DATATILSYNET

7. september 2021

J.nr. 2021-09-0091
Dok.nr. 388692
AFR

UDKAST

Brødtekst til vejledning om cloud høringsversion.

1. Indledning

Databeskyttelsesforordningen og databeskyttelsesloven er teknologineutral. Det vil sige, at reglerne ikke fortæller noget om hvilken type software, infrastruktur eller sikkerhedsmodel, der vil være det rigtige at bruge. Denne valgfrihed er en styrke for den enkelte dataansvarlige forretning, der frit kan vælge både den forretningsmodel og teknologi de mener bedst egnet til at løse opgaven. Det kan samtidigt opleves som om, at der mangler konkrete ja og nej svar, på hvorvidt en given løsning, lovligt kan rummes inden for databeskyttelsesreglernes rammer. Et af de teknologiområder hvor dette giver anledning til de fleste spørgsmål, har i mange år været brugen af det der bredt kaldes cloud. En af årsagerne er, at disse cloudservices over tid, er blevet meget udbredte i markedet og, at det på mange forretningsområder er den primært benyttede form for IT leverancemodel.
Denne vejledning prøver at sætte fokus på de databeskyttelsesretlige overvejelser, en dataansvarlig eller databehandler skal foretage i forhold til brugen af cloudservices. Det er dog vigtigt at fastslå, at mange af de belyste emner med lige så stor ret gør sig gældende ved de fleste andre leverancemodeller for it-ydelser og services.
Denne vejledning indeholder dele af flere allerede offentliggjorte vejledninger, særligt de 2 vejledninger fra 2021 om overførsel til 3. lande og

Med andre ord, cloud introducerer ikke andre eller nye problemstillinger i forhold til databeskyttelsesreglerne, end andre leverancemodeller. Derimod tilsiger forholdets natur ved den måde cloudservices leveres på, dog at særlige områder af de databeskyttelsesretlige regler, kommer mere i fokus end andre. Særligt forhold der udspringer af databehandlerkonstruktionerne og databeskyttelsesforordningens kapitel 5, om overførsler til 3. lande, er i fokus.
Denne vejledning søger ikke at tilføje nyt i definitionen af cloudservices og forholder sig ikke til de forretningsmæssige incitamenter, eller mangel på samme, ved brugen heraf. En gennemgang af disse sider ved brugen af cloudservices kan findes i Digitaliseringsstyrelsens "vejleding i brugen af cloudservices" version 1.1 fra 2020.

2. Hvad er cloud?

Helt overordnet bliver begrebet "cloud" brugt om en model til at tilvejebringe standardiserede IT ressourcer, typisk på større decentrale samlinger af computere, der leveres som en service eller samlinger af services, ofte til en flerhed af aftagere. Men også brugen af forskellige enkeltservices, hvor der i et interface forespørges med et sæt af parametre for at udføre en forretningsmæssig behandling på oplysningerne bliver typisk leveret i cloud.

”Cloudservices” er en fællesbetegnelse for en bred vifte af forskellige services. Disse varierer i indhold, fleksibilitet og ansvarsfordeling imellem leverandøren og aftageren af ydelserne. Cloud løsninger kan derfor være dybt specialiserede og skræddersyede til den enkelt virksomhed, men også være helt standardiserede produkter eller enkeltservices som mange aftagere benytter.
Med andre ord, cloud kan antage alle former og hybrider, i såvel leverancens omfang som de forskellige aktørers fordeling af opgaveløsning og ansvar forbundet hermed. De mere komplekse dataretlige problemstillinger, kan ofte relateres til den fragmentering af klarhed og oplysninger, som skyldes at helhedsbilledet for behandlingerne er opdelt på flere aktører, alle med hvert sit løsningsfokus og aftalegrundlag.
Typisk har aftagere af cloud ydelser, en opfattelse 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 (f.eks. kontinent, land eller datacenter). Eksempler på ressourcer kan være grundlæggende lagring, processorkraft, hukommelse og netværkstopografi og båndbredde.
Cloud servicemodellerne beskriver typisk indholdet af den ressource, man anvender, og hedder ofte noget med ”xx som en service”.

- Infrastruktur som en service (IaaS). IaaS er den mest basale af de tre servicemodeller. Med IaaS køber anvenderen alene adgang til ren 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 over og ansvar for etablering, sikring og drift af driftsmiljøet, herunder operativsystemer, netværk og lagring af data, forud for de implementerede forretningsapplikationer.

- Platform som en service (PaaS). 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 indkøbte applikationer. Anvenderen har typisk kontrol med og ansvar for de implementerede applikationer og ofte også de tilhørende konfigurationsindstillinger for applikationens driftsmiljø. Kontrol med og ansvar for den underliggende cloudinfrastruktur og operativsystemer overlades normalt til leverandøren. PaaS vil typisk dække hovedparten af de mest gængse behov og herudover kan platformen indeholde standardværktøjer til også avancerede funktioner, f.eks. algoritmer til big data analyse, kunstig intelligens og AI chatbots. Anvenderen kan vil typisk benytte egne applikationer i samspil med de services, der indgår i platformen. Fordi leverandøren udpeger og har ansvar for vedligehold af operativsystemer og services på infrastrukturen, vil anvenderen typisk ikke have udviklings- og driftsansvar andet end for egne forretningsapplikationer.

- Software som en service (SaaS). 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. Leverandøren har typisk det fulde ansvar for drift og vedligehold af den samlede løsning. Anvenderen har få eller ingen muligheder for selv at tilpasse produktet. Dette er særligt vigtigt at være opmærksom på, hvis SaaS-løsningen skal integreres i et miljø af eksisterende systemer, da tilpasninger af en SaaS-løsning kan være vanskeligt. I SaaS har leverandøren ansvar for drift og vedligehold af løsningen.

Databeskyttelsesretligt vil valg af servicemodel typisk påvirke den databehandlerkonstruktion der ligger i servicen. Forstået på den måde, at jo mere ansvaret overgives til leverandøren, des mere skal den dataansvarlige være sikker på, at de standardiserede ydelser giver den fornødne behandlingssikkerhed, styring af change management, overblik over hele leverancekæden og datas bevægelser i denne.

De enkelte services kan leveres på flere forskellige metoder, der afspejler fra hvilke fysiske servere og netværk ydelsen leveres fra og i hvilken grad disse ressourcer deles med andre anvendere. De typisk anvendte modeller er kaldt privat-, fælles-, offentlig- og hybrid cloud.

- 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.

- Fælles (shared) 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. 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 (public) cloudservice. Cloudservicen udbydes typisk på generelle 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 eller 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 styring. 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.
Markedet for cloudservices, navnlig IaaS og PaaS-services, har i en årrække været domineret af få, globale spillere. 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. Ligesom markedet for SaaS løsninger er meget bredt med mange typer hyppigt brugte standardiserede løsninger, der rangerer fra totale CRM og CMS løsninger til specifikke services som f.eks. billedbehandling, bookingsystemer og fødereret PKI funktionalitet bare få at nævne nogle få.

Flere databeskyttelsesretlige problemstillinger, der opstår spørgsmål om i cloudleverancer f.eks. overførsler til 3. lande, samt ansvarlighed og dokumentation af databeskyttelsesforordningens overholdelse og kontrol med databehandlere, hænger ofte sammen med aspekter der opstår i behandlingssituationer hvor det ikke er gennemsigtigt hvordan servicen leveres i sin helhed, eller hvor standardkontraktsbestemmelser ikke kan ændres, sådan at aftalen afspejler en dataansvarligs individuelle krav.

3. Databeskyttelsesretlige opmærksomhedspunkter.

Som sagt i indledningen er databeskyttelsesforordningen teknologineutral. Datatilsynet kan både se de forretningsmæssige fordele ved cloudydelser og mulighederne i det store udbud af services, der kan tilgodese en flerhed af forretningsmæssige behov hos mange dataansvarlige. Herudover har Datatilsynet forståelse for den udvikling der er sket i markedet, der gør at mange services næsten udelukkende kan leveres som en cloudydelse.
Det er dog relevant, at påpege, at disse mere kommercielle hensyn på ingen måde må føre til, at reglerne om databeskyttelse ikke kan overholdes.
Hvilke opmærksomhedspunkter er så de vigtige når det kommer til cloudydelser.

Kend dine services.

Som dataansvarlig er det nødvendigt, at vide hvad der sker med de persondata der behandles, i hele den kæde af databehandlere der er.
Forståelsen for denne forudsætning skal ses i lyset af blandt andet følgende regler, databeskyttelses forordningens artikel 5, stk. 2, 24, 25, 32 og 28, samt reglerne i kapitel 5.
Hovedprincippet om ansvarlighed og evnen til at kunne dokumentere dette efter databeskyttelsesforordningens artikel 5, stk. 2 og 24, er en væsentlig bestanddel af databeskyttelsen.
Det betyder at du som dataansvarlig skal kunne dokumentere overholdelse af hele forordningen og ikke kun dennes principper. Dokumentationen skal afspejle de overvejelser og valg du har foretaget i databeskyttelsesretlig henseende, herudover er det en væsentlig datakilde til at påvise over for Datatilsynet, at du på relevante tidspunkter – i forhold til behandlingen – har vurderet risikoen for de registreredes rettighedes rettigheder, og truffet de fornødne forholdsregler til at beskytte disse.
Det er helt ok, og ganske normalt forekommende, at en cloudleverance bliver leveret gennem flere databehandlere. Selvom dette er tilfældet skal den dataansvarlige sikre sig og kunne dokumentere, at databehandlerkonstruktionen i sin helhed sikrer overoverholdelse af databeskyttelsesreglerne.
Dette kan forekomme uoverskueligt for den enkelte dataansvarlige, men det er ikke desto mindre den grundlæggende hovedregel, at man som dataansvarlig ikke foretager behandlinger af persondata, på en måde man ikke har en sådan grad af kontrol over, at man kan sikre hele databeskyttelsesforordningens overholdelse.
Den væsentlige kortlægning af de behandlinger, der skal foretages ved brug af services fra en cloudleverandør, bør man kunne få svar på fra leverandøren. Denne bør relativt let kunne give svar på følgende:

- Kunne give en gennemgang af hvordan behandlinger bliver udført.
- Give en redegørelse for hvilke services hos underleverandører der benyttes og hvem disse underleverandører er.
- Redegøre for hvordan sikkerheden er for hele leverancen (hvordan er persondata beskyttet i og under behandlingerne), dette er særligt væsentligt at vurdere op imod den sikkerhed den dataansvarlige selv har fundet fornøden for behandlingen.
- Kunne redgøre for, af hvem og hvorfra de behandlede personoplysninger kan blive tilgået også selvom dette kun er i sjældne komplicerede fejlsøgnings og service/support tilfælde.
- Kunne redegøre for hvilke metadata og andre styringsdata, der eventuelt også behandles. (så det kan dokumenteres, om disse er persondata eller ej)
- Kunne oplyse om hvor behandlingerne foregår, herunder om persondata overføres og behandles i 3. lande (lande uden for EU/EØS).

Herudover, er det væsentlig, at de aftalevilkår man kan få med sin leverandør er så klare og overskuelige, at den dataansvarlige til stadighed er i kontrol over formålet og midlerne for behandlingen. Der må derfor ikke på baggrund i kontrakten kunne ske en underminering af de registreredes rettigheder, eller ændring af leverancen, uden at den dataansvarlige kan siges at være i fuld kontrol herover.

Databehandlerkonstruktionen.

Det følger af databeskyttelsesforordningens artikel 28, stk. 1, at en databehandler alene må benytte en databehandler der kan stille de fornødne garantier for, at denne overholder forordningens regler.

Databehandleren skal herudover (i forhold til de behandlede persondata) alene agere i overensstemmelse med den instruks, der er givet fra den dataansvarlige.

Hvis der foreligger en databehandlerkonstruktion skal der udarbejdes en databehandleraftale.

Databehandleraftalen skal indgås mellem den dataansvarlige og databehandleren, og skal leve op til kravene til databehandleraftaler i databeskyttelsesforordningen særligt indholdet i artikel 28, stk. 3. Det indebærer, at der skal være tale om en kontrakt eller andet retligt dokument, som er bindende for databehandleren. Det er desuden et krav, at databehandleraftalen er skriftlig, dette kan være i elektronisk form.

Databeskyttelsesforordningens artikel 28, stk. 3, fastsætter herudover en del specifikke krav til indholdet af den databehandleraftale, som skal indgås med databehandleren. Aftalen skal bl.a. indeholde oplysninger om genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger, kategorierne af registrerede og dine forpligtelser og rettigheder som dataansvarlig samt de pligter, som databehandleren har i forhold til at varetage opgaven

For en uddybning heraf henvises til Datatilsynets vejledning om dataansvarlige og databehandlere (henvisning) samt den af EDPB godkendte standarddatabehandleraftale med tilhørende vejledning, og reglerne i databeskyttelsesforordningens artikel 28, stk. 3, litra a-h.

Udgangspunktet for databehandlerens brug af andre databehandlere er, at dette kun må ske hvis den dataansvarlige enten har givet lov til, at der alene må benyttes en række nævnte (specifikke) databehandlere, eller der generelt er givet tilladelse til brug af andre databehandlere (også kaldet underdatabehandlere). Det sidste kan kun ske såfremt databehandleren underetter den dataansvarlige, før der sker ændringer og udskiftning i kredsen af underdatabehandlere. Dette er et udtryk for, at den ”kontrol” den dataansvarlige skal være i, i forhold til hvordan persondata bliver behandlet i hele kæden af databehandlere.

Herudover er det vigtigt at notere sig, at reglen i artikel 28, stk. 4, ikke kan føre til, at en dataansvarlig, bare kan stille sig tilfreds med kun at fokusere på den første databehandlers behandlinger, men stadigvæk skal kende behandlingernes vej og sikkerhed i hele behandlingskæden.

Kontrol med databehandlere.

Generelt kan man sige, at jo mere der kan gå galt ved behandlingen hos databehandleren (stor risiko), jo større krav stilles der til dit tilsyn med databehandleren. Her skal du være opmærksom på, at når det handler om databeskyttelse, er det ikke risikoen for, at du (som virksomhed eller som myndighed) kommer galt afsted. Det er derimod risikoen for de registrerede, fx medarbejderne, kunderne og borgerne, man skal have for øje. Hvor sandsynligt er det, at noget går galt, og hvad er konsekvenserne, hvis det rent faktisk går galt.

Som tommelfingerregel kan du regne med, at kravene til tilsynet med databehandlere stiger i takt med:

- At databehandleren behandler **flere** personoplysninger
- At oplysninger får en mere **fortrolig** eller **følsom** karakter
- At behandlingen bliver mere **indgribende**

I Datatilsynets vejledning, fra efteråret 2021, om tilsyn med databehandlere (henvisning) er der fastsat en trinvis model man kan benytte som inspiration.
Som eksempler på de mere indgribende behandlinger kan nævnes:
Behandling af oplysninger om fx lokationsdata med henblik på at kortlægge eller følge personers adfærd Systematisk overvågning af personer med henblik på at kontrollere dem
Profilering, hvor fx relativt harmløse oplysninger anvendes til at give meget præcise oplysninger om personers (aktuelle eller fremtidige) behov, adfærd eller personlighed
Afgørelser, der alene er baseret på automatisk behandling, herunder profilering, og som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende
Samkøring af datasæt med henblik på at tilvejebringe nye oplysninger, som ligger ud over, hvad de registrerede personer med rimelighed kan forvente
Behandling af oplysninger om sårbare personer, som vil have svært ved at varetage egne interesser, fx børn, ældre, psykisk syge, patienter, asylansøgere samt personer, hvor der er en ubalance i forholdet mellem den dataansvarlige og den registrerede person.
Der er til en vis grad sammenfald med, hvornår man skal foretage en konsekvensanalyse.
Du kan derfor også skæve til Datatilsynets liste over behandlingstyper, der er underlagt kravet om konsekvensanalyse.
For en gennemgang af hvad et tilsyn kan indeholde, er der gode eksempler hertil i vejledningens kapitel 5.
Jo mere kritisk behandlingen er for de registrerede (de personer som oplysningerne omhandler), jo mere intensiv kontrol skal den dataansvarlige føre med databehandleren. I nogle tilfælde kan det således være nødvendigt at påse behandlingssikkerheden hos databehandlerne årligt. Ligesom det – alt efter omstændighederne – kan være tilstrækkeligt, hvis risikoen er lav at påse behandlingssikkerheden med en lavere frekvens.
Det er vigtigt i denne forbindelse at forstå, at "databehandlere" også omfatter underdatabehandlere (leverandører) til databehandleren.
Eksempler på elementer der taler for en høj frekvens:

- Databehandleren har haft problemer med at overholde aftaler (ikke bare databehandleraftalen).
- Databehandleren har oplevet flere alvorlige sikkerhedsbrud, herunder brud på persondatasikkerheden.

Dette kræver naturligvis, at du som dataansvarlig bliver informeret om dette, men i nogle tilfælde vil du opdage det, f.eks. fordi bruddet afbryder den service, du får som kunde, og derfor er det måske nødvendigt at forlange en forklaring for afbrydelsen af en service. Dermed kan databehandleren ikke skjule årsagen eller alvoren af et brud.
Når det kommer til brud på persondatasikkerheden[1], er det et lovkrav, at databehandleren informerer dig om disse, uden unødig forsinkelse.

- Der skiftes ofte underdatabehandler.
- Der sker ofte ejerskifte, opkøb, fusion eller gennemgribende ændringer i strategien hos databehandleren.

Den slags vil man ofte bemærke som kunde. Ejerskifte/fusion kan umiddelbart fremstå ligegyldigt, når databehandleraftalen stadig gælder, men den slags kan ændre markant på et firmas strategi og dermed ændrede prioriteringer, der påvirker behandlingssikkerheden. Ejerskifte kan også medføre, at der i skifteprocessen tabes fokus på beskyttelsen af visse dele af it-miljøet, både i forhold til administrationen af miljøet og den fysiske flytning, udskiftning eller kassering.
Eksempler på elementer der kan indikere et behov for et ekstra tilsyn uden for den normale frekvens:

[1] Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet – altså de personoplysninger databehandleren behandler på dine vegne.

Ejerskifte, opkøb, fusion eller gennemgribende ændringer i strategien hos databehandleren.
En pandemi ændrer på den måde der arbejdes på, og tilgangen til personoplysninger (flere hjemmearbejdspladser).
Eksempler på elementer der taler for en lav frekvens:
Lang tids erfaring med databehandlere (databehandler og underdatabehandlere) viser en stabil service, og ingen eller få ikke-alvorlige sikkerhedsbrud.

Overførsler til 3. lande.

Det er ikke forbudt, at den cloudservice der benyttes, overfører og behandler persondata til et eller flere 3. lande. Det er her dog væsentligt, at alle databeskyttelsesretlige regler overholdes, men det er her særligt databeskyttelsesforordningens kapitel 5, der kommer i spil.
Datatilsynet har i sommeren 2021 udgivet en ny revideret vejledning om overførsler til 3. lande (henvisning), som gennemgår emnet mere i dybden.
For cloudservices er det særligt den kortlægning af hvor persondata behandles, som blev behandlet ovenfor under punktet ”kend dine services”, der danner grundlag for vurderingen.
Hvis det i kortlægningen konstateres, at persondata bliver behandlet på udstyr fysisk placeret i 3. lande, eller bliver tilgået fra 3. lande, eller på anden vis ”overføres”, skal der ud over den indgåede databehandleraftale med instruks for databehandlerkonstruktioner, også foreligge et gyldigt overførselsgrundlag. Dette gælder for alle typer af behandlinger hvor databeskyttelsesforordningen finder anvendelse, altså også personoplysninger der benyttes i service og support funktioner eller data der overføres til afregning af eller til fejlsøgning på servicen. Dette gælder uanset om overførslen sker til en databehandler, en selvstændigt dataansvarlig eller andre modtagere herunder 3. mænd.
En overførsel kan herudover kun ske hvis det overførselsgrundlag der benyttes, eventuelt med tillæg af supplerende foranstaltninger, sikrer den registrerede en retsstilling, der er tilnærmelsesvis lige så god (”essentielt ækvivalent”) med beskyttelsen af rettigheder forordningen giver (altså inden for EU/EØS området).
Hvor reel anonymisering ikke er omfattet af databeskyttelsesforordningen, da det ikke er en personoplysning som defineret i artikel 4, nr. 1., er pseudonyme oplysninger stadigvæk fuldt ud omfattet af reglerne. Det skal derfor sikres, at der også for pseudonyme oplysninger skal foreligge et gyldigt overførselsgrundlag, ved overførsler til 3. lande.

Cloud og USA.

Hvis din cloudservice, der behandler personoplysninger, bliver leveret fra USA, kører på udstyr i USA, eller oplysninger på anden vis bliver behandlet i USA, f.eks. ved at service-support medarbejdere i USA har adgang til oplysningerne på servere uden for USA, er der tale om en overførsel til USA.
USA er et 3. land i databeskyttelsesforordningens forstand, dvs. forordningens kapitel 5, skal iagttages.
EU-Domstolen har senest ved den såkaldte Schremms2 afgørelse foretaget en vurdering af USA som modtagerland.
For en gennemgang af dommen og påvirkningen af muligheden for at overføre personoplysninger til USA, kan man læse Datatilsynets nyhed om Schremms2 dommen (henvisning), det Europæiske Databeskyttelsesråds vejledning 02/2020 om de 4 essentielle garantier (henvisning) og vejledning 01/2020 om supplerende foranstaltninger (henvisning).
Den korte version i forhold til cloudservices er som følger.
De behandlinger der sker i cloudservicen i USA vil oftest være omfattet af det, der i EDPBs vejledning om supplerende foranstaltninger kaldes ”problematisk lovgivning”.
EU-Domstolen slog fast, at flere navngivne USA regler, bl.a. gik videre end det der var nødvendigt i et demokratisk samfund, ikke havde den fornødne klarhed og ikke kunne prøves ved en reelt uafhængig instans, af den registrerede.
Langt de fleste udbydere af cloudservices i USA vil typisk være omfattet af bl.a. lovgivningen FISA Sec 702, da de er ”electronic communication service providers”.

Hvis de persondata der behandles, er oplysningerne om andre nationaliteter end USA statsborgere og disse personer opholder sig uden for USA's grænser, er oplysninger om dem typisk omfattet af FISA Sec. 702.
Det vil sige, at de potentielt er genstand for reglerne i lovgivningen, som var en af dem som EU-Domstolen fandt for indgribende.
Overførselsgrundlagene, standardkontrakter fra EU-Kommissionen og bindende virksomhedsregler kan ikke i sig selv kompensere for de mangler der er i dette konkrete retsgrundlag, primært fordi man ikke i kontrakten eller i virksomhedsreglerne, effektivt vil kunne forhindre den amerikanske stat i at anvende lovgivningen, eller i aftale tillægge den registrerede rettigheder over USA som stat.
Der er herefter skitseret 2 muligheder for, alligevel, at kunne overføre oplysninger til USA.

1. Undergive behandlingen nogle yderligere supplerende foranstaltninger, der i samspil med overførselsgrundlaget, samlet sikrer et essentielt ækvivalent beskyttelsesniveau.
2. Såfremt det objektivt kan godtgøres, at de persondata der behandles, reelt aldrig vil være genstand for en anmodning fra de myndigheder der kan indhente oplysninger.

De supplerende foranstaltninger findes gennemgået i EDPBs vejledning der er nævnt ovenfor, det er særligt vejledningens annex 2, og usescases, der gennemgår de forskellige scenarier. Det er usecase 1-5, der beskriver mulige tekniske foranstaltninger, der kan give den fornødne beskyttelse.
Herudover er der i Datatilsynets vejledning om overførsel til 3. lande, også eksempler der gennemgår typer af overførselsscenarier.
Det er ingen hemmelighed, at indholdet af disse usecases kun i begrænset omfang giver brugbare resultater i praktikkens verden, da services for at virke normalt, kræver at data skal foreligge i reel klar tekst.
Reelt er det kun er kryptering af data, pseudonymisering, samt behandlinger hvor data opsplittes til behandling i flere lande, der giver usecases hvor beskyttelsen i bestemte tilfælde kan anses som fornøden. Der er i dagens cloudscenarier ikke mange services der kan placeres brugbart i en af disse tekniske muligheder.
Den anden mulige vej til overførsel, er en dokumentation for, at de behandlede oplysninger ikke vil blive gjort til genstand for anmodninger under den problematiske lovgivning.
Det er vejledningens punkt 46 der beskriver fremgangsmåden og kvaliteten af den dokumentation der skal til. Den skal være: **Relevant** i forhold til overførslen og de data der behandles. Baseret på o**bjektiv information**, altså empirisk konstaterbart fakta ikke antagelser. **Troværdig** også i forhold til kilden den hidrører fra. **Verificibar** altså mulig at holde op imod og bekræfte ved brug af andre kilder. Hidrøre fra **tilgængelige eller offentlige kilder.**
Som dataansvarlig må du gerne inddrage dine databehandleres vurdering. Det er dog vigtigt at pointere, at vejledningens punkt 47 siger, at databehandlerens udsagn ikke kan stå alene, men skal være understøttet af andre kilder.
Det er Datatilsynets opfattelse, at denne undtagelse giver et reelt rum, også i praksis, for nogle typer af overførsler. Der vil være typer af persondata, der – objektivt dokumenterbart – ikke er efterretningsmæssige efterspurgte.

Behandlinger foretaget i EU/EØS af USA-baserede firmaer.

Det er ikke i sig selv diskvalificerende for en databehandler, at denne er underlagt lovgivning i ”moderlandet”, der kan kræve oplysninger udleveret fra datterselskaber og etableringer i EU/EØS.
Der henvises til eksempel 10, i Datatilsynets vejledning om overførsler til 3. lande.

Særligt om udlevering af personoplysninger efter anmodning fra myndigheder i tredjelande

En databehandler må kun behandle personoplysninger, herunder overføre oplysnin- gerne til tredjelande, i det omfang den dataansvarlige har givet instruktioner om det i databehandleraftalen, eller det er krævet ifølge EU-ret eller medlemsstaternes natio- nale ret.
Hvis en databehandler i EU/EØS også er etableret i et tredjeland, kan databehandle- ren dog i nogle tilfælde blive mødt af en anmodning fra myndighederne i et tredjeland om udlevering af personoplysninger, som databehandleren behandler for den dataan- svarlige.
Hvis databehandleren vælger at overføre personoplysninger til tredjelandet i strid med databehandleraftalen, vil der være tale om en utilsigtet overførsel, og det betyder, at databeskyttelsesforordningens regler om overførsel til tredjelande ikke finder anven- delse i forhold til den dataansvarlige.
Den dataansvarlige skal dog være opmærksom på en række forhold i den forbindelse:

- For det første må den dataansvarlige kun benytte databehandlere, som kan sikre tilstrækkelige garantier for, at databeskyttelsesforordningens regler bliver over-holdt. I den forbindelse bør den dataansvarlige anmode databehandleren om ty-deligt at tilkendegive, om denne er underlagt lovgivning i tredjelandet, som - på trods af den dataansvarliges instruks om det modsatte - pålægger databehandleren at udlevere personoplysninger, som befinder sig i EU/EØS, til tredjelandets myndigheder.
- For det andet skal den dataansvarlige sikre den nødvendige behandlingssikkerhed, herunder at databehandleren behandler personoplysningerne fortroligt og ikke gør dem tilgængelige for uvedkommende. Den dataansvarlige må i den forbindelse foretage en risikovurdering med henblik på at vurdere, hvilke tiltag der skal iværksættes for at sikre dette.
- For det tredje skal den dataansvarlige føre tilsyn med sin databehandler. Hvis den dataansvarlige bliver bekendt med, at databehandleren handler i strid med data-behandleraftalen ved at overføre personoplysninger til et tredjeland mod den da-taansvarliges instruks, skal den dataansvarlige straks gribe ind over for dette.

Det bemærkes i øvrigt, at hvis en databehandler handler i strid med databehandleraftalen ved at videregive personoplysninger til en myndighed i et tredjeland og dermed selv fastlægger formålene med og hjælpemidlerne til en behandling, vil denne anses for selvstændig dataansvarlig for den pågældende behandling.

Det er dog vigtigt, at alle behandlinger udføres i EU/EØS, det gælder også service/support adgange, behandling af metadataoplysninger (der måtte være personoplysninger) der benyttes til kapacitetsstyring og afregning samt de administrative adgange, der giver adgang til personoplysninger.
En potentiel kontrol kunne være en fast opfølgning på logoplysninger om adgange med administrative privilegier, holdt op i mod de adgange der er sanktioneret af den dataansvarlige selv. Når det er sagt, er det formentlig forbundet med noget besvær, 100 % effektivt at identificere en myndighedsadgang fra 3. landet.
Der er et sidste opmærksomhedspunkt, nemlig de tilfælde hvor databehandleren også behandler dele af personoplysningerne til egne formål og med egne midler. Her er den pågældende selv dataansvarlig for disse behandlinger. Det betyder, at den oprindelige dataansvarlige skal have hjemmel til videregivelse i artikel 6, stk. 1 og eventuelt også en undtagelse i art 9, stk. 2, eller andre relevante regler i databeskyttelsesloven, da videregivelsen ofte kan være uden for det oprindelige formål for behandlingen.