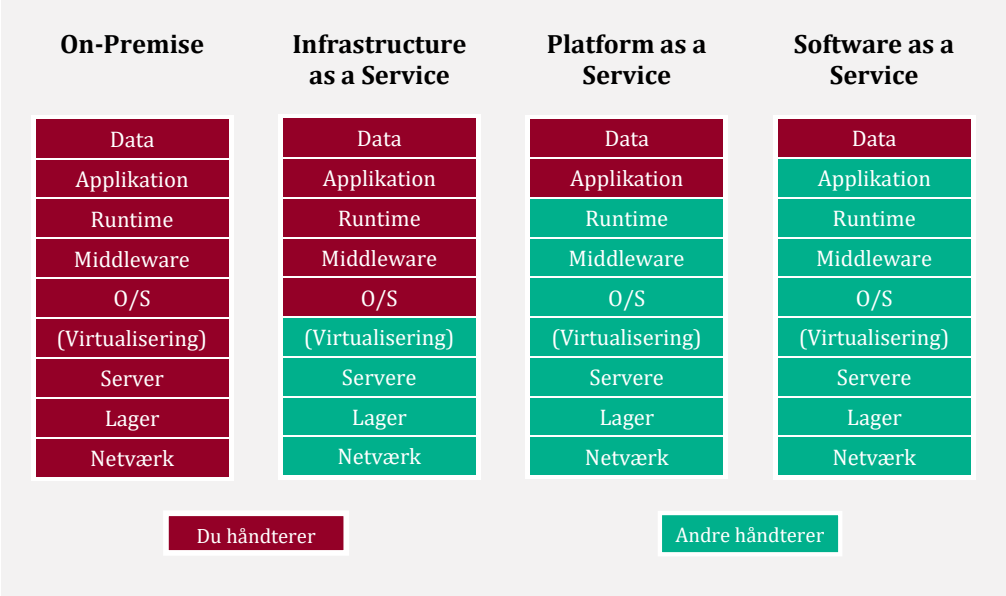
- *Infrastruktur som en service (IaaS).* IaaS er den mest basale af de tre servicemodeller. Med IaaS har anvenderen adgang til rå infrastruktur, det vil sige grundlæggende ressourcer som processorkraft, lagring og netværk. For at udnytte infrastrukturen skal anvenderen selv installere og drive al software, såvel operativsystemer som applikationer. Anvenderen har dermed selv kontrol med og ansvar for etablering, sikring og drift af driftsmiljøet, herunder operativsystemer, netværk og lagring af data, forud for de implementerede forretningsapplikationer. Med frit valg af blandt andet operativsystemer og driftsmiljøer giver IaaS anvenderen den største fleksibilitet, men også det største drifts- og vedligeholdelsesansvar.

- *Platform som en service (PaaS).* PaaS balancerer fleksibilitet og ansvar. Med PaaS har anvenderen adgang til en infrastruktur, som leverandøren servicerer med blandt andet databaser, operativsystemer og centrale API'er. Herpå kan anvenderen implementere egenudviklede eller erhvervede applikationer. Anvenderen har kontrol med og ansvar for de implementerede applikationer og muligvis tilhørende konfigurationsindstillinger for applikationens driftsmiljø. Kontrol med og ansvar for den underliggende cloudinfrastruktur og operativsystemer overlades til leverandøren.
  PaaS vil typisk dække hovedparten af de mest gængse behov og endvidere kunne inkludere meget avancerede funktioner, eksempelvis algoritmer til big data analyse, kunstig intelligens og chatbots. Anvenderen kan dermed fokusere på sine forretningsapplikationer og anvende de services, der indgår i platformen. Fordi leverandøren udpeger og har ansvar for vedligehold af operativsystemer og services på infrastrukturen, giver PaaS anvenderen mindre fleksibilitet end IaaS, men indebærer tilsvarende, at anvenderens udviklings- og driftsansvar begrænses til forretningsapplikationerne.

- *Software som en service (SaaS).* SaaS er den mest komplette servicemodel. Med SaaS har anvenderen adgang til at bruge leverandørens færdigudviklede, cloudbaserede forretningsapplikationer. SaaS kan tilvejebringes ved indkøb af allerede udviklede løsninger, eller ved samlet udbud af udvikling og drift af en løsning, forudsat driftsvilkårene har de fem centrale egenskaber for cloudservices, eksempelvis selvbetjening og forbrugsafregning. Leverandøren har det fulde ansvar for drift og vedligehold af den samlede løsning, hvilket giver anvenderen mulighed for udelukkende at fokusere på anvendelsen af produktet. Idet anvenderen typisk har få muligheder for selv at tilpasse produktet, skal forretningsbehovene være dækket af produktet, som det foreligger. Dette er særligt vigtigt at være opmærksom på, hvis SaaS-løsningen skal integreres i et miljø af eksiste-

rende systemer, da tilpasninger af en SaaS-løsning kan være ressourcekrævende. SaaS er den af de tre servicemodeller, der giver anvenderen mindst fleksibilitet, men tilsvarende mindst ansvar for drift og vedligehold af løsningen.

Elementer af servicemodellerne er velkendte fra andre typer af it-services og indgår typisk allerede i overvejelserne ved indkøb eller udvikling af især større systemer. Figur 1 viser forskellene i ansvarsfordelingen ved de tre servicemodeller i forhold til at have en løsning baseret på eget hardware og software (en on-premise løsning).



Figur 1. Ansvarsfordeling ved forskellige servicemodeller sammenlignet med en on premise-løsning.

Leverancemodeller:

Leverancemodellerne beskriver, hvordan den valgte service teknisk leveres, herunder om den tilbydes til én eller flere anvendere.[2]

- *Privat cloudservice.* Cloudservicen er til eksklusiv brug af en enkelt organisation. Den kan ejes, forvaltes og drives af organisationen selv, en tredjepart eller en kombination af dem, og den kan være etableret i eller uden for organisationens egne faciliteter. Da man skal betale for alle ressourcerne, der er knyttet til den konkrete cloudimplementering, vil prisen for

[2] Begrebet "leverancemodeller" henviser her til begrebet "deployment models" i definitionen fra NIST. Se Mell, Peter og Timothy Grance, 2011: *The NIST Definition of Cloudservices Computing,* NIST Special Publication 800-145.

en privat cloudservice typisk være højere og den kapacitetsmæssige fleksibilitet lavere i forhold til en offentligt tilgængelig cloudservice. Til gengæld er der mulighed for at skræddersy løsningen til ens behov.

- *Fælles cloudservice.* Cloudservicen er til eksklusiv brug af en veldefineret gruppe af organisationer. Den kan ejes, forvaltes og drives af en eller flere af organisationerne i fællesskabet, en tredjepart eller en kombination af dem, og den kan være etableret i eller uden for organisationernes egne faciliteter. En fælles cloudservice tilgodeser typisk de deltagende organisationers fælles behov under hensyntagen til den samlede økonomi. For hver enkelt organisation giver dette en økonomisk fordel og en større kapacitetsmæssig fleksibilitet sammenlignet med den private cloudservice. Samtidig vil governancestrukturerne for en fælles cloudservice give hver organisation større indflydelse på udviklingen, end det er tilfældet ved en offentligt tilgængelig cloudservice.

- *Offentligt tilgængelig cloudservice.* Cloudservicen udbydes typisk på kommercielle vilkår. Den kan ejes, forvaltes og drives af en erhvervs-, akademisk eller statslig organisation eller en kombination af dem. Den er etableret i cloudleverandørens faciliteter og cloudleverandøren fastsætter egenhændigt politikkerne for servicen. De offentligt tilgængelige cloudservices tilbyder typisk den største kapacitetsmæssige fleksibilitet, den bredeste vifte af services og den hurtigste udvikling af nye services. Endvidere er de offentligt tilgængelige cloudservices typisk billigere for hver enkelt organisation end den private cloudservice eller den fælles cloudtjeneste, om end sidstnævnte kan være økonomisk attraktiv, hvis de deltagende organisationer har en tilstrækkelig masse. Hvis ens forretningsbehov er meget tidsfølsomme skal man dog være opmærksom på, om den geografiske afstand til cloudleverandørens datacentre indebærer en for lang responstid.

- *Hybrid cloudservice.* Cloudservicen er en sammensætning af to eller flere forskellige cloudservices (privat, fælles eller offentlig). Hver cloudservice forbliver en unik enhed, men de er forbundet på en måde, der muliggør, at data og applikationer kan flyttes rundt imellem hver enhed (fx til balancering af belastning). En hybrid-cloudservice er altså ikke det samme som at have flere individuelle, ukoordinerede cloudservices og bruges i denne vejledning heller ikke om kombinationen af traditionel on-premise infrastruktur med en cloudservice. Afhængig af ens forretningsbehov kan en hybrid cloudservice give anvenderen den største kapacitetsmæssige fleksibilitet, det største serviceudbud og den laveste pris, men for at indfri gevinsterne kræves en høj grad af teknisk og organisatorisk modenhed.

De forskellige service- og leverancemodeller adskiller sig altså væsentligt på indhold, ansvarsfordeling, teknisk kompleksitet for anvenderen og sikkerhedsprofiler samt krav til økonomistyring. Uanset disse forskelle i service- og leverancemodellerne, kendetegnes modellen "cloud" dog ved, at ressourcen ikke leveres som et produkt med en levetid, men som en service med kvalitetskriterier, som leverandøren har ansvaret for at indfri.

For at opnå en succesrig anvendelse af cloudservices er det helt afgørende, at man nøje overvejer, hvilke forretningsbehov anvendelsen skal dække. Først når disse behov er beskrevet grundigt, er det muligt at udvælge de rigtige service- og leverancemodeller.

Markedet for cloudservices, navnlig IaaS og PaaS-services, har i en årrække været domineret af få, globale spillere, der var først med succesrige, kommercielle tilbud. Den teknologiske udvikling og den generelt hastigt stigende interesse for cloudservices, har dog betydet, at det er blevet nemmere og mere attraktivt at tilbyde cloudservices. Der er derfor stadigt flere leverandører af cloudservices. Leverandører af traditionelle serverbaserede datacentre er eksempelvis begyndt at tilbyde cloudservices, ligesom mulighederne for at få leveret private cloudservices er vokset.

Det er derfor ikke nødvendigvis et spørgsmål om at vælge cloudservices til eller fra, men derimod med udgangspunkt i ens forretningsbehov at efterspørge de egenskaber ved cloud, man har behov for.

Forretningsmæssige overvejelser

3. Forretningsmæssige overvejelser

Når man overvejer at anvende cloudservices, er det, ligesom med anskaffelse af traditionel serverbaseret it, vigtigt at fokusere på, hvilke konkrete forretningsmæssige behov anvendelsen skal dække.

I dette kapitel gennemgås hvordan cloudløsninger kan besvare konkrete forretningsbehov, eksempelvis behov for at kunne skalere løsningen i forbindelse med spidsbelastninger, behov for at koble sig på stærke standardløsninger og behov for at understøtte agil udvikling og drift. Der er også fokus på, at valg af cloudservices ofte betyder, at det er hensigtsmæssigt at udvide de forretningsmæssige overvejelser til også at inkludere overvejelser om organisering af udvikling og drift, om hvilke kompetencer organisationen ønsker at have internt, om hvordan ansvarsfordelingen skal være mellem organisationen og leverandører og om hvordan man skal håndtere behov for udskiftning af leverandører.

3.1 Organisering og kompetencebehov

Udvikling, drift og vedligehold ved hjælp af cloudservices er på en række områder anderledes end i en klassisk serverbaseret løsning. Cloudservices kan eksempelvis anvendes til at minimere behovet for interne tekniske kompetencer til eksempelvis drift af servere. Ligeledes kan cloudservices være en vej til at hjemtage ansvaret for dele af udviklings- og vedligeholdsopgaver, eksempelvis af forretningsapplikationer.

Implementering af cloudservices ændrer derfor på kravene til den interne organisering og ansvarsfordelingen mellem leverandør og kunde. Dette muliggør en større leverandøruafhængighed, men forudsætter, at organisationen opbygger de rigtige kompetencer og samarbejdsrelationer imellem it-specialister og generalister. Jurister og økonomer bør eksempelvis etablere den juridiske og økonomiske ramme for systemet i nært samspil med løsningsarkitekternes udarbejdelse af en løsningsarkitektur, som understøtter de forretningsmæssige valg. Tilsvarende bør der efterfølgende være et tæt samarbejde om den løbende udvikling af løsningen og styring af forbrug. Strategiske overvejelser om anvendelse af cloudservices bør derfor inkludere overvejelser om dels, hvilket ansvar organisationen ønsker at have for løsningens udvikling og drift, dels hvilke kompetencer organisationen ønsker at have internt.

Som tidligere beskrevet køber man med servicemodellen SaaS adgang til software, der tilgås via internettet. Dette kan være ved udbud af udvikling og drift af en løsning, hvor man som udbyder af opgaven har ansvar for at specificere løsningen, så den dækker ens forretningsbehov. Det kan også være ved indkøb af allerede udviklede, standardiserede løsninger, hvor man har ansvar for at sikre, at den tilbudte løsning dækker forretningsbehovene. Indkøb af SaaS-ydelser minder

således meget om indkøb af almindelige serverbaserede ydelser. Afhængig af udgangspunktet vil det dog særligt fordre overvejelser om ændringer af organiseringen af den tekniske drift og vedligehold, samt krav til eksempelvis leverandør- og økonomistyring, se kapitel 3.5 Økonomistyring.

I modsætning til SaaS og traditionel outsourcing af en samlet løsning, indebærer anvendelsen af IaaS og PaaS typisk behov for styring af flere leverandører: Henholdsvis leverandøren af cloudservicen og leverandøren af forretningsapplikationen. Dette kræver et selvstændigt styringssetup, og det er en vigtig strategisk beslutning, om organisationen selv skal have processer, roller og ikke mindst kompetencer inden for dette område. Samtidig er det vigtigt, at omkostningerne hertil indregnes, da sammenligningsgrundlaget med eksempelvis traditionel outsourcing eller SaaS ellers vil være ufuldstændigt. Kun i de tilfælde hvor organisationen ønsker at tage ansvar for udvikling, drift, vedligehold og informationssikkerhed mod til gengæld at opnå en bedre dækning af de forretningsmæssige behov, bør IaaS og PaaS anvendes i stedet for SaaS. Dette skyldes, at en succesrig anvendelse heraf forudsætter en række nye kompetencer til eksempelvis design og kodning af systemer til cloud.

Det er her vigtigt at understrege, at ansvar for data er det samme uanset service- og leverancemodel, og der bør ske en organisatorisk forankring af de nødvendige processer for at sikre et tilstrækkeligt tilsyn med leverandører uanset type af servicemodel. Det er centralt, at organisationen ikke undervurderer behovet for at sikre sig de fornødne kompetencer og ressourcer til at sikre et tilstrækkeligt tilsyn og de fornødne organisatoriske processer til at sikre anvendelsen af cloudløsninger i organisationen. For nærmere beskrivelse af dataansvar, herunder hvordan valg af service- og leverancemodel kan have indflydelse på, hvordan dette dataansvar forvaltes, se kapitel 4.

3.2 Agilitet og innovation

Løsninger baseret på IaaS eller PaaS kan være særligt relevante for organisationer, der ønsker at anvende agile processer til udvikling af løsninger eller ønsker kontinuerligt at have adgang til nyeste innovation på et specifikt område, og hvor organisationen selv ønsker en tættere styring af udviklingen, end der er mulighed for med SaaS-løsninger.

Mulighederne ved cloudservices for selvbetjening og automatiserede processer understøtter anvendelsen af agile metoder, da nye versioner af et system kan bringes fra udvikling til produktion meget hurtigt og med meget høj frekvens (fx hver dag). Den høje frekvens af opdateringerne og muligheden for at automatisere en række led i opdateringsprocessen betyder samtidig, at ændringerne ved hver opdatering kan være meget små, hvilket igen minimerer risikoen for, at en opdatering mislykkes. Dette kræver dog, at løsningen er designet til løbende udvikling, eksempelvis ved at være baseret på mikroservices eller ved at være opdelt i containere, der kan opdateres individuelt og rullende, jf. boks 1. For eksisterende løsninger kan det være hensigtsmæssigt at opdele systemet i containere for

at forenkle tilpasninger af løsningens skalérbarhed og mindske løsningens afhængighed af den enkelte cloudleverandør. Det kan her bemærkes, at anvendelsen af virtuelle platforme i en driftsfunktion kan give samme service, forudsat at disse er konfigureret til at kunne skalere i et stort omfang.

Boks 1
Container

En container er en standardiseret softwarepakke, der indeholder kode og alt underliggende software, som koden er afhængig af for at kunne køre isoleret. Det betyder, at en applikation, der er pakket i en container, i langt højere grad er uafhængig af den specifikke platform. Den kan altså flyttes fra én platform til en anden, uden at det kræver andet end de allermest basale integrationer. Det giver stor fleksibilitet og understøtter leverandøruafhængighed.

Mikroservices og containere kan også anvendes i traditionelle server-baserede løsninger. Sådanne løsninger kan ofte migreres til cloud uden grundlæggende ændringer. Løsninger, der ikke har denne arkitektur og opdeling, vil oftere skulle gennemgå større ændringer for at kunne opnå de største fordele ved at migrere til cloud. Er der ikke en positiv business case i at gennemføre større ændringer, kan cloudservices for disse løsninger i stedet være en attraktiv mulighed for hurtigt at etablere og nedlægge test- og udviklingsmiljøer i stedet for at have dedikerede servere til formålet.

Med en cloudløsning får anvenderen typisk også automatisk adgang til nyeste version af softwarefunktionaliteter. Det kan være brugervendte SaaS-løsninger som ESDH-systemer, regneark, skriveprogrammer og lignende., Det kan også være systemkomponenter eller en meget bred og varieret værktøjskasse af eksempelvis analyseværktøjer, BI-værktøjer, algoritmer til maskinlæring og lignende. Uanset om disse anvendes som selvstændige systemer, eller indarbejdes som komponenter i egne systemer, giver udbuddet af funktioner, og hastigheden, hvormed dette udbud udvikles, mulighed for markant at nedbringe udviklingstiden og -omkostningerne for nye løsninger. Ulempen er til gengæld en stigende binding til og afhængighed af den givne cloudleverandør. Se kapitel 3.4 Leverandørafhængighed for beskrivelse af denne problemstilling.

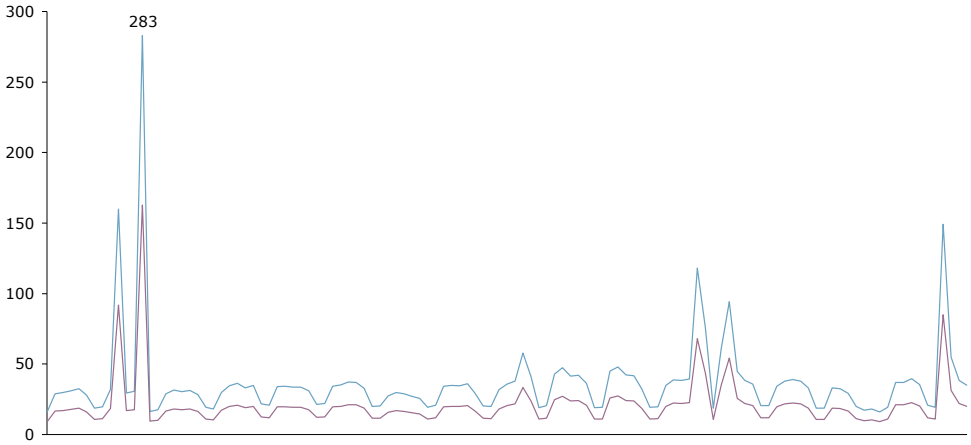
Det er vigtigt at være opmærksom på, at anvendelsen af visse værktøjer og funktioner på en cloudplatform eller i en SaaS-løsning kan forudsætte overførsel af data til tredjelande. Se kapitel 4.3 Tredjelandsoverførsler for nærmere beskrivelse af de juridiske forhold ved overførsler af data til tredjelande, samt kapitel 5.1 Risikovurdering af cloudløsningen for nærmere beskrivelse af de sikkerhedsmæssige forhold.

3.3 Skalering

Med cloudservices opnår organisationen generelt en mulighed for løbende at kunne tilpasse kapaciteten til de faktiske behov. Denne evne til at skalere umiddelbart, er et af de centrale kendetegn ved cloudservices.

Figur 2 viser et eksempel med få, men betydelige udsving i kravet til kapacitet over tid. Stort set alle it-løsninger vil have forskellige kapacitetsbehov over tid, men visse typer af løsninger har særligt store udsving. Det gælder fx:

- Systemer, der i korte perioder anvendes af mange brugere, fx web-baserede, eksternt rettede løsninger, hvor særlige begivenheder kan drive en stor brugeraktivitet, eksempelvis publicering af data, der er relevante for mange brugere, åbning for ansøgninger, særlige tilbud og indberetningsfrister.
- Systemer, hvor der på bestemte tidspunkter gennemføres tunge beregninger, der kræver særlig meget computerkraft, eller hvor der overføres meget data.



Figur 2: Eksempel på kapacitetsbehovet for en applikation.

Skal man håndtere disse spidsbelastninger i et traditionelt serverbaseret setup, er man enten nødt til at dimensionere sin kapacitet efter dem, hvilket leder til betydelig og omkostningsbærende overkapacitet resten af tiden, eller dimensionere efter en mere gennemsnitlig belastning, hvor der så ved spidsbelastninger må accepteres lange svartider og andre udfordringer.

Det er dog vigtigt at notere sig, at skalering ikke behøver at være alt eller intet i cloud. Det er muligt, og kan være økonomisk fordelagtigt, at dække sin minimum- eller gennemsnitlige belastning via in-house servere og nøjes med at skalere til cloudservicen ved spidsbelastninger. Hvis ens forretningsapplikationer behandler meget store datamængder og er meget tidsfølsomme, er det væsentligt at være opmærksom på, om den geografiske afstand til cloud-datacentre kan resultere i lang reaktionstid. For at opnå tilfredsstillende performance, kan en løsning eksempelvis baseres på hybrid cloud, hvor in-house cloudservere skalerer til større cloud-datacentre ved spidsbelastning.

Uanset om systemet er baseret udelukkende på cloudservices eller kun skalerer til cloudservices ved spidsbelastninger, er det i skaleringsøjemed afgørende for mulighederne for omkostningseffektivt at kunne anvende cloudservices, at systemet er designet til at kunne skalere hensigtsmæssigt. Det kræver, at systemet er designet til at skalere lige præcis den komponent, der er særligt behov for i det specifikke øjeblik, hvilket kan opnås ved eksempelvis at lade applikationen være inddelt i containere efter ens skaleringsbehov. Systemer, der er udviklet til drift på traditionelle servere, vil sjældent have denne indre opdeling af komponenterne i veldefinerede, selvstændige enheder. Skaleringsbehovet skal derfor understøttes af et skaleringsparat systemdesign.

Et skaleringsparat design bidrager samtidig til løbende udvikling og vedligehold samt til bedre økonomistyring, fordi det giver mulighed for at vedligeholde eller forny præcis de komponenter, der er behov for, uden at dette har indflydelse på resten af løsningen. Dette kan også have positiv indflydelse på sikkerheden. Se kapitel 3.4 Leverandørafhængighed, 3.5 Økonomistyring og 5. Sikkerhedsmæssige overvejelser for uddybning heraf.

Helt generelt kan det derfor siges, at eksisterende applikationer, der flyttes til et cloudmiljø, tager eventuelle problemer med, eksempelvis performanceproblemer og problemer med vedligehold. For at kunne udnytte fordelene ved cloudservices er det afgørende, at it-systemerne etableres med cloud-applikationsarkitektur.

3.4 Leverandørafhængighed

Al anvendelse af it skaber en vis afhængighed til de teknologier, som anvendes eller de leverandører, hvis kompetencer benyttes. Dette gælder uanset, om løsningen er en hyldevare eller er udviklet til det specifikke forretningsformål. Særligt i den offentlige sektor, hvor ressortændringer, politiske initiativer med videre med jævne mellemrum påvirker, deler eller samler it-landskaber i nye konstellationer, er det derfor vigtigt, at løsningerne er forberedt til forandring, såvel teknisk som kontraktuelt.

Leverandørafhængighed opstår, når man etablerer en binding, eksempelvis teknisk, kontraktuelt eller kompetencemæssigt, til én specifik leverandør, hvilket kan vanskeliggøre genudbud eller videreudvikling af løsninger. Bindinger kan være på enkelte komponenter eller følge som konsekvens af kompleksiteten af et system med mange integrerede komponenter. Graden af afhængighed kan dog variere, og det er derfor centralt ved al anvendelse og udvikling af it at minimere afhængigheder og at have en klar exit-strategi. Dette gælder også for cloudservices. Ved valg af standardiserede SaaS-løsninger vil anvenderen typisk have begrænset mulighed for omkostningseffektivt at påvirke leverandørens valg af underliggende teknologier eller udviklingen af nye funktioner. Anvenderen af en SaaS-ydelse er derfor afhængig af leverandøren til at vurdere behov og tempo for udvikling af ydelsen. Ved anvendelse af SaaS-løsninger vil et skift af leverandør ofte

indebære en fuld udskiftning af løsningen, som det også kendes fra serverbaseret software.

Hvis en organisation selv ønsker at have ejerskab til en løsning for at mindske afhængigheden af én leverandør og muliggøre leverandørskift uden fuld udskiftning af løsningen, kan opbygning af løsninger på en cloudinfrastruktur (IaaS) eller -platform (PaaS) være en attraktiv mulighed. Det er dog centralt, at man i den forbindelse analyserer de totale omkostninger til en sådan løsning. I denne situation vil man kunne blive mindre afhængig af forskelige applikationsleverandører, men mere afhængig af en cloudleverandør. Derfor skal man overveje, hvordan man undgår en for stærk afhængighed af den specifikke cloudinfrastruktur eller -platform. Dette opnås bl.a. ved at designe sin løsning til at blive idriftsat i containere og ved kun at anvende leverandørspecifikke komponenter og funktioner, hvis det vurderes effektivt i lyset af de langsigtede omkostninger ved en stærk binding til de pågældende komponenter.

Boks 2

Arkitekturmæssig understøttelse af forretningsmæssige overvejelser

For at understøtte de i kapitlet beskrevne forretningsmæssige overvejelser, herunder at sikre at applikationer og data kan flyttes til en anden cloudplatform med et minimum af tekniske og økonomiske konsekvenser, og at der er klarhed over de omkostninger, der vil være ved at flytte til en anden cloudplatform, kan følgende overvejes:

- **Adskil data, applikation og service og administrer individuelt (design):** Data, applikationer og services har forskellig forventet levetid. Data kan være relevant i årtier, applikationer kan ofte undergå forandringer for at imødekomme nye behov og regler, og services kan indgå i et komplekst landskab af interne og eksterne systemer, der indebærer et særligt governance-setup. Adskillelsen af de tre lag maksimerer råderummet for hvert lag og er fundamentet for at undgå leverandørafhængighed.
- **Opdel applikationer og idriftsæt i containere (design):** Applikationer opdeles i hensigtsmæssige komponenter, der hver især idriftsættes i applikations-containere, der er bredt understøttet, frem for direkte på cloudplatformen. Hermed kan applikationer lettere flyttes til andre platforme med begrænsede omkostninger.
- **Tilgå cloudplatformen via åbne snitflader (design):** På mange cloudplatforme udvikles der løbende nye ressourcer og funktioner, som kan anvendes enten selvstændigt eller integreret i en løsning. Nogle af disse funktioner vil være baseret på proprietære snitflader og teknologier, andre på åbne snitflader og teknologier. Anvend så vidt muligt funktioner, der er baseret på åbne snitflader og teknologier. Hermed muliggøres, at tilsvarende ressourcer og funktioner kan anvendes på en anden cloudplatform.
- **Anvend kryptering ved både opbevaring og transport af data (design):** Kryptering af data er central for at understøtte databeskyttelse gennem design og sikkerhed gennem design. Krypteres data ved både opbevaring og transport, sikres det, at data ikke umiddelbart kan opsnappes, og at konsekvenserne ved et sikkerhedsbrud på datalaget igennem komponenter uden for ens umiddelbare kontrol minimeres. Anvendes en uafhængig tredjepart som leverandør af krypteringsnøgler, minimeres afhængigheden af leverandøren af cloudservices (eksempelvis platformleverandøren), men det kan tilføje andre sikkerheds- og leverandørstyringsmæssige risici.
- **Dokumenter exit-strategien (forretning):** Ved etablering af bindinger til en cloudløsning bør alternativer dokumenteres således, at det sandsynliggøres, at de umiddelbare gevinster, der opnås i kraft af bindingerne, står mål med de fremtidige omkostninger ved evt. senere at bryde disse bindinger. I omkostningerne bør indgå såvel økonomiske, tekniske, tidsmæssige som produktionsmæssige omkostninger. Denne exit-strategi bør regelmæssigt genbesøges.

En opdelt og flytbar arkitektur understøtter, at løsninger kan udvikles på én cloudplatform og på et senere tidspunkt overflyttes til en anden dataplatform baseret på åbne standarder med færre omkostninger, samt at der tages eksplicit og strategisk stilling til eventuelle bindinger, der etableres til en cloudplatform.

3.5 Økonomistyring

Cloudservices kan være billigere end traditionel datacenterdrift, eksempelvis for løsninger med stort behov for skalering. Hvor den traditionelle serverløsning kræver, at man altid skal have nok kapacitet til at dække spidsbelastningsbehovet, giver cloudservices mulighed for løbende at skalere efter det nøjagtige behov. Dette kan give betydelige økonomiske gevinster for systemer med store udsving i belastningen. For løsninger med relativt konstant behov kan anvendelsen af cloudservices også blive dyrere, fordi cloudleverandørens priser ved stabilt forbrug måske ikke er konkurrencedygtige i forhold til traditionel serverdrift. Her skal man være særligt opmærksom på, at alle omkostninger tages med i betragtning for såvel cloud- som serverløsningen.

Det kan dog være yderst vanskeligt på forhånd at gennemskue cloudmetrikker og svært at sammenligne priser fra forskellige cloududbydere. Det er derfor vigtigt, at man har gjort sig klart, hvad det forventede brugsscenarium er og kan gøre rede for de forventede omkostninger.

Ved SaaS er afregningsmetrikkerne forskellige fra løsning til løsning, men de er ofte prissat efter relativt få metrikker – fx antal brugere, antal transaktioner, sager eller andet, der er udtryk for, hvor meget løsningen anvendes. Ofte er der flere muligheder for den samme løsning; der kan fx vælges at betale pr. bruger eller pr. transaktion. Nogle metrikker kan give en høj forudsigelighed, eksempelvis antallet af medarbejdere på løsningen, men der kan også afregnes efter metrikker, der kan være vanskelige at forudsige, fx antallet af transaktioner eller sager.

For IaaS og PaaS er der typisk langt flere prismetrikker, og der afregnes i mindre tidsintervaller. En af disse metrikker kan være netværkstrafik, og der kan her være forskel på, om data overføres til eller fra skyen. Det betyder, at hvis man fx har en applikation, hvor brugerne henter meget data, kan det have en stor indvirkning på den samlede pris for drift af løsningen. Uanset hvilke metrikker, der anvendes i den specifikke konfiguration af service- og leverancemodel, er det derfor vigtigt at have fuldt overblik over metrikkerne. Dernæst kan man søge at få metrikkerne låst i en længere aftaleperiode. På baggrund af overblikket over metrikker, samt en prognose for udviklingen af behovene, kan der etableres en business case. Hvis man ikke på forhånd har lavet realistiske beregninger af behovene, vil det være vanskeligt at forudsige de økonomiske konsekvenser af selv simple metrikker.

På grund af kompleksiteten af metrikkerne kan de praktiske økonomiske konsekvenser af en implementering dog være svære at beregne på forhånd. For at forbedre beslutningsgrundlaget om de økonomiske konsekvenser kan man derfor

gøre brug af beregningssimulationsløsninger, der stilles til rådighed af cloudleverandører, eller man kan med fordel udnytte cloudmodellens iboende fleksibilitet til at gøre indledende praktiske erfaringer med cloudservicen, inden der træffes endelig beslutning om implementering for hele løsningen.

Selvom kompleksiteten i afregningen afhænger af den valgte service- og leverancemodel, vil anvendelsen af cloudløsninger ofte indebære mere uforudsigelige driftsomkostninger. Dette er en konsekvens af cloudløsningens løbende skalering til det faktiske forbrug, og er derfor som udgangspunkt positivt. Det betyder dog, at organisationen skal være forberedt på, at der kan være store variationer i betalingen måned for måned, samt at fakturaerne kan være langt mere omfattende og detaljerede end normalt. På grund af den høje detaljeringsgrad for afregningen af metrikkerne er det eksempelvis ikke unormalt, at fakturaer for forbruget af IaaS eller PaaS over nogle måneder kan have over 10.000 fakturalinjer. Fordi fakturaer af denne karakter ikke kan håndteres på samme måde som almindelige fakturaer, stiller det krav til en række nye processer i organisationen til at analysere og godkende faktureringen samt håndtere budgetusikkerheden.

Udover løbende at følge forbruget i forhold til det budgetterede, skal organisationen også være i løbende dialog med sine udviklere om, hvordan anvendelsen af de primære udgiftsdrivende ressourcer kan nedbringes. Muligheden for at påvirke anvendelsen af specifikke udgiftsdrivende ressourcer er dog betinget af, at anvendelsen af hver ressource kan håndteres individuelt. Dette forudsætter, at løsningen er designet hertil ved at være opdelt i hensigtsmæssige delkomponenter, der eksempelvis hver især er idriftsat i containere.

Hvis skaleringsbehovene er rutineprægede, kan det give en økonomisk gevinst at undersøge mulighederne for at reservere kapacitet hos udbyderen, da ressourcerne så kan fås med en væsentlig rabat i forhold til listeprisen for skalering efter realtidsbehov.

Vær opmærksom på, at udbudslovens tærskelværdier stadig gælder, selvom en offentlig organisation anvender en cloudservice, der afregnes efter forbrug. Dette betyder, at overskrider ens forbrug de relevante tærskelværdier, skal behovet for cloudservices sendes i udbud. Dette har især konsekvenser for løsningens arkitektur, da det betyder, at forretningsapplikationen skal være forberedt til at blive migreret fra én leverandørs IaaS- eller PaaS-service til en anden leverandørs IaaS- eller PaaS-service.

Boks 3

Opsummering på økonomistyring

For at opnå en tilfredsstillende økonomistyring er følgende afgørende:

- Afklar det forventede brugsscenarium
- Hav overblik over afregningsmetrikkerne
- Vurder forbrug på relevante afregningsmetrikker
- Vurder finansielle risici forbundet med usikkerhed af forbrug
- Overvej særskilte aftaler om forbrugsloft, reserveret kapacitet og lignende
- Overvåg løbende forbrug

Juridiske overvejelser

4. Juridiske overvejelser

Både offentlige og private aktører kan benytte sig af cloudservices, men som ved ethvert andet kontraktforhold sætter lovgivningen visse rammer for anvendelsen, bl.a. udbudslovgivningen og databeskyttelseslovgivningen. Overordnet set handler det om at sikre, at det juridiske grundlag, de sikkerhedsmæssige foranstaltninger og organisationens risikovurdering af løsningen svarer til hinanden og muliggør en tilstrækkelig kontrol af, at leverandøren lever op til aftalte krav. Vurderingen bør altid tage udgangspunkt i en konkret risikovurdering af løsningen og af de registreredes rettigheder, som eventuelt skal suppleres med en konsekvensanalyse, hvis behandlingen af personoplysninger vurderes at indebære en høj risiko for de registreredes rettigheder.

Som ved anden anvendelse af leverandører, er det ved anvendelse af cloudservices ikke altid muligt for en anvender fysisk at kontrollere, at en leverandør efterlever alle relevante juridiske krav. Generelt må anvenderen i stedet læne sig op ad leverandørens dokumentation af overholdelse af kravene. Det gælder derfor for hovedparten af nedenstående, at myndigheden i forbindelse med markedsafdækning og kontraktindgåelse, samt løbende under kontraktforholdet, nøje må vurdere den foreliggende dokumentation, herunder certificeringer og revisionserklæringer, for overholdelsen af hvert af de juridiske krav og de krav, som stilles på baggrund af den konkrete risikovurdering, samt for om der samlet set er tillid til leverandøren.

I dette kapitel gennemgås væsentlige juridiske overvejelser, som en offentlig myndighed bør gøre sig, når man overvejer at anvende cloudservices. De præsenterede overvejelser er også gældende i andre sammenhænge, og er således ikke specifikke for anvendelsen af cloudservices, men vurderes væsentlige for anvendelsen af cloud.

4.1 Særlige krav ved behandling af personoplysninger

Hvis der i et it-system skal behandles personoplysninger, regulerer databeskyttelseslovgivningen de generelle rammer for bl.a. opbevaring og behandling af oplysningerne i systemet.

Personoplysninger er defineret som enhver form for information, der kan henføres til en fysisk person. Der skelnes mellem almindelige og særlige kategorier af personoplysninger, hvor der stilles højere sikkerhedsmæssige krav til behandlingen af særlige kategorier af oplysninger. For nærmere beskrivelse af de forskellige typer personoplysninger, henvises der til Datatilsynets hjemmeside. Ydermere kan eksempelvis sundhedsloven finde anvendelse, hvis der behandles sundhedsoplysninger. Uanset om systemet skal anvende cloudservices eller er baseret på traditionelle servere, bør man derfor først klarlægge, hvilke typer personoplysninger der skal behandles i systemet.

Herefter skal det vurderes, om behandlingen af personoplysninger vil udgøre en høj risiko for de registreredes rettigheder, fx rettigheder for borgere eller ansatte. Hvis dette er tilfældet, skal der udarbejdes en konsekvensanalyse, se kapitel 4.4 Konsekvensanalyse. Det er vigtigt at belyse konsekvenserne af behandlingen af personoplysninger tidligt i anskaffelsesprocessen, da en høj risiko kan have konsekvenser for anvendelsen af cloudløsninger, herunder hvilke cloudleverandører, der kan anvendes. En høj risiko for de registreredes rettigheder betyder, at man i design af system og tilhørende forretningsprocesser skal være særligt opmærksom på at reducere denne risiko.

Herudover er der en række rettigheder i databeskyttelsesforordningen, der skal overholdes, bl.a. at den registrerede har ret til indsigt i data om pågældende, ret til berigtigelse, ret til sletning og ret til indsigelse. Disse rettigheder gøres som udgangspunkt gældende over for den dataansvarlige, men leverandøren kan forpligtes til at bistå med udøvelsen af disse rettigheder. For nærmere beskrivelse af de registreredes rettigheder henvises der til Datatilsynets "*Vejledning om de registreredes rettigheder*" (juli 2018).[3]

Uanset om der anvendes cloudservices eller traditionelle servere, skal man være opmærksom på, at de registreredes rettigheder understøttes i både forretningsapplikationen, den underliggende it-infrastruktur, og de tilhørende organisatoriske processer hos hver aktør, der bidrager til det samlede system. Eksempelvis vil leverandøren af forretningsapplikationen skulle sikre, at de registreredes rettigheder sikres med hensyn til berigtigelse, sletning og indsigt, og at disse også understøttes i processer for gendannelse af data fra backup. Tilsvarende vil leverandøren af den underliggende it-infrastruktur skulle sikre, at de registreredes rettigheder sikres i forbindelse med eksempelvis bortskaffelse af hardware.

4.2 Databehandleraftaler

Når man anvender cloudservices til behandling af personoplysninger - enten direkte eller som underleverandør til en leverandør af en forretningsapplikation - anses leverandøren af cloudservicen i juridisk forstand normalt for at være en databehandler. Den offentlige organisation, databehandlingen foretages på vegne af, anses for at være dataansvarlig. I disse situationer stiller databeskyttelsesforordningen krav om, at der indgås en databehandleraftale. En sådan databehandleraftale skal leve op til en række minimumskrav, eksempelvis at cloudleverandøren udelukkende må handle efter instruks fra den dataansvarlige. Ligeledes må leverandøren kun benytte sig af underleverandører, hvis den dataansvarlige på forhånd har givet en generel eller specifik godkendelse heraf.

Som dataansvarlig har en offentlig organisation, der ønsker at anvende en cloudservice, det fulde ansvar for at vælge en cloudleverandør, der håndterer person-

[3] Datatilsynet, juli 2018, *Vejledning om de registreredes rettigheder*.

oplysninger i overensstemmelse med databeskyttelseslovgivningen. Den offentlige organisation er således som dataansvarlig direkte ansvarlig dels for overholdelsen af databeskyttelseslovgivningen og dels for at kunne dokumentere en sådan overholdelse. Af hensyn til den dataansvarliges forpligtelse til at føre kontrol og tilsyn med overholdelsen af databeskyttelsesreglerne, følger det af lovgivningen, at den offentlige organisation som dataansvarlig skal sikre sig, at cloudleverandøren forpligtes til at stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene, til rådighed. Cloudleverandøren skal ligeledes give mulighed for og bidrage til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Såfremt det efter en konkret risikovurdering anses for tilstrækkeligt med en årlig indhentelse af en revisionserklæring, kan dette aftales mellem leverandøren og anvenderen i databehandleraftalen.

Mens det ved indkøb af private eller fælles cloudløsninger kan være muligt at indgå en kundetilpasset databehandleraftale med leverandøren af cloudservicen, vil leverandører af offentligt tilgængelige cloudservices ofte kun anvende egne standarddatabehandleraftaler. Dette er ikke nødvendigvis et problem, da cloudleverandørerne i stigende grad lever op til fælleseuropæiske regler på området. Såfremt man, efter en gennemgang af disse og en eventuel drøftelse med leverandøren om vilkårene, finder, at aftalen er tilstrækkelig, kan man indgå en aftale om brug af deres cloudservices. Det påhviler dog den offentlige organisation som dataansvarlig at sikre sig, at den pågældende aftale lever op til alle lovgivningsmæssige krav samt dækker eventuelle øvrige behov.

Datatilsynet har udarbejdet en standarddatabehandleraftale,[4] som kan anvendes, da den sikrer, at parterne lever op til databeskyttelsesforordningens minimumskrav. Der er ikke noget til hinder for, at der benyttes en anden databehandleraftale, hvis denne lever op til samme minimumskrav. Da en række cloudleverandører anvender egne standardkontrakter for behandlingen af personoplysninger, skal man dog være opmærksom på, at krav i et udbud om anvendelse af specifikke databehandleraftaler kan betyde, at cloudservices, der ellers måtte vurderes at være attraktive, må fravælges.

Hvis en offentlig organisation har krav, der går ud over minimumkravene i databeskyttelseslovgivningen, kan der være nogle områder, hvor cloudleverandørers standardaftaler ikke lever op til disse ekstra krav, selvom leverandørens standardaftale lever op til minimumkravene i databeskyttelsesforordningen. Hvis der i et EU-udbud er stillet krav, der går ud over minimumkravene i databeskyttelsesforordningen, skal man være særligt opmærksom på, at:

- sådanne skærpede krav ikke efterfølgende umiddelbart kan frafaldes, også selvom de vurderes at have været unødvendige.

[4] Datatilsynet, standarddatabehandleraftale.

- hvis sådanne skærpede krav ikke honoreres af cloudleverandørens standardaftale, vil den nødvendige konsekvens ofte være, at cloudleverandøren må fravælges.

I forbindelse med formuleringen af krav til udbud er det derfor ofte væsentligt, at man som led i markedsafdækningen nøje har klarlagt, hvilke sikkerhedsmæssige tiltag markedet tilbyder for at imødegå forskellige typer af risici samt hvilke vilkår, disse tiltag tilbydes under.

4.3 Tredjelandsoverførsler

Når personoplysninger overføres til et tredjeland, hvilket i denne sammenhæng vil sige et land, som ikke er medlem af EU eller EØS, skal de særlige regler om overførsel af personoplysninger til tredjelande i databeskyttelsesforordningens kapitel 5 iagttages. Formålet er at sikre, at beskyttelsesniveauet er tilstrækkeligt, selvom data bliver opbevaret i eller tilgået fra lande, der ikke er direkte omfattet af forordningen. Når der overføres personoplysninger til et tredjeland, skal der, ud over en databehandleraftale, foreligge et overførselsgrundlag.

Som udgangspunkt skelnes der mellem såkaldte *sikre* og *usikre* tredjelande. Et *sikkert* tredjeland er et land, som EU-Kommissionen har vurderet er *tilstrækkeligt* sikkert, og som det på den baggrund er godkendt at overføre personoplysninger til. Bliver personoplysninger således behandlet i et af landene på listen, er det ikke nødvendigt at indhente yderligere garantier i medfør af databeskyttelseslovgivningen. For disse sikre lande udgør EU-Kommissionens vurdering det fornødne overførselsgrundlag. Listen over sådanne lande opdateres løbende af EU-Kommissionen.[5]

Det skal bemærkes, at USA ikke er på listen over sikre tredjelande, men at certificeringsordningen EU-U.S. Privacy Shield tidligere er blevet vurderet tilstrækkeligt sikker. Den Europæiske Unions Domstol har dog d. 16. juli 2020 afgjort, at EU-U.S. Privacy Shield ikke yder tilstrækkelig beskyttelse[6], hvorfor denne ikke længere kan anvendes som overførselsgrundlag. Der henvises til Datatilsynet for yderligere information. Denne vejledning vil blive opdateret, når eventuelle andre konsekvenser af dommen er klarlagt.

Hvis man overvejer at benytte en cloudleverandør i et *usikkert* tredjeland til behandling af personoplysninger, skal man som offentlig myndighed, som ved anden databehandling, sikre, at databeskyttelseslovgivningen i sin helhed overholdes, at der foreligger et overførselsgrundlag, og at der er et tilstrækkeligt sikkerhedsniveau for behandlingen.
Databeskyttelsesforordningen muliggør forskellige typer af overførselsgrundlag

[5] Listen over lande, for hvilke EU-Kommissionen har truffet en såkaldt "tilstrækkelighedsafgørelse", kan findes på Europa-Kommissionens hjemmeside.
[6] Se pressemeddelelse fra Den Europæiske Unions Domstol om dom i sagen C311/18

til usikre tredjelande, eksempelvis bindende virksomhedsregler (BCR), adfærdskodekser og certificeringsmekanismer.[7] EU-Kommissionen har udgivet en standardkontrakt,[8] som kan benyttes som overførselsgrundlag imellem en dataansvarlig i EU/EØS og en databehandler uden for EU/EØS. Der kan læses mere herom i Datatilsynets *"Vejledning - Overførsel af personoplysninger til tredjelande*" (juni 2019).[9] Hvis man som offentlig myndighed indgår en kontrakt med en databehandler i EU, der gør brug af en underdatabehandler i et sikkert eller et usikkert tredjeland, skal man således være særligt opmærksom på, at ansvaret for behandlingen og sikkerheden ved behandlingen er delegeret til underdatabehandleren, og at den oprindelige databehandler forbliver fuldt ansvarlig over for den dataansvarlige, hvis underdatabehandleren ikke opfylder sine databeskyttelsesretlige forpligtelser. Hvis en dataansvarlig godkender anvendelsen af en underleverandør gælder således, at den dataansvarlige har ansvaret for, at:

1. leverandøren sikrer, at underleverandøren er underlagt samme beskyttelseskrav som leverandøren
2. leverandøren kontrollerer, at disse krav bliver overholdt

Det er dermed som udgangspunkt leverandøren, der sikrer indgåelsen af en tilfredsstillende databehandleraftale med underleverandøren. Det påligger dog den dataansvarlige at sikre sig, at aftaler med eventuelle underleverandører lever op til de vilkår, som parterne aftaler, samt at den oprindelige databehandler fører det aftalte tilsyn med, at underdatabehandleren opfylder betingelserne i databehandleraftalen. Dette kan eksempelvis gøres ved, at databehandleren sender dokumentation for afholdte tilsyn og eventuelle opfølgende handlinger på baggrund af de afholdte tilsyn til den dataansvarlige i form af revisionsrapporter eller andet relevant materiale. Der kan læses mere herom i Datatilsynets "*Vejledende tekst om tilsyn med databehandlere og underdatabehandlere"*.[10]

Når spørgsmålet om overførsel til tredjelande er særligt relevant for cloudservices, skyldes det bl.a., at de store cloudleverandører råder over datacentre i hele verden, og at data kan flyttes imellem disse, hvis den dataansvarlige har godkendt dette for at realisere den samlede service. Det er derfor ikke tilstrækkeligt at afklare, hvorfra cloudleverandøren primært leverer servicen, men det skal også afklares, om der ved hver enkelt af de valgte cloudservices sker en overførsel til et sikkert eller usikkert tredjeland, uanset i hvilket led af leverandørkæden dette måtte forekomme. Hvis det på denne baggrund besluttes at tage servicen i brug, skal det sikres, at der er det fornødne overførsels- og behandlingsgrundlag.

---

[7] Listen over godkendte adfærdskodeks og certificeringsmekanismer kan findes på European Data Protection Board.https://edpb.europa.eu/our-work-tools/accountability-tools_en
[8] EU-Kommissionen, standard kontraktuelle bestemmelser.
[9] Datatilsynet, juni 2019, "Vejledning - Overførsel af personoplysninger til tredjelande".
[10] Datatilsynet, maj 2018, "*Vejledende tekst om tilsyn med databehandlere og underdatabehandlere*".

Fordi cloudbaserede løsninger ofte består af en række individuelle cloudservices, der kan have forskellige sikkerhedspolitikker, kan det ved anvendelsen af cloudservices være særligt gavnligt at indarbejde databeskyttelse gennem design og standardindstillinger for såvel løsning som tilhørende forretningsgange. Herved kan mulighederne for tredjelandsoverførsler dels kortlægges, dels kan sådanne tiltag bidrage til at forhindre, at man uforvarende initierer en overførsel, eksempelvis ved at tage en ny service i brug, ved ikke at opdage, at en anvendt service ændres til at indebære overførsler, eller ved at en service anvendes på måder, den ikke er godkendt til af den dataansvarlige. Se desuden kapitel 4.6 Databeskyttelse gennem design og standardindstillinger. Dette gælder i særlig grad, hvis behandlingen af data indebærer en høj risiko for de registreredes rettigheder, eksempelvis fordi der i stort omfang behandles særlige kategorier af personoplysninger.

Dokumentation af såvel overførselsmulighederne som de tekniske og procesmæssige foranstaltninger til at undgå utilsigtede overførsler skal kunne rekvireres fra leverandøren af forretningsapplikationen og leverandøren af cloudservicen.

Såfremt reglerne i databeskyttelsesforordningens kapital 5 iagttages, og der dermed kan etableres et tilstrækkeligt overførselsgrundlag, samt at det ud fra en risikovurdering og eventuelt en konsekvensanalyse vurderes, at der er et passende sikkerhedsniveau, er der således ikke noget generelt til hinder for at anvende en cloudløsning, der indebærer overførsel af data til tredjelande. Domænespecifik lovgivning, som sundhedsloven og retshåndhævelsesloven, kan dog stille skærpede krav på området. Se kapitel 4.7 Øvrig lovgivning for uddybning.

4.4 Konsekvensanalyse

Databeskyttelsesforordningen stiller krav om, at der forud for påbegyndelsen af en ny type behandling af personoplysninger foretages en konsekvensanalyse, når den behandling, der ønskes foretaget, sandsynligvis vil indebære en *høj risiko* for fysiske personers rettigheder og frihedsrettigheder. Dette omfatter bl.a. situationer, hvor der foretages profilering ved hjælp af en systematisk og omfattende vurdering af personlige forhold, og tilfælde hvor der i stort omfang behandles særlige kategorier af personoplysninger.

Anvendelsen af cloudservices betinger i sig selv ikke udarbejdelsen af en konsekvensanalyse. Anvendelse af ny teknologi kan dog øge risikoen for fysiske personers rettigheder og frihedsrettigheder, eksempelvis ved anvendelse af kunstig intelligens til understøttelse af myndighedsopgaver. Pligten indtræder i det omfang, der er tale om en "høj risiko" for fysiske personers rettigheder og frihedsrettigheder. Offentlige myndigheder vil derfor ikke i alle tilfælde være forpligtede til at udarbejde en konsekvensanalyse. Det er vigtigt at være opmærksom på, at pligten til at udarbejde en konsekvensanalyse inden en behandling påbegyndes ikke er det samme som den indledende og herefter den løbende årlige risikovurdering, som offentlige myndigheder skal foretage efter sikkerhedsstandarden ISO27001.

En nærmere gennemgang af reglerne kan findes i Datatilsynet og Justitsministeriets vejledning *"Konsekvensanalyse"* (marts 2018),[11] samt Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse.

Hvis der er behov for at udarbejde en konsekvensanalyse, kan ISO 29134, der er en international standard til udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, med fordel benyttes.

4.5 Lokationskravet i databeskyttelsesloven

Det følger af databeskyttelseslovens § 3, stk. 9, at justitsministeren efter forhandling med vedkommende minister kan fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvist alene må opbevares hér i landet.[12] Det kan eksempelvis gælde for visse større, landsdækkende administrative systemer og specialregistre. For nærmere beskrivelse af lokationskravet, herunder hvilke systemer, der kan vurderes at være omfattet heraf, henvises til Justitsministeriets kommende vejledning herom.

Hvis et system er omfattet af lokationskravet, medfører det begrænsninger i brugen af cloudleverandører til disse it-systemer. Selvom cloudservices og anvendelse af internationale leverandører ikke generelt er et problem med hensyn til lovgivningen, så vil it-systemer, der er omfattet af lokationskravet, helt eller delvist skulle placeres i Danmark af hensyn til statens sikkerhed.

Dette vil i praksis forhindre disse løsninger i at blive driftet hos de fleste internationale cloudleverandører, men udelukker ikke som sådan, at der anvendes cloudservices. I denne situation skal cloudservicen blot være inden for Danmarks grænser, bl.a. ved at være baseret på datacentre på dansk jord.

Det er her væsentligt at bemærke, at en geografisk afgrænsning af en cloudservice til dansk jord ikke er ensbetydende med, at cloudleverandørens generelle sikkerhedsniveau er tilstrækkeligt. Uanset placeringen af cloudleverandøren er det derfor vigtigt, at man nøje undersøger og vurderer leverandørens sikkerhedsniveau, jf. kapitel 5. Sikkerhedsmæssige overvejelser.

4.6 Databeskyttelse gennem design og standardindstillinger

Databeskyttelsesforordningens artikel 25 medfører krav om, at den dataansvarlige allerede fra tidspunktet, hvor midlerne for behandlingen fastlægges, skal gennemføre tekniske og organisatoriske foranstaltninger, der sikrer en effektiv implementering af de grundlæggende databeskyttelsesprincipper, opfyldelse af kravene i forordningen og beskyttelse af registreredes rettigheder.

---

[11] Datatilsynet og Justitsministeriet, marts 2018, *"Konsekvensanalyse"*.
[12] Lokationskravet afløser den såkaldte "krigsregel" efter persondatalovens § 41, stk. 4.

Reglerne om databeskyttelse gennem design og standardindstillinger findes i forordningens artikel 25. En nærmere gennemgang af bestemmelsen kan findes i Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsens vejledning "*Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger*".[13]

Derudover kan standarderne ISO 27701, 27017 og 27018 med fordel anvendes til at kortlægge sammenhænge mellem bestemmelser i GDPR og informationssikkerhedskrav, samt stille specifikke krav om informationssikkerhed til cloudløsninger. Standarderne supplerer organisationens eksisterende sikkerhedsarbejde med ISO 27001.

En myndigheds hjemmel til at indsamle og behandle personoplysninger er uafhængig af, om it-systemet, behandlingen foretages i, er baseret på traditionelle servere eller cloudservices. Anvendelsen af cloudservices kan dog have indflydelse på, hvordan behandlingen finder sted, og dermed hvilke designmæssige tiltag, der kan være relevante. Sådanne cloudrelevante designvalg kan eksempelvis være:

- Geografisk afgrænsning af datas opbevaring til lande inden for EU, herunder EØS, eller et sikkert tredjeland. Denne afgrænsning kan være aftalebaseret, men den kan også være teknisk understøttet i form af eksempelvis automatisk deaktivering af services, der indebærer overførsel til tredjelande.
- Kortlægning af mulighederne for og eventuelt begrænsning af overførslen af data i forbindelse med support. Dette kan eksempelvis gøres ved at indgå aftale med cloudleverandøren om og teknisk realisere, at support udelukkende finder sted fra lande i EU og EØS eller sikre tredjelande.
- Kryptering af data i transit og i hvile og eventuelt pseudonymisering af data ved behandling. Dette kan minimere konsekvenserne for de registrerede ved kompromittering af datas fortrolighed.

Hertil kan det være væsentligt at være opmærksom på, at der ikke uforvarende indsamles oplysninger, som servicen ikke er indrettet til. Dette kan eksempelvis være indsamlingen af oplysninger som cpr-nummer, sundhedsoplysninger eller andre typer oplysninger af relevans for sagsbehandlingen i kontaktformularer til generelle henvendelser eller i almindelig mail. Her vil det være hensigtsmæssigt dels at informere borgerne klart og tydeligt om, hvad kontaktkanalen kan benyttes til, dels i designet af løsningen at have indarbejdet datavalideringsmekanismer, der sikrer, at borgerne ikke kan angive oplysninger, som bør formidles igennem andre kontaktkanaler, så som digital post.

Uanset hvilke designmæssige valg af tekniske eller organisatoriske foranstaltninger, der gennemføres for at understøtte databeskyttelse, er det dog særligt vigtigt, at man er i stand til at kontrollere det faktiske beskyttelsesniveau og er i stand til

---

[13] Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen, juni 2018, "*Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger*".

at reagere på tegn på uønsket adfærd. I den forbindelse kan det være hensigtsmæssigt at sikre sig adgang til loginformation om tilgang til data, og at denne information behandles løbende.

Det er her vigtigt at understrege, at princippet om databeskyttelse gennem design også gælder ved brug af on-premise-løsninger. Det er dog særligt vigtig ved anvendelse af cloudservices, da hver service i en samlet løsning kan have sin egen informationssikkerhedspolitik, eksempelvis for tredjelandsoverførsler. Man bør derfor sikre, at hver service kun anvendes som tiltænkt og godkendt.

4.7 Øvrig lovgivning

Ud over de lovgivningsmæssige krav, der er beskrevet ovenfor, kan der være særlige krav, som følger af andre regler, lovgivning og reguleringsmæssige regimer, der kan have konsekvenser for anvendelsen af cloudservices. Som udgangspunkt følger det af EU-forordningen 2018/1807, at andre typer data end persondata frit kan lagres og behandles overalt i EU. I nogle tilfælde kan det dog være relevant at iagttage eksempelvis bogføringsloven og regnskabsloven, der indeholder regler om opbevaring af regnskabsmateriale samt arkivloven, der gælder for offentlige myndigheder og som kan have afledt betydning for en myndigheds opbevaring af sit sagsbehandlingssystem. Ligeledes kan sundhedsloven begrænse anvendelsen af cloudservices ved behandling af sundhedsdata, og retshåndhævelsesloven kan begrænse retshåndhævende myndigheders anvendelse af cloudservices. Tilsvarende kan særlig regulering eller certificering under certificerings- og standardiseringsordninger begrænse anvendelsen af cloudservices ved at stille krav om, at organisationens it-systemer skal valideres – det vil sige, at systemerne testes efter særligt udførlige test-procedurer, og der er skærpede krav til dokumentation og navnlig håndtering af ændringer. I et sådant miljø kan tvungne opdateringer fra en cloudleverandør eller ændringer af et hardware-setup være udfordringer, der skal håndteres i validerings-processerne.

Er man underlagt sådanne krav, bør det derfor indgå relativt tidligt i markedsafdækningen og tidligt i design af løsning, hvorvidt og hvordan det vil være muligt at opretholde efterlevelsen af disse krav. Som nævnt i kapitel 4.5 Lokationskravet i databeskyttelsesloven indebærer sådanne regler dog ikke nødvendigvis, at cloudservices som sådan ikke kan anvendes, blot valg af service- og leverancemodeller samt leverandør tilpasses herefter.

Boks 4

Øvrige relevante kontraktbestemmelser

I tillæg til de ovenfor fremhævede juridiske forhold, er der en række krav, som kan være særligt relevante ved indkøb af cloudservices:

- **Sørg for, at aftalen indeholder en veldefineret Service Level Agreement.** Hvad er forventningen eksempelvis til oppetider, svartider, tidshorisont for fejlrettelser og evt. bodsbestemmelser?
- **Katastrofeberedskab.** Aftalen bør adressere, hvad der sker, hvis leverandøren rammes af pludselige og udefrakommende **uforudsete** omstændigheder, der fører til tab af data? Hvad er eksempelvis kravene og forpligtelserne med hensyn til genskabelse af data, genoprettelse af drift eller udlevering af backup?
- **Hvad sker der ved opkøb, fusion mv. af leverandøren.** Hvordan påvirker det aftaleforholdet, hvis leverandøren opkøbes, fusioneres eller indgår i en ny virksomhedskonstruktion?

Sikkerhedsmæssige overvejelser

5. Sikkerhedsmæssige overvejelser

Ved fastlæggelse af sikkerhedsniveauet for et it-system er det vigtigt at være opmærksom på, at der ikke er nogle udtømmende, objektive kriterier for sikkerhed. Som offentlig organisation med ansvar for data og for anvendelsen af en samlet it-løsning er det derfor et spørgsmål om i forbindelse med risikovurderingen at få kortlagt sikkerhedsbehovene og sammenholdt disse med sikkerhedsprofilerne for forskellige typer løsninger.

Cloudløsninger kan på nogle områder være mere sikre end andre alternativer. Den høje standardiseringsgrad, der kendetegner cloudservices, giver generelt mulighed for at etablere meget robuste strukturer, og især de store cloudleverandører er typisk kendetegnet ved en høj grad af teknisk ekspertise og et systematisk fokus på såvel fysisk som logisk sikkerhed. Det betyder eksempelvis typisk meget restriktive adgangspolitikker, og at en hændelse i ét datacenter ikke påvirker driften, da der på grund af geografisk redundans automatisk skiftes til et andet. Cloudleverandører tilbyder desuden ofte en bred vifte af sikkerhedsprodukter og ydelser, der yderligere kan sikre systemlandskabet.

Det kan dog også byde på sikkerhedsmæssige udfordringer at anvende cloudservices, da det eksempelvis kan være sværere for anvenderen selv at kontrollere de sikkerhedsmæssige tiltag. Denne kontrol af de sikkerhedsmæssige foranstaltninger skal derfor i høj grad foretages på basis af dokumentation fra leverandøren i form af eksempelvis certificeringer, revisionsrapporter og sikkerhedslogs samt relevant dokumentation fra en uafhængig tredjepart. Ingen af disse dokumentationstyper kan som udgangspunkt stå alene, og man bør derfor nøje overveje, hvilke typer dokumentation, der sammenlagt vil kunne udgøre et tilfredsstillende grundlag for kontrol.
Valget af cloudservices som løsningsalternativ bør derfor træffes på baggrund af nuancerede overvejelser, som også inkluderer overvejelser om egen og cloudløsningens risikoprofiler.

Sikkerhedsmæssigt kan der være stor forskel på, om man som kunde vælger en cloudløsning baseret på en standardløsning, eller man vælger en cloudløsning, der kan tilpasses forretningens individuelle sikkerhedskrav. Begge løsninger stiller store, men forskellige, krav til kunden, idet man i den ene situation får en løsning, hvor man selv skal varetage alle de sikkerhedsaspekter, der ligger uden for standardaftalen, mens man i den anden skal være sikker på, at man får stillet de rette sikkerhedskrav til leverandøren. Begge løsninger kræver dog, at man som kunde har fastlagt sine sikkerhedskrav, og at man efterfølgende løbende sikrer, at leverandøren leverer det aftalte.

Fokus i dette kapitel er primært på de elementer, der ikke er dækket i det juridiske kapitel og de elementer, der er særlige for cloudservices. Traditionelle sikkerhedsdiscipliner skal stadig håndteres gennem virksomhedens generelle styring af informationssikkerheden. En organisation skal, uanset om der anvendes cloudservices eller ej, altid udarbejde risikovurderinger, beredskabsplaner og sikkerhedspolitikker, overveje behovet for undervisning af medarbejderne, have en hensigtsmæssig exit-strategi, osv. For generel vejledning om informationssikkerhed henvises til www.sikkerdigital.dk, hvor blandt andet vejledningen fra Center for Cybersikkerhed og Digitaliseringsstyrelsen om "*Informationssikkerhed i leverandørforhold*" (2019) kan findes.[14]

5.1 Risikovurdering af cloudløsningen

Risikovurderingen er et centralt værktøj til at få kortlagt de sikkerhedsmæssige risici, som anvendelsen af en hvilken som helst it-løsning medfører, uanset om løsningen anvender cloudservices eller ej. Når der behandles personoplysninger, skal risikovurderingen behandle risici for de registreredes rettigheder. Da risikovurderingen også er afgørende for, hvilke foranstaltninger man konkret skal stille krav om, skal risikovurderingen udarbejdes, inden en løsning udvikles og tages i brug, ligesom den bør revideres jævnligt. Relevante sikkerhedsmæssige aspekter skal således behandles for alle faser af en aftale (behovsafklaring, anskaffelse, drift, ophør eller skift), uanset om der er tale om en traditionelt serverbaseret løsning eller en, der omfatter cloudbaserede services.

Gennem risikovurderingen identificeres og vurderes mulige trusler, sårbarheder og konsekvenser ved brud på systemer og datas fortrolighed, integritet og tilgængelighed. I arbejdet med risikohåndteringen kan det være en fordel at skele til specifikke leverandørers løsninger med henblik på at identificere mulige risikonedbringende tiltag. Eksempelvis tilbyder nogle leverandører automatiske sårbarhedsscanninger, kryptering af data, herunder ved anvendelse af tredjepart, eller at driften af en given løsning "låses" til specifikke områder inden for eksempelvis EU. Sådanne tiltag kan generelt være hensigtsmæssige til at imødegå risici. Vælger man at låse sine data eller sin løsning til specifikke geografiske områder, skal man blot være opmærksom på, om det har konsekvens for driftsstabiliteten og fleksibiliteten af den tilbudte løsning eksempelvis i en krisesituation. Samtidig er en sådan låsning ikke nødvendigvis en garanti for, at delmængder af ens data ikke overføres til tredjelande i forbindelse med fx "follow the sun-support" eller anvendelsen af specifikke services.

Der kan findes inspiration og relevant viden om risikovurderinger på www.sikkerdigital.dk, i Datatilsynet og Rådet for Digital Sikkerheds "*Vejledende tekst om risikovurderinger*" (juni 2019),[15] samt i ISO-standarderne 27001, 27002, 27017,

---

[14] Center for Cybersikkerhed og Digitaliseringsstyrelsen, 2019, "Informationssikkerhed i leverandørforhold".
[15] Datatilsynet og Rådet for Digital Sikkerhed, juni 2019, "*Vejledende tekst om risikovurderinger*".

27018 og 27701.

På baggrund af den samlede risikovurdering skal man vurdere, hvorledes identificerede risici kan og skal håndteres i samspil med de øvrige krav, der er til den planlagte løsning.[16]

5.2 Behandlingssikkerhed

Ved anvendelse af cloudservices overlades behandlingen af data på en række områder til cloudleverandøren, og det påvirker risikoprofilen for såvel løsningen som behandlingen af data.

Såfremt der behandles personoplysninger, er det efter databeskyttelsesforordningen et krav (jf. artikel 32), at den dataansvarlige og databehandleren af hensyn til at opretholde sikkerheden og hindre behandling i strid med databeskyttelsesreglerne, skal gennemføre tekniske og organisatoriske foranstaltninger for at sikre et *passende* sikkerhedsniveau. Der er ikke nogle udtømmende, objektive kriterier for, hvad et passende niveau er. Fastlæggelse af sikkerhedsniveauet forudsætter en konkret risikovurdering, som tager højde for risiciene for fysiske personers rettigheder og frihedsrettigheder. Se nærmere herom i kapitel 5.1 om risikovurderinger og hvilke tiltag, det kan være særligt relevant at stille krav om. Det er altså en forudsætning for at opnå den efter forordningen tilstræbte databeskyttelse, at den dataansvarlige stiller krav til sikkerhedsniveauet, som modsvarer de risici, der er ved en given behandling af personoplysninger.

For en nærmere gennemgang af reglerne om behandlingssikkerhed, henvises der til vejledningen "*Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger*",[17] som ligeledes indeholder en række eksempler på tekniske og organisatoriske foranstaltninger til tilvejebringelse af et passende sikkerhedsniveau. Se også kapitel 5. Sikkerhed for nærmere oplysninger, samt Datatilsynet og Rådet for Digital Sikkerheds "*Vejledende tekst om risikovurderinger*" (juni 2019).[18]

5.3 Sikkerhed under behovsafklaringen

I forbindelse med afklaringen af ens behov sættes rammerne for hele det fremtidige arbejde med anskaffelse og drift af en løsning. For at få optimalt samspil imellem forretningsbehov og sikkerhedsbehov, er det afgørende, at sikkerhedsbehovene indgår tidligt i denne proces, frem for at blive forsøgt indarbejdet senere hen. Man skal derfor, jf. databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og standardindstillinger, identificere de risici, som skal håndteres i samspil med de øvrige krav til den planlagte løsning samt mulige designmæssige tiltag til at sikre databeskyttelse.

---

[16] Der henvises endvidere til publikationen *Cloudservices Computing Risk Assessment* fra ENISA: https://www.enisa.europa.eu/publications/cloudcomputing-risk-assessment.

[17] Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen, juni 2018, "*Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger*".

[18] Datatilsynet og Rådet for Digital Sikkerhed, juni 2019, "*Vejledende tekst om risikovurderinger*".

Her vil it-arkitektur være vigtig. Mange sikkerhedsmæssige aspekter kan styres bedre med den rette it- og sikkerhedsarkitektur, eksempelvis gennem brugen af centralt placerede adgangspunkter, der via VPN-forbindelser er eneste vej ind i cloudløsningen. Hermed kan autentifikationen af brugerne holdes in-house, og man undgår dermed at have potentielt følsomme brugeroplysninger liggende eksternt. Et andet eksempel er anvendelse af kryptering af de informationer og data, der indgår i den planlagte cloudløsning. Dette ses ofte som en umiddelbar og oplagt mulighed for at beskytte fortroligheden, men anvendelse af kryptering skal gennemtænkes således, at løsningen stemmer overens med behovene for fortrolighed samt evnen til at administrere løsningen, herunder administrationen af krypteringsnøgler. I tillæg hertil skal man være opmærksom på, at behandling af data typisk vil kræve, at data dekrypteres. Det kan derfor være relevant at overveje, om man har behov for adgang til loginformation om tilgang til data.

5.4 Sikkerhed i forbindelse med anskaffelsen

Før man træffer endeligt valg af leverandør, er der en række sikkerhedsforhold, der skal undersøges, herunder:

- Leverandørens evne til at leve op til de stillede sikkerhedskrav
- Leverandørens valg af teknologisk løsning – kan have indflydelse på kundens risikovurdering
- Leverandørens generelle modenhed med hensyn til sikkerhed

For cloudløsninger, der tilbydes af internationale leverandører, kan det være svært at påvirke leverandørens sikkerhedsmæssige profil. Det skyldes, at leverandørens sikkerhedsprofil ofte er globalt defineret og udbydes som en standardiseret service, som netop er tilpasset med henblik på optimering af ydelse i forhold til pris mv. Dette kan selvsagt også betyde, at der er et endog meget højt sikkerhedsniveau i løsningen. Ofte vil der desuden være mulighed for at tilkøbe yderligere sikkerhedsrelaterede ydelser, eksempelvis særskilte audits, yderligere adgang til loginformation, automatiske adviseringer om hændelser og begrænsninger på oversendelsen af oplysninger til specifikke geografiske lokationer.

Med udgangspunkt i ens sikkerhedskrav vurderer man potentielle cloudleverandørers sikkerhedsservice og sammenholder med den tilsvarende sikkerheds-, risiko- og omkostningsprofil for en traditionel serverbaseret løsning. Man har derved mulighed for på forhånd at vurdere, hvilken type løsning, der bedst dækker ens behov, og i givet fald hvordan eventuelle kompenserende foranstaltninger til denne løsning skal etableres, samt hvorledes dette vil påvirke økonomien for den samlede løsning.

Det skal her bemærkes, at uanset hvor og hvordan en løsning anskaffes og om denne anvender cloudløsninger eller on-premise servere, er det, jf. kapitel 4 om jura, altid myndighedens ansvar at sikre, at de informationer og data, der indgår i løsningen, er tilstrækkeligt beskyttet.

Til arbejdet med at definere de tekniske og sikkerhedsmæssige krav kan der hentes inspiration og hjælp i Digitaliseringsstyrelsens klausuler til informationssikkerhed,[19] samt i Digitaliseringsstyrelsens kommende vejledning "*Minimumskrav for samfundskritiske it-systemer*". Vejledningen omhandler særligt it-sikkerheden og forsyningssikkerheden i outsourcede it-systemer og indeholder en beskrivelse af de minimumskrav, der skal indgå i myndigheders fremtidige kontrakter vedrørende outsourcede samfundskritiske it-systemer.

5.5 Sikkerhed under drift

Anvendelsen af cloudservices forudsætter ofte et samarbejde, hvor der aftales en tydelig fordeling af sikkerhedsrelaterede opgaver, hvor cloudleverandøren fokuserer på eksempelvis at sikre og dokumentere fysisk perimetersikkerhed, høj tilgængelighed og sikring af infrastrukturen mod uautoriseret indtrængen. Hertil kan uafhængige certificeringsorganer og revisorer sikre tilsyn med cloudleverandørens sikkerhedsleverancer, og den offentlige organisation kan opnå et mere solidt grundlag til at vurdere det samlede informationssikkerhedsniveau og derved opnå et solidt grundlag for at reagere effektivt på hændelser.

For at sikre, at den faktiske sikkerhed i løsningen lever op til ens krav i hele driftsperioden, bør man som kunde løbende monitorere leverandørens sikkerhedsmæssige leverancer. Dette kan enten ske på baggrund af de informationer, som indgår i den indgåede serviceaftale, eller på baggrund af informationer man selv tilser, bliver indsamlet.

Monitoreringen skal være med til at sikre, at de aftalte sikkerhedsydelser bliver leveret, men den kan også have til formål at identificere eventuelle forhold, der bør forbedres, hvis det viser sig, at ydelserne ikke lever op til det forventede. Dette er specielt vigtigt i de situationer, hvor der er tale om en standardservice, der ikke giver nogen mulighed for ændring. En metode til monitorering er gennemgang af de opsamlede sikkerheds-logs, som bl.a. kan bruges til at sikre, at man er i stand til at reagere fornuftig på eventuelle sikkerhedshændelser.

Derudover bør man som kunde være opmærksom på eksempelvis svartider på support, hastigheden hvormed leverandøren udruller sikkerhedsopdateringer og hastigheden hvormed leverandøren gennemfører serviceforespørgsler. Eksempelvis vil der ved anvendelse af en PaaS- eller SaaS-løsning skulle være opmærksomhed på leverandørens processer og regler for oprettelse og sletning af brugere eller gendannelse af backupdata, som alt sammen er vigtigt i en driftssituation. Henset til at en række af de seneste større cyberangreb har udnyttet svagheder i operativsystemer, der ikke længere opdateres, er det desuden afgørende, uanset om man anvender cloudløsninger eller on-premise servere, at man er opmærksom på, om de anvendte operativsystemer stadig supporteres med relevante

[19] Digitaliseringsstyrelsen, klausuler til informationssikkerhed.

sikkerhedsopdateringer, eller om ens leverandør har truffet andre foranstaltninger til at forhindre sikkerhedshændelser. Det er med andre ord vigtigt, at man som kunde er opmærksom på, at drift af en cloudbaseret løsning adskiller sig fra drift af en serverbaseret løsning og at man skal have de rette kompetencer og processer til at varetage sin valgte rolle i driftssituationen afhængig af den valgte service- og leverancemodel. Man kan ikke fraskrive sig ansvaret for sikkerheden i en cloudløsning, selv om man ikke selv varetager driften af løsningen. Se eventuelt kapitel 3.1 Organisering og kompetencebehov og kapitel 5.7 Håndtering af tvungne opdateringer for uddybning heraf.

5.6 Ophør eller skift i leverandørforhold

I forbindelse med ophør eller skift af kontraktforholdet er det vigtigt, at informationssikkerheden bevares i hele ophørsfasen, uanset om driften overdrages til en anden leverandør, ophører eller hjemtages.

For anvendelsen af cloudservices gælder især, at man skal være opmærksom på, om de angivne underleverandører er specifikke for kundens anvendelse af cloudservicen. Samtidig skal man være opmærksom på, om de varslingsfrister, cloudleverandører anvender ved skift af underleverandører, giver mulighed for at vurdere behov for tilpasninger af løsningen og eventuelt at gennemføre disse tilpasninger.

Man skal som kunde derfor have udarbejdet en exit-strategi, som bl.a. sikrer, at der er mulighed for at flytte forretningsapplikationer og eventuelle tilhørende styringssystemer, samt at få tilbageleveret data, såfremt dette er ønskeligt, jf. forretningsbehov. Man skal også være opmærksom på, hvad en aftale i givet fald dækker efter samarbejdet er ophørt, eksempelvis med hensyn til opretholdelse af tavshedspligt og sletning af data, herunder backup, hos såvel leverandører som underleverandører. Se også kapitel 3.4 om leverandørafhængighed for beskrivelse af arkitekturmæssig understøttelse af skift i leverandørforhold.

5.7 Håndtering af tvungne opdateringer

En særlig sikkerhedsmæssig udfordring i visse cloudmiljøer kan være håndteringen af tvungne opdateringer, dvs. opdateringer, der rulles ud til alle kunder hos en given cloudleverandør, uden at hver enkelt kunde har mulighed for at udskyde eller påvirke opdateringerne. I cloudmiljøer bliver der typisk notificeret om planlagte ændringer og opdateringer, men sikkerhedsopdateringer af kritisk karakter kan blive installeret med meget kort varsel. Det betyder, at kunden kan vide sig nogenlunde beskyttet mod sårbarheder. Det betyder dog også, at kunden skal være forberedt til at håndtere ændringer både hyppigere og på andre tidspunkter, end det måske ville være tilfældet i en traditionel serverbaseret løsning, hvor miljøet er mere isoleret, samt at kunden kan komme i en situation, hvor der ikke er mulighed for på forhånd at teste applikationerne for sådanne opdateringer.

Organisationen bør derfor have et beredskab, der kan sikre, at organisationen 1) kan vurdere om en opdatering udgør en potentiel risiko, 2) får testet sine systemer for sådanne opdateringer i god tid, inden de implementeres og 3) kan håndtere opdateringer, der gennemføres med meget kort eller intet varsel.

Samtidig bør der etableres processer, der sikrer, at systemer overvåges særlig tæt umiddelbart efter en opdatering – særligt i forbindelse med opdateringer, hvor organisationen ikke har haft mulighed for at foretage en forudgående test.

Det skal endvidere sikres, at internt uddannelsesmateriale, instruktioner mm. opdateres ved opdateringer og ændringer, særligt ifm. brugen af cloudbaserede fagsystemer.

I forbindelse med de tvungne opdateringer skal organisationen være opmærksom på afledte effekter for andre systemer, som det aktuelle system er integreret med. En ændring i ét system, som konsekvens af en opdatering, kan have konsekvenser for andre systemer.

5.8 Uddannelse

Som led i arbejdet med cloudservices er det vigtigt, at både it-specialister og øvrige ansatte, så som juridiske og økonomiske ressourcer, kvalificeres til at kunne tage stilling til anvendelsen af cloudservices. Uddannelse bidrager til at løfte niveauet for sikkerhed ved at skabe et grundlæggende kendskab til en række tekniske aspekter, og de juridiske, sikkerhedsmæssige og økonomiske aspekter, der følger heraf. Det kan fx være i valg af service- og leverancemodeller, netværk og placering af data, brugen af indbyggede løsninger til samarbejde på tværs af brugere både inden for og uden for organisationen samt datadeling og dataudtræk.

Et særligt opmærksomhedspunkt ved cloudservices er risikoen for, at de cloudbaserede løsninger uforvarende eller bevidst anvendes på måder, der er muligt i systemerne, men som strider mod organisationens sikkerhedspolitik. Dette er en konsekvens af, at den offentlige organisation ikke har samme kontrol over præcis hvilken funktionalitet, der tilbydes i et givent system, og at der løbende kan tilbydes og udrulles ny funktionalitet, uden at myndigheden er forberedt herpå.

Organisationen bør derfor vurdere, hvilke uhensigtsmæssige brugsscenarier, der er mest sandsynlige og bør samtidig sikre, at det er kommunikeret klart og tydeligt, såvel til udviklere som slutbrugere, hvordan systemet må udvikles og anvendes. Undervisning og opmærksomhed om retningslinjer kan med fordel indgå både i specifikke aktiviteter vedrørende det enkelte system og i myndighedens mere generelle aktiviteter på sikkerhedsområdet.

Se eventuelt www.sikkerdigital.dk for yderligere information om sikkerhedspolitik og vejledning i uddannelse om sikkerhedspolitik.

5.9 Test og udvikling

Som tidligere nævnt er udviklingsafdelingerne ofte de første til at tage cloudløsninger i brug, fordi det giver en stor fleksibilitet ved såvel udvikling som test. Lige netop dette område indebærer imidlertid også en sikkerheds- og compliancerisiko, navnlig hvis organisationen arbejder med kopier af "ægte" data, der er dækket af fx databeskyttelsesbestemmelser. Man skal derfor sikre, at informationssikkerhedsforanstaltningerne svarer til de identificerede risici på hvert stadium af en udviklings- og testcyklus, herunder ved i videst muligt omfang at undgå at udvikling og test sker med kopier af ægte data. Selve systemets kode kan også være særligt følsomt, hvorfor en passende sikring mod uautoriseret adgang kan være et væsentligt krav.

Organisationen bør afdække de mulige risici gennem analyser i udviklingsorganisationen og håndtere dem ved hjælp af passende retningslinjer for opsætning og anvendelse af cloudservices i udviklingsorganisationen.

Opsummering

6. Opsummering

Anvendelsen af cloudservices kan på mange måder bidrage positivt til udviklingen og driften af løsninger i den offentlige sektor, og offentlige organisationer kan som udgangspunkt trygt anvende cloudløsninger på lige fod med andre typer løsninger.
Her opsummeres vejledningens centrale pointer, som bør gennemgås inden der træffes beslutning om anvendelse af en cloudløsning.

- Afklar forretningsmæssige behov og eventuelle organisatoriske implikationer af cloudbaseret drift og udvikling.
- Risikovurderingen skal fyldestgørende afspejle tekniske, sikkerhedsmæssige, økonomiske, processuelle, organisatoriske og kompetencemæssige risici. Herved skal den bl.a. sikre, at de sikkerhedsmæssige foranstaltninger afspejles i krav til cloudløsningen og muliggør en tilstrækkelig kontrol af, at leverandøren lever op til de aftalte krav. Er der tale om et samfundskritisk it-system, skal der tages højde for de kommende minimumskrav til disse.
- Hvis der skal indgå personoplysninger i cloudløsningen, er der nogle særlige forhold, man skal være opmærksom på, som følger af databeskyttelsesforordningen. Blandt andet skal en risikovurdering forholde sig til de risici, der kan være ved behandlingen af personoplysninger, og hvis risikoen for de registreredes rettigheder er høj, skal der udarbejdes en konsekvensanalyse.
- Hvis der indgår personoplysninger i cloudløsningen, skal de registreredes rettigheder sikres, herunder ved databeskyttelse gennem design. Herudover skal det vurderes, om aktiviteterne evt. vil blive omfattet af lokationskravet, hvilket vil sige, at opbevaring af hensyn til statens sikkerhed skal ske på servere i Danmark.
- Hvis der indgår personoplysninger i cloudløsningen, skal der indgås en databehandleraftale, gerne en standardaftale, der regulerer databehandlerforholdet, herunder indeholder vilkår om bl.a. instruks, tilsyn, revisionserklæring, overførsel til tredjelande, behandlingsgrundlag samt tilbagelevering og sletning af data ved aftalens ophør.

Man kan med fordel finde inspiration i ISO 27701-standarden til at kortlægge sammenhænge mellem bestemmelser i databeskyttelsesforordningen og informationssikkerhed. Man kan ligeledes overveje at stille krav om, at cloudleverandøren benytter standarderne ISO 27001 og 27002, samt 27017 og 27018, der vedrører sikkerheden ved behandlingen af personoplysninger i cloudløsninger.

Hvis ovenstående punkter er afklaret, og leverandøren kan dokumentere efterlevelse af relevante standarder, kan man generelt have tillid til, at informationssikkerheden er tilfredsstillende, og at behandlingen af personoplysninger sker i overensstemmelse med relevant lovgivning.

Vejledningen er udarbejdet af Digitaliseringsstyrelsen og Center for Cybersikkerhed

digst.dk