Vejledning om cloud

Marts 2022

DATATILSYNET

Indhold

1. Indledning

Databeskyttelsesreglerne er teknologineutrale. Reglerne fortæller ikke noget om, hvilken type software eller hvilken infrastruktur det er rigtigt at bruge til behandling af personoplysninger. Denne valgfrihed er en styrke for den enkelte organisation. Organisationen kan dermed frit vælge såvel den forretningsmodel som den teknologi, som organisationen selv vurderer er bedst egnet til at løse opgaven. Dette kan dog samtidig opleves som om, der mangler konkrete ja- eller nej-svar på, om – og i givet fald hvordan – en given løsning lovligt kan bruges inden for databeskyttelsesreglernes rammer.

En af de teknologier, der giver anledning til mange spørgsmål, har i flere år været brugen af cloud. Det skyldes bl.a., at cloudservices over tid er blevet meget udbredte i markedet, og at det på mange forretningsområder er den primært benyttede it-leverancemodel.

Denne vejledning henvender sig primært til organisationer, som gerne vil benytte en eller flere cloudservice(s), og forsøger at beskrive og bistå med de databeskyttelsesretlige overvejelser, du som den dataansvarlige skal foretage dig, når du påtænker at bruge cloudservice(s). Mange af de belyste emner gør sig dog med lige så stor ret også gældende for de fleste andre leverancemodeller for it-ydelser og services.

Datatilsynet forstår dog også, at en lang række cloudservices leveres som standardiserede ydelser, hvor den enkelte organisation som kunde som regel har begrænsede muligheder for at tilpasse den pågældende service til organisationens individuelle behov og krav. Dele af vejledningen henvender sig derfor samtidigt til cloudleverandører, der kan læse mere om, hvordan de kan levere ydelser i overensstemmelse med databeskyttelsesreglerne.

Vejledningen indeholder elementer fra flere andre vejledninger, som Datatilsynet har offentliggjort. Det gælder særligt Datatilsynets vejledning om overførsel af personoplysninger til tredjelande og Datatilsynets vejledning om tilsyn med databehandlere. Begge vejledninger er tilgængelige på Datatilsynets hjemmeside.

Derudover indeholder Det Europæiske Databeskyttelsesråds anbefalinger om supplerende foranstaltninger[1] og vejledningen om samspillet mellem databeskyttelsesforordningens artikel 3 og kapitel 5[2] også vejledning om forhold, der hyppigt skal vurderes ved brugen af cloud.

Cloud introducerer ikke andre eller nye problemstillinger i forhold til databeskyttelsesreglerne end andre leverancemodeller. Dog indebærer den måde, som cloudservices leveres på, at udvalgte databeskyttelsesretlige regler er særligt relevante. Det drejer sig bl.a. om (i) brugen af databehandlere og underdatabehandlere, (ii) behandlingssikkerhed, og (iii) overførsel af personoplysninger til tredjelande.

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 af cloudservices. En gennemgang heraf kan findes i Digitaliseringsstyrelsens "Vejleding i anvendelse af cloudservices".

1 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

2 EDPB's Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

2. Hvad er cloud?

Begrebet ”cloud” bruges overordnet om en model til at tilvejebringe standardiserede it-ressourcer, typisk på større decentrale samlinger af servere, der tilgås via internettet.

Cloud kan leveres som en service eller samlinger af services. Der kan være tale om en simpel service, der består i håndtering af konkrete forespørgsler med en eller flere givne parametre – med andre ord ”ren regnekraft” – eller mere komplicerede services i form af komplette applikationer.

Eksempel 1

Scenarie 1

Et forsikringsselskab ønsker at sammenlægge flere af sine forsikringsprodukter til ét samlet produkt. Med henblik på at fastsætte en passende forsikringspræmie for den samlede forsikring benytter forsikringsselskabet en cloudservice til at regne på en række datasæt, der stammer fra selskabets øvrige forsikringsprodukter, som skal sammenlægges.

Scenarie 2

En skakforening udgiver et nyhedsbrev. På skakforeningens webside kan medlemmerne eller andre interesserede indtaste deres e-mailadresse med henblik på at modtage foreningens nyhedsbrev. Nyhedsbrevene bliver håndteret via en cloudservice, som skakforeningen bruger. Cloudservicen med design, udgivelse og arkivering af nyhedsbrevene bliver afviklet på en server i USA og betjenes gennem et interface i en browser.

Scenarie 3

En kommune benytter et tekstbehandlingsprogram, hvor funktionaliteten skabes på en server i Irland og vises på brugernes skærme. Kommunen gemmer og opbevarer alle skabte dokumenter på kommunens egen server, men tekstbehandlingsprogrammet, herunder login, opsætninger, brug af orddeling, stavekontrol og al anden funktionalitet, afvikles på serveren i Irland.

”Cloudservices” er således en fællesbetegnelse for en bred vifte af forskellige services. Cloudservices kan både være dybt specialiserede services, der er skræddersyet til den enkelt organisation, og helt standardiserede produkter eller enkeltservices, der benyttes af mange kunder.

Cloud kan dermed antage mange former og hybrider i såvel leverancens omfang som cloudleverandørens og kundens opgave- og ansvarsfordeling. Det kan derfor ofte være vanskeligt at få et fuldstændigt overblik over den samlede leverancemodel, der bruges til levering af cloudservices. Eksempelvis kan aktørerne, der indgår i leverancemodellen, have hver sit eget løsningsfokus og aftalegrundlag. Dette er også oftest årsag til de komplekse databeskyttelsesretlige problemstillinger, der kan være forbundet med brug af cloud.

Det er bl.a. kendetegnende for cloudservices, at du som kunde alene har kontrol over typen og mængden af ressourcer, fx lagring, processorkraft og netværkstopografi, du ønsker leveret. Du har derimod generelt ikke kontrol over hvilke specifikke ressourcer, som cloudleverandøren tilvejebringer, eller hvor disse ressourcer tilvejebringes. Du kan typisk kun specificere eller afgrænse placeringen af en ressource på et højere niveau fx til et bestemt kontinent eller land.

Cloudservicemodellerne beskriver typisk indholdet af den ressource, du anvender, og betegnes ofte ”xx som en service” (”xx as a Service”).

Typer af cloud

Infrastruktur som en service (IaaS). IaaS er den mest basale af de tre servicemodeller. Med IaaS har kunden alene adgang til ren infrastruktur, hvilket vil sige grundlæggende ressourcer som processorkraft, lagring og netværk. For at udnytte infrastrukturen skal kunden selv installere og drive al software, såvel operativsystemer som applikationer. Kunden har dermed selv kontrol over og ansvar for etablering, sikring og drift af driftsmiljøet, herunder operativsystemer, netværk og lagring af data samt sine implementerede forretningsapplikationer.

Platform som en service (PaaS). Med PaaS har kunden adgang til en infrastruktur, som leverandøren servicerer, med blandt andet databaser, operativsystemer og centrale API'er. På infrastrukturen kan kunden implementere egenudviklede eller indkøbte applikationer. Kunden 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 infrastruktur og operativsystemer overlades normalt til leverandøren. PaaS kan også indeholde standardværktøjer til avancerede funktioner fx algoritmer til big data analyse, kunstig intelligens og AI chatbots. Kunden vil typisk benytte egne applikationer i samspil med de services, der indgår i platformen. Idet leverandøren udpeger og har ansvar for vedligehold af operativsystemer og services på infrastrukturen, vil kunden typisk ikke have udviklings- og driftsansvar for andet end egne forretningsapplikationer.

Software som en service (SaaS). Med SaaS har kunden 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. Kunden 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.

Valg af servicemodel påvirker naturligt de databeskyttelsesretlige vurderinger, du skal foretage i forbindelse med brugen af servicen. Jo flere opgaver, der overlades til cloudleverandøren, des mere skal du som den dataansvarlige sikre dig, at leverandøren varetager disse opgaver inden for rammerne af databeskyttelsesreglerne, herunder bl.a. at leverandøren sikrer den fornødne behandlingssikkerhed og den fornødne leverandørstyring. Det er dig, der – inden en cloudleverandør kan benyttes – skal påse og dokumentere, at leverandøren kan stille de fornødne garantier for, at hele databeskyttelsesforordningen overholdes ved de behandlinger, der foretages hos leverandøren.[3]

Cloudservices kan leveres på flere forskellige måder, der afspejler, hvilke fysiske servere og netværk ydelsen leveres fra, og i hvilken grad disse ressourcer deles med andre kunder. Leverancemodellerne kaldes privat, fælles, offentlig og hybrid cloud.

Typer af leverancemodeller

Privat cloud. Cloudservicen er til eksklusiv brug af og i 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.

3 Se databeskyttelsesforordningens artikel 28, stk. 1, og artikel 24.

Fælles (shared) cloud. 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. Samtidig vil governancestrukturerne (aftalerne og styringsmekanismerne) for en fælles cloudservice typisk give hver organisation større indflydelse på styring og udvikling, end det er tilfældet ved en mere generisk offentligt tilgængelig cloudservice.

Offentligt tilgængelig (public) cloud. Cloudservicen udbydes typisk på generelle kommercielle vilkår. Den kan ejes, forvaltes og drives af en virksomhed, en akademisk eller en 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.

Hybrid cloud. 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.

De forskellige service- og leverancemodeller adskiller sig altså væsentligt på indhold, ansvarsfordeling, sikkerhedsprofiler og teknisk kompleksitet for kunden samt krav til styring. Uanset disse forskelle i service- og leverancemodellerne kendetegnes "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.

Du skal som den dataansvarlige sikre dig, at der i hovedaftalen og i databehandleraftalen er taget stilling til og nedfældet alle de databeskyttelsesretlige forhold, som du vurderer er nødvendige at pålægge og kunne gøre gældende over for cloudleverandøren.

Eksempler på sådanne forhold kunne være:

- Særlige, foruddefinerede sikkerhedsforanstaltninger, fx særlige forhold omkring brugerstyring af privilegerede adgange og adgang til personoplysninger
- Brugen af underdatabehandlere, herunder i tredjelande
- Tilsyn med cloudleverandøren og underdatabehandlere
- Sikring og dokumentation af, at cloudleverandøren ikke behandler personoplysninger til andre formål

Eksempel 2

Et forsikringsselskab vil benytte en cloudservice til at håndtere service- og supportsager omkring selskabets produkter. Cloudleverandøren bruger et it-system til at dokumentere og håndtere henvendelserne. It-systemet afvikles på en server i Tyskland.

I forlængelse af behandlingen af personoplysninger i it-systemet, som forsikringsselskabet er dataansvarlig for, tilbyder cloudleverandøren en tillægsservice for it-support døgnet rundt. For at kunne levere denne tillægsservice benytter leverandøren en underdatabehandler i Indien. Personoplysningerne vil således i sjældne tilfælde kunne tilgås af en begrænset gruppe medarbejdere hos underdatabehandleren i Indien.

Forsikringsselskaber vurderer imidlertid, at oplysningerne ikke lovligt kan overføres til underdatabehandleren i Indien. På den baggrund fravælger selskaber den konkrete tillægsservice.

Eksemplet illustrerer, at der kan være forhold omkring leverancemodellen, fx ved service og support, som også skal vurderes databeskyttelsesretligt. Det er ikke altid tilstrækkeligt kun at se på kerneydelsen i en cloudservice. Eventuelle accessoriske ydelser, hvori der sker behandling af personoplysninger, skal også medtages i vurderingen.

En lang række af de databeskyttelsesretlige problemstillinger, der opstår i forbindelse med brug af cloud, skyldes ofte mangel på gennemsigtighed i, hvordan servicen leveres i sin helhed. De kan også opstå som følge af, at aftalevilkår og kontraktbestemmelser er udtryk for cloudleverandørens standarder, der ikke kan ændres på en sådan måde, at aftalen afspejler den dataansvarliges individuelle krav.

En cloudleverandørs standardvilkår kan dog sagtens leve op til, at behandlingen af personoplysninger ved brug af cloud sker inden for rammerne af databeskyttelsesforordningen. Det er dog altid den dataansvarliges pligt at være betrygget i dette og altid kunne dokumentere dette over for Datatilsynet.

Momenter, der vil indgå i Datatilsynets vurdering af, hvorvidt brug af cloudservices sker inden for rammerne af databeskyttelsesreglerne, kan eksempelvis være:

- Din evne til at kunne redegøre for dine behandlingsaktiviteter, herunder datastrømme
- Din vurdering og dokumentation af cloudleverandørens evne til at sikre, at behandlingen sker i overensstemmelse med databeskyttelsesreglerne
- Kontraktens ordlyd og gennemsigtighed
- Databehandleraftalens afspejling af dine krav med hensyn til behandlingsaktiviteten
- Dine kontroller og opfølgning på eventuelle afvigelser i forhold til det aftalte

3. Databeskyttelsesretlige overvejelser ved brug af cloud

Som nævnt indledningsvis er databeskyttelsesreglerne teknologineutrale. Der tilkommer således dig som den dataansvarlige fuld valgfrihed med hensyn til, hvilke services der bedst muligt imødekommer dine forretningsmæssige behov.

Datatilsynet forstår fordelene for organisationer ved outsourcing af deres it-infrastruktur til en cloudleverandør, der er specialiseret i at levere infrastrukturydelser, ligesom tilsynet også kan se mulighederne i det store udbud af cloudservices, som kan tilgodese en flerhed af forretningsmæssige behov hos mange organisationer. Endelig har Datatilsynet også forståelse for den udvikling, der er sket i markedet og som indebærer, at mange services næsten udelukkende leveres ved brug af en cloudbaseret leverancemodel.

Det skal dog bemærkes, at Datatilsynet generelt ikke tillægger kommercielle hensyn vægt ved vurderingen af, om en behandlingsaktivitet sker inden for rammerne af databeskyttelsesreglerne. Opbygningen af et it-system eller en service kan således ikke begrunde manglende overholdelse af databeskyttelsesreglerne.

Nedenfor finder du en køreplan, som du kan tage udgangspunkt i ved vurderingen af brugen af cloud.

3.1 Kend dine services

En grundlæggende forudsætning for lovlig behandling af personoplysninger er, at du har kendskab til og har kortlagt, (i) hvilke personoplysninger du behandler, (ii) til hvilke(t) formål, og (iii) hvordan oplysningerne behandles.

Med afsæt i denne kortlægning er du herefter i stand til at vurdere, om behandlingsaktiviteten kan ske inden for rammerne af databeskyttelsesreglerne, eller om behandlingsaktiviteten alternativt skal tilpasses.

Disse vurderinger, som navnlig omfatter kravene i databeskyttelsesforordningens kapitel II-V, skal du dokumentere og altid kunne påvise over for Datatilsynet.

Hovedprincippet om ansvarlighed og evnen til at kunne dokumentere dette[4] er et væsentligt element i databeskyttelsesretten. Dokumentationen skal afspejle de overvejelser og valg – og fravalg – du har foretaget i databeskyttelsesretlig henseende og skal bl.a. bruges til at kunne påvise over for Datatilsynet, at du med hensyn til din behandlingsaktivitet på relevante tidspunkter har vurderet risiciene for de registreredes rettigheder og truffet de fornødne foranstaltninger for at reducere disse risici.

Eksempel 3

Et stort regionalt sygehus benytter en cloudservice til behandling af CT-scanninger. Servicen består i, at en computer i Sverige fremkalder flere billedpunkter i scanningen, end scanningsudstyret i Danmark er i stand til.

Den behandlende danske læge kan derudover – efter en konkret vurdering – via servicen bestille forslag til fortolkning af billedmaterialet. Det sker ved, at råfilen sendes til et universitet i Storbritannien, der har udviklet specialiseret software til analyse af

4 Se databeskyttelsesforordningens artikel 24 og artikel 5, stk. 2.

CT-scanninger. Softwaren udarbejder et forslag til fortolkning af billedmaterialet, ligesom råfilen også benyttes af softwaren til at forfine programmets evne til at foreslå fortolkningsbidrag.

Servicen leveres af en svensk virksomhed, der er databehandler for regionen, mens det britiske universitet leverer sin software som underdatabehandler (via den svenske virksomhed) til regionen.

Af regionens dokumentation fremgår det, at scanningerne er unikke på individniveau og betragtes som personoplysninger. Herudover indeholder scanningerne flere metadatapunkter som patientoplysninger, scanningssted, tidspunkt og en kort anamnese (sygehistorie).

Dokumentationen af behandlingsaktiviteten er konsolideret fra flere kilder og indeholder bl.a.:

a) En komplet beskrivelse af behandlingsaktiviteten, herunder datastrømme og behandlingsgrundlag for analyse af billedmaterialet samt hvilke risici behandlingsaktiviteten frembyder for de registreredes rettigheder.
b) En indledende screening af, at den svenske virksomhed og det britiske universitet kan sikre, at behandlingen vil ske i overensstemmelse med databeskyttelsesreglerne og (den kommende) databehandleraftale(n).
c) En indgået databehandleraftale med den svenske virksomhed, der afspejler risikovurderingen i pkt. a, og bl.a. indeholder regionens instruks om overførsel af personoplysninger til Storbritannien og en beskrivelse af overførselsgrundlaget (EU-Kommissionens tilstrækkelighedsvurdering).
d) Et tilsagn fra den svenske virksomhed om, at virksomhedens databehandleraftale med det britiske universitet afspejler de samme forpligtelser, som den svenske virksomhed er pålagt af regionen. (Alternativt dokumentation for regionens gennemgang og vurdering af underdatabehandleraftalen mellem den svenske virksomhed og det britiske universitet).
e) En risikovurdering vedrørende behandlingssikkerhed som afspejler, at behandlingsaktiviteten indebærer outsourcing, og en vurdering af, at regionen kan tilslutte sig risikovurderingerne foretaget af den svenske virksomhed og det britiske universitet.
f) En beskrivelse af det etablerede behandlingssikkerhedsniveau, herunder også hos den svenske virksomhed og det britiske universitet på baggrund af risikovurderingen i pkt. e.

Det er Datatilsynets opfattelse, at en sådan dokumentation generelt fremstår sammenhængende og i overensstemmelse med den foretagne behandlingsaktivitet.

Dokumentationen indeholder imidlertid *ikke* en særskilt vurdering af, med hvilken hjemmel oplysningerne kan videregives til det britiske universitet til brug for universitets eget formål, navnlig forbedring af programmets evne til at foreslå fortolkningsbidrag.

Eksemplet illustrerer de mange aspekter af en behandlingsaktivitet, der skal identificeres, vurderes og dokumenteres inden brugen af en cloudservice.

Bemærk endvidere, at en databehandlers behandling af personoplysninger, som vedkommende har fået overladt af den dataansvarlige, til egne formål, betragtes som en videregivelse af personoplysninger fra dataansvarlig til dataansvarlig. Der skal derfor identificeres et retligt grundlag for videregivelsen, ligesom den oprindelige dataansvarlige skal vurdere, om videregivelsen er uforenelig med det oprindelige formål med behandlingen af oplysningerne.

3.1.1 Risikovurdering vedrørende databeskyttelse

Kendskabet til din påtænkte behandlingsaktivitet er den grundlæggende forudsætning for, at du kan vurdere risiciene for den registreredes rettigheder og frihedsrettigheder og implementere tekniske og organisatoriske foranstaltninger, der sikrer, at disse risici imødegås, og at behandlingsaktiviteten sker lovligt.

Du skal med andre ord foretage en risikovurdering vedrørende databeskyttelse. Disse krav følger af bestemmelserne om den dataansvarliges ansvar og om databeskyttelse gennem design og gennem standardindstillinger.[5] Denne risikovurdering er selvstændig fra risikovurderingen vedrørende behandlingssikkerhed, der er nærmere omtalt nedenfor i afsnit 3.1.2.

For så vidt angår behandlingsaktiviteter, der understøttes af et it-system, betyder det eksempelvis, at der kan være en risiko for indsamling af yderligere oplysninger end nødvendigt eller en risiko for, at den registrerede ikke modtager de informationer, der følger af den dataansvarliges oplysningspligt. Reglerne om databeskyttelse gennem design og gennem standardindstillinger indebærer, at du skal træffe foranstaltninger – tekniske og organisatoriske – med henblik på, at sådanne risici mitigeres.

Når du foretager din risikovurdering vedrørende databeskyttelse, skal du tage udgangspunkt i selve den påtænkte behandlingsaktivitet. Hvis behandlingsaktiviteten understøttes af et it-system, skal systemet og dets indretning dermed også indgå i vurderingen.

Som nævnt ovenfor er det imidlertid karakteristisk for cloudservices, at disse leveres som standardløsninger, hvor der er intet eller alene et begrænset rum for dig som den dataansvarlige at anmode om tilpasninger af leverancemodellen eller applikationerne. Der kan derfor være et begrænset rum for at træffe de nødvendige tekniske foranstaltninger for at imødegå eventuelle databeskyttelsesrisici eller alternativt ændre systemets indretning således, at den identificerede risiko helt fjernes.

Det betyder, at der kan være cloudservices, som du på baggrund af din risikovurdering vedrørende databeskyttelse er nødt til at fravælge, hvis – og i det omfang – det ikke er muligt at implementere tekniske foranstaltninger, som du vurderer som nødvendige.

Dette vil oftest være tilfældet for SaaS-løsninger, da du i disse tilfælde overlader mest muligt kontrol til cloudleverandøren, men det kan også være tilfældet for PaaS- og IaaS-løsninger.

Inden du iværksætter eller væsentligt ændrer en behandlingsaktivitet, skal du gennemføre en risikovurdering vedrørende databeskyttelse. Med udgangspunkt i denne risikovurdering kan du herefter vurdere, om den påtænkte cloudservice kan understøtte din behandlingsaktivitet, uden at det medfører større risici for de registrerede.

Med hensyn til brugen af cloudservices er det særligt relevant at afdække bl.a. følgende, herunder eventuelt i samarbejde med leverandøren:

- Behandler cloudleverandøren andre personoplysninger end de oplysninger, som leverandøren får overladt? Der kan eksempelvis være tale om indsamling af metadata eller andre styringsdata. I bekræftende fald skal du vurdere, hvem der er ansvarlig for behandlingen af disse oplysninger mv.
- Behandler cloudleverandøren de oplysninger, som leverandøren får overladt, til egne formål? I bekræftende fald skal du vurdere, om – og i givet fald med hvilken hjemmel – de omhandlede personoplysninger kan videregives til cloudleverandøren.

5 Se databeskyttelsesforordningens artikel 24 og 25. En nærmere gennemgang heraf findes i Datatilsynets vejledning om behandlingssikkerhed og databeskyttelse gennem design og gennem standardindstillinger.

3.1.2 Risikovurdering vedrørende behandlingssikkerhed

For enhver behandlingsaktivitet skal du som den dataansvarlige – oftest sammen med din databehandler (i dette tilfælde cloudleverandøren) – etablere et passende behandlingssikkerhedsniveau.

Forudsætningen for at kunne etablere og opretholde passende sikkerhed er, at du forinden har gennemført en risikovurdering.

Datatilsynet forstår, at det kan forekomme som en vanskelig opgave for den enkelte dataansvarlige. Det er ikke desto mindre den grundlæggende forudsætning for at etablere passende sikkerhed, at du som dataansvarlige har overblik over, hvilke scenarier du skal sikre dig imod.

Brug af cloudleverandører har – ligesom enhver anden brug af databehandlere – den sikkerhedsmæssige betydning, at det ikke længere er dig som den dataansvarlige, men derimod databehandleren, som har den praktiske opgave med at implementere de nødvendige sikkerhedsforanstaltninger. Derudover er det sædvanligt, at cloudleverandører allerede har etableret et vist behandlingssikkerhedsniveau, når leverandørne begynder at udbyde en eller flere services på markedet.

Din opgave som den dataansvarlige består dermed i – eventuelt med bistand fra cloudleverandøren – at:

- Afdække det etablerede behandlingssikkerhedsniveau hos cloudleverandøren, herunder ved en gennemgang af leverandørens dokumentation og eventuelt via en uddybende dialog med leverandøren
- Vurdere, om dette behandlingssikkerhedsniveau svarer til det niveau, som du som den dataansvarlige vurderer er passende på baggrund af din egen risikovurdering

Datatilsynet anerkender, at mange cloudleverandører vil have passende – eller endda mere end passende – behandlingssikkerhed for størstedelen af de behandlingsaktiviteter, som leverandøren får overladt af sine kunder. Din opgave som den dataansvarlige består dermed ”blot” i at verificere, at dette er tilfældet og dokumentere din vurdering.

Der kan dog være tilfælde, hvor du som den dataansvarlige har en særlig behandlingsaktivitet, som eksempelvis omfatter behandling af helbredsoplysninger i stort omfang, hvor du finder, at yderligere foranstaltninger, end dem som cloudleverandøren allerede har implementeret, er nødvendige. I så fald skal du sikre dig, at aftalegrundlaget med cloudleverandøren giver dig ret til at kræve, at cloudleverandøren implementerer disse yderligere sikkerhedsforanstaltninger, som du finder nødvendige.

Du skal også være opmærksom på opgave- og ansvarsfordelingen mellem dig og cloudleverandøren for så vidt angår din behandlingsaktivitet. Hvis du tidligere har udført den pågældende behandlingsaktivitet selv, vil en overladelse til en cloudleverandør betyde, at du sandsynligvis skal genbesøge din egen risikovurdering og dine eventuelle eksisterende sikkerhedsforanstaltninger. Det skyldes, at risikobilledet for din behandlingsaktivitet sandsynligvis vil have ændret sig som følge af din brug af en databehandler (cloudleverandøren), ligesom dine eventuelle sikkerhedsforanstaltninger skal revideres som følge af den ændrede opgavefordeling, herunder eksempelvis kontroller for så vidt angår adgangsstyring, change control mv.

Eksempel 4

En kommune benytter en IaaS-løsning, hvor personoplysninger transporteres/routes i transit gennem et tredjeland. Oplysningerne bliver på intet tidspunkt behandlet i tredjelandet på anden måde end selve transmissionen.

Her er der som udgangspunkt ikke tale om en tredjelandsoverførsel som forstået i databeskyttelsesforordningens kapitel V.[6]

Kommunen skal dog stadig sikre et passende behandlingssikkerhedsniveau, herunder fx for at imødegå indsamling af oplysningerne af en efterretningstjeneste direkte fra kabeltransmissionen. I praksis vil dette ofte ske ved, at kommunen vurderer i hvilket omfang de sikkerhedsforanstaltninger, som IaaS-leverandøren har etableret, er tilstrækkelige.

Hvis IaaS-leverandøren alene har implementeret kryptering af transportlaget under anvendelse af en nøgle, som er under IaaS-leverandørens kontrol, kan det eksempelvis være en nødvendig yderligere sikkerhedsforanstaltning, at kommunen sikrer kryptering på data (indholdskryptering) under transporten med en nøgle, der alene er tilgængelig i EU/EØS og under kommunens kontrol.

3.2 Kend din leverandør

Brug af cloudservices indebærer normalt, at cloudleverandøren behandler oplysningerne på dine vegne som databehandler. Det betyder, at leverandøren alene må behandle oplysningerne efter din instruks.

Det er derfor også et krav, at der indgås en databehandleraftale med leverandøren. Aftalen skal opfylde en række mindstekrav og skal bl.a. indeholde din instruks til leverandøren, ligesom aftalen generelt skal fastlægge rammerne for leverandørens behandling af oplysningerne. Se afsnit 3.2.2. nedenfor for nærmere om indgåelse af databehandleraftalen.

3.2.1 Screening af leverandør(e)

Grundlæggende har du som den dataansvarlige fuld valgfrihed med hensyn til, hvilken cloudleverandør, du ønsker at overlade behandling af personoplysninger til.

Valgfriheden er alene afgrænset af, at du kun må benytte en leverandør, der kan stille de fornødne garantier for, at vedkommende vil overholde databeskyttelsesreglerne i forbindelse med sin behandling af oplysningerne på dine vegne.[7]

Det betyder, at du på forhånd skal screene de(n) potentielle cloudleverandør(er) for at vurdere, om leverandøren vil være i stand til at leve op til de databeskyttelseskrav, som du vurderer er passende for din behandlingsaktivitet.

Det er Datatilsynets opfattelse, at denne screening med fordel kan tage udgangspunkt i den databehandleraftale, som du påregner at indgå med cloudleverandøren. Det kan eksempelvis være Datatilsynets standarddatabehandleraftale, EU-Kommissionens databehandleraftale[8] eller leverandørens egen databehandleraftale.

Du bør således have bl.a. følgende spørgsmål besvaret af cloudleverandøren – enten via en dialog med leverandøren eller ved gennemgang af leverandørens egen dokumentation:

a) Er cloudleverandøren i henhold til databehandleraftalen forpligtet til alene at behandle personoplysninger efter din instruks, eller forbeholder leverandøren sig ret til at behandle oplysninger til egne formål?

6 EDPB's guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

7 Se databeskyttelsesforordningens artikel 28, stk. 1.

8 EU-Kommissionen offentliggjorde den 4. juni 2021 i henhold til forordningens artikel 28, stk. 7, et sæt standardkontraktbestemmelser, der har samme karakter som Datatilsynets skabelon mellem dataansvarlige og databehandlere. Se nærmere her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/okt/databehandleraftale-skal-jeg-bruge-dansk-skabelon-eller-eu-standardkontraktbestemmelser

b) Har cloudleverandøren etableret politikker og procedurer, der sikrer, at leverandørens medarbejdere har forpligtet sig til fortrolighed eller er underlagt en anden passende tavshedspligt, og kan leverandøren påvise dette?
c) Har cloudleverandøren etableret et passende niveau af behandlingssikkerhed i lyset af den overladte behandlingsaktivitet, herunder henset til ansvarsfordelingen mellem dig og leverandøren?
d) Har cloudleverandøren en procedure for screening af eventuelle underdatabehandlere med henblik på at sikre, at underdatabehandleren også vil være i stand til at leve op til de databeskyttelseskrav, som du har fastsat over for leverandøren, og indebærer proceduren i givet fald fremsendelse af underdatabehandlerens dokumentation til dig som den dataansvarlige?
e) Indeholder ovennævnte procedure en frist for fremsendelse af dokumentation af screening af underdatabehandleren, der stemmer overens med fristen for varsling om brugen af nye underdatabehandlere eller ændring af nuværende underdatabehandlere?
f) Afspejler den (eventuelle) underdatabehandleraftale de samme krav, som vil blive pålagt cloudleverandøren af dig som den dataansvarlige?
g) Har cloudleverandøren en fuldstændig oversigt over, hvilke underdatabehandlere leverandøren benytter til brug for levering af sine services, herunder hvilke lande – særligt uden for EU/EØS – disse underdatabehandlere befinder sig i, og fra hvilke lande leverandøren og eventuelle underdatabehandlere kan tilgå oplysningerne? Har cloudleverandøren, i bekræftende fald, etableret et overførselsgrundlag, der er effektivt i lyset af den behandlingsaktivitet, du overlader til leverandøren?
h) Har cloudleverandøren – henset til den overladte behandlingsaktivitet – procedurer for at bistå dig med håndtering af anmodninger fra de registrerede efter databeskyttelsesforordningens kapitel III?
i) Har cloudleverandøren procedurer for håndtering af brud på persondatasikkerheden, og omfatter disse procedurer i givet fald cloudleverandørens bistand til dig med din forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet?
j) Kan cloudleverandøren slette eller tilbagelevere personoplysningerne ved behandlingsaktivitetens ophør?[9]
k) Har cloudleverandøren en procedure for at bistå dig i forbindelse med dit tilsyn med vedkommende eller for gennemførelse af revision ved uafhængige tredjemænd fx revisorer?

I din gennemgang af leverandørens dokumentation eller din dialog med leverandøren er der for en række af de ovennævnte punkter særlige forhold, som du bør være opmærksom på.

Særligt ad pkt. a)

Cloudleverandøren må (med hensyn til de behandlede personoplysninger) kun agere i overensstemmelse med den instruks, der er givet fra dig som den dataansvarlige. Leverandøren må derfor som udgangspunkt ikke behandle de overladte personoplysninger til egne formål, medmindre leverandøren er forpligtet hertil på baggrund af lovkrav i EU-retten eller medlemsstaternes nationale ret.

Hvis en cloudleverandør behandler personoplysninger til egne formål uden tilladelse fra dig som den dataansvarlige, vil det (i) udgøre et brud på persondatasikkerheden for den dataansvarliges vedkommende, ligesom (ii) cloudleverandøren vil være selvstændigt ansvarlig for denne behandlingsaktivitet.

Cloudleverandørens behandling af oplysninger til egne formål skal efter Datatilsynets opfattelse anses som en videregivelse af personoplysninger til leverandøren.

9 Der kan bl.a. være forhold relateret til cloudleverandørens brug af fælles hardware, der indebærer, at leverandøren ikke er i stand til at kunne sikre effektiv sletning af oplysningerne, ligesom cloudleverandøren kan være omfattet af tredjelandes lovgivning, der indebærer, at leverandøren ikke er berettiget til at slette oplysningerne. Det bemærkes, at overholdelse af tredjelandes lovgivning ikke kan begrunde en fravigelse af sletteforpligtelsen.

Hvis du ønsker at tillade leverandøren at behandle oplysninger til egne formål eller ønsker at benytte en leverandør, der forbeholder sig retten til at behandle oplysninger, som overlades til vedkommende, til egne formål, skal du være opmærksom på følgende:

a) Formålene, hvortil leverandøren ønsker at behandle personoplysningerne, må ikke være uforenelige med de formål, hvortil oplysningerne oprindeligt blev indsamlet af dig
b) Du skal have et retligt grundlag for at videregive personoplysningerne til leverandøren til brug for dennes behandlingsaktiviteter (ligesom leverandøren også skal identificere et retligt grundlag for sin behandling)

Datatilsynet bemærker endvidere, at der i tilfælde, hvor leverandøren generelt forbeholder sig retten til at behandle de overladte personoplysninger til egne formål, vil være tale om videregivelse af alle de overladte personoplysninger – og ikke alene de oplysninger, som leverandøren reelt beslutter at behandle til sine egne formål. Det skyldes, at leverandøren ved et sådant generelt forbehold reelt har kontrol over alle oplysningerne og træffer beslutning om, hvilke oplysninger leverandøren ønsker at behandle. Leverandøren skal derfor anses som den dataansvarlige for alle oplysningerne, herunder også de oplysninger, som leverandøren fravælger at behandle til egne formål.

Derudover skal du som den dataansvarlige efter Datatilsynets opfattelse[10] til en vis grad påse, at modtageren, som personoplysninger videregives til, har et retligt grundlag for at behandle disse oplysninger.

Hvis du er eller bliver opmærksom på, at det er usandsynligt, at cloudleverandøren vil have et retligt grundlag for sin behandling af personoplysningerne til sine egne formål, vil det ikke være lovligt for dig at videregive oplysningerne til leverandøren.

Du bør derfor omhyggeligt gennemgå den databehandleraftale, som du påtænker at indgå med cloudleverandøren, med henblik på at afdække, om – og i givet fald i hvilket omfang – leverandøren påtænker at behandle de overladte personoplysninger til egne formål.

Eksempel 5

En konsulentvirksomhed ønsker at overgå til et cloudbaseret customer relationship management system (CRM system). Virksomheden påregner at behandle oplysninger om navn, arbejdsmailadresser, oplysninger om udført arbejde samt kundernes feedback i systemet.

En nærmere undersøgelse af aftalevilkårene, herunder databehandleraftalen, som cloudleverandøren tilbyder det pågældende CRM system under, viser, at leverandøren pseudonymiserer oplysningerne, der registreres i systemet, og behandler de pseudonymiserede oplysninger til (i) forbedring af systemets funktionalitet samt (ii) intern rapportering og modellering, fx kapacitetsplanlægning o. lign.

Konsulentvirksomheden vurderer, at cloudleverandørens behandling af personoplysninger til sine egne to ovennævnte formål ikke er uforeneligt med de(t) formål, som konsulentvirksomheden oprindeligt indsamlede oplysningerne til, og at cloudleverandørens behandling til de to formål sker med henblik på at forfølge en legitim interesse.

I dette tilfælde udgør cloudleverandørens behandling af oplysningerne til egne formål ikke en hindring for konsulentvirksomhedens brug af den omhandlede cloudservice. Det bemærkes, at cloudleverandøren er selvstændigt ansvarlig for, at behandlingen af oplysningerne til de ovennævnte to formål i øvrigt sker inden for rammerne af databeskyttelsesreglerne.

10 I medfør af princippet om lovlighed i databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Særligt ad pkt. d)

Som nævnt er det et krav i databeskyttelsesforordningen, at du kun må benytte en databehandler, der kan stille de fornødne garantier for, at vedkommende vil overholde databeskyttelsesreglerne i forbindelse med sin behandling af oplysningerne. Denne pligt er ikke afgrænset til den første databehandler, du benytter. Foruden selve cloudleverandøren skal du således også sikre, at leverandørens eventuelle brug af underdatabehandlere vil ske på en sådan måde, at behandlingen overholder databeskyttelsesreglerne.

Grundtanken er, at den registreredes rettigheder og frihedsrettigheder skal nyde en tilsvarende beskyttelse hele vejen i leverandørkæden, og at beskyttelsesniveauet ikke sænkes som følge af, at behandlingen overlades til en underdatabehandler.

I praksis er det nærliggende, at cloudleverandøren har foretaget screeningen af eventuelle underdatabehandlere for at sikre, at disse også kan overholde databeskyttelsesreglerne. Resultaterne af disse screeninger skal dog være tilgængelige for dig som den dataansvarlige som en del af cloudleverandørens dokumentation eller kunne udleveres efter anmodning med henblik på, at du kan verificere disse screeninger.

Du skal også være opmærksom på dette krav, når cloudleverandøren eventuelt udskifter underdatabehandlere. Cloudleverandørens procedurer for screening af underdatabehandlere bør derfor også omfatte fremsendelse af eventuelle underdatabehandleres dokumentation til dig, når leverandøren anmoder om en specifik godkendelse til brugen af en ny eller anden underdatabehandler eller underretter om den påtænkte brug af en ny eller anden databehandler, hvis leverandøren har en generel godkendelse.

Særligt ad pkt. f)

Det er også et krav efter databeskyttelsesforordningen, at cloudleverandøren pålægger sine eventuelle underdatabehandlere tilsvarende krav, som leverandøren selv har forpligtet sig til efter den databehandleraftale, der indgås mellem leverandøren og dig som den dataansvarlige.

Det sker oftest gennem indgåelse af en underdatabehandleraftale mellem cloudleverandøren og eventuelle underdatabehandlere.

Det er ikke et krav, at ordlyden af underdatabehandleraftalen er identisk med den databehandleraftale, som du påtænker at indgå med cloudleverandøren. Underdatabehandleraftalen skal derimod ses i lyset af de specifikke behandlingsaktiviteter, der konkret er overladt til underdatabehandleren. Underdatabehandleren skal dog grundlæggende være underlagt de samme databeskyttelsesforpligtelser, som cloudleverandøren vil blive underlagt.

Som eksempel kan nævnes, at hvis cloudleverandøren efter databehandleraftalen er forpligtet til at anmode om din forudgående specifikke godkendelse til eller (i tilfælde af en generel godkendelse) at underrette om udskiftning af underdatabehandler med 6 måneders varsel, vil det ikke være tilstrækkeligt, hvis underdatabehandleren – i henhold til aftalen mellem cloudleverandøren og underdatabehandleren – alene skal varsle cloudleverandøren med 30 dages varsel.

Særligt ad pkt. g)

Det er hyppigt forekommende, at en cloudleverandør benytter sig af en række underleverandører til brug for levering af sin(e) service(s).

Som den dataansvarlige skal du have et komplet overblik over, hvilke databehandlere – foruden selve cloudleverandøren – du overlader behandling af personoplysninger til. Du skal således kortlægge alle de underleverandører, som cloudleverandøren benytter, og eventulle yderligere underleverandører, der måtte findes i leverandørkæden.

Det skyldes, at du som den dataansvarlige skal kunne dokumentere, at alle de pågældende databehandlere – cloudleverandøren og eventuelle underleverandører – kan stille de fornødne garantier for, at behandlingen af personoplysninger vil overholde databeskyttelsesforordningen.

Det skyldes også, at personoplysninger kun må overføres til lande uden for EU/EØS efter aktiv instruks fra dig som den dataansvarlige. Du skal derfor aktivt forholde dig til, om du vil instruere cloudleverandøren i at overføre personoplysninger til eventuelle underdatabehandlere i tredjelande, som leverandøren benytter. Se nærmere herom i afsnit 3.4 nedenfor.

3.2.2 Indgåelse af databehandleraftale

Når du benytter en cloudleverandør, sker det oftest i form af en databehandlerkonstruktion, og der skal derfor indgås en databehandleraftale mellem dig og cloudleverandøren.

Databeskyttelsesforordningen indeholder en række mindstekrav, som en databehandleraftale skal leve op til for at være gyldig. Det er bl.a. et krav, at databehandleraftalen er skriftlig og foreligger i elektronisk form.

En databehandleraftale skal bl.a. indeholde oplysninger om genstanden for og varigheden af behandlingsaktiviteten, behandlingens karakter og formål, typen af personoplysninger, kategorierne af registrerede og dine forpligtelser og rettigheder som den dataansvarlige samt databehandlerens pligter ved behandling af personoplysningerne.

For nærmere om databehandleraftaler og mindstekravene hertil henvises til Datatilsynets vejledning om dataansvarlige og databehandlere, Datatilsynets standarddatabehandleraftale, der er godkendt af Det Europæiske Databeskyttelsesråd, og EU-Kommissionens standardbestemmelser i henhold til artikel 28, stk. 7.

3.3 Tilsyn med cloudleverandøren og eventuelle underleverandører

Du har – som den dataansvarlige – en pligt til at føre tilsyn med dine databehandlere for at sikre, at disse – på samme måde som dig selv – behandler oplysningerne forsvarligt. Det gælder også, når du overlader behandlingen til en eller flere cloudleverandører.

Datatilsynet har udarbejdet en overordnet vejledning om tilsyn med databehandlere, hvor du kan læse mere om hvordan og hvor hyppigt, du bør føre tilsyn med dine databehandlere. Nedenfor beskrives kort de momenter, der bør indgå i din vurdering af hvordan og hvor hyppigt, du skal føre tilsyn med din(e) leverandør(er).

3.3.1 Intensitet

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**

3.3.2 Hyppighed

Jo mere kritisk behandlingen er for de registrerede (de personer som oplysningerne omhandler), jo mere intensiv kontrol skal du som 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 at påse behandlingssikkerheden med en lavere frekvens, hvis risikoen er lav.

Momenter, der taler for høj eller lav frekvens

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 bliver informeret om dette, men i nogle tilfælde vil du opdage det, fx fordi bruddet afbryder den service, du får som kunde, og derfor er det måske nødvendigt at forlange en forklaring på afbrydelsen af en service. Dermed kan databehandleren ikke skjule årsagen eller alvoren af et brud. Når det kommer til brud på persondatasikkerheden, er det et lovkrav, at databehandleren informerer dig om disse, uden unødig forsinkelse.
- Der skiftes ofte underdatabehandler(e).
- Der sker ofte ejerskifte, opkøb, fusion eller gennemgribende ændringer i strategien hos databehandleren. Den slags vil du 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:

- Ejerskifte, fusion eller gennemgribende ændringer i strategien hos databehandleren.
- En pandemi ændrer på den måde der arbejdes på, og på tilgangen til personoplysninger (flere hjemmearbejdspladser og en ændring i forudsætningerne for brug af den pågældende service).

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 alvorlige sikkerhedsbrud.

3.3.3 Særligt for cloudleverandører

Datatilsynet forstår, at cloudleverandører sædvanligvis – som led i leverandørens generelle informationssikkerhedsledelsessystem – har etableret procedurer for og får gennemført revisioner af en eller flere uafhængige tredjemænd, som udarbejder revisionsrapporter på den baggrund.

Det vil i den forbindelse normalt være tilstrækkeligt, at du som den dataansvarlige gennemgår de revisionsrapporter, som cloudleverandøren årligt får udarbejdet.

Det er dog væsentligt at være opmærksom på, i hvilket omfang revisionsrapporten dækker de behandlingsaktiviteter, som du har overladt til cloudleverandøren.

Hvis dette ikke er tilfældet for de revisionsrapporter, som leverandøren får udarbejdet af egen drift, skal du sikre dig, at du efter aftalegrundlaget med leverandøren er berettiget til at kræve en revision under et andet omfang og eller under anvendelse af anden metode, der er dækkende for dine behandlingsaktiviteter.

3.4 Overførsler til tredjelande

Hvis din påtænkte cloudleverandør befinder sig i et land uden for EU/EØS – et såkaldt tredjeland – eller benytter sig af én eller flere underdatabehandlere, der befinder sig uden for EU/EØS, skal du være særligt opmærksom på en række bestemte krav. Datatilsynet har i den forbindelse i juli 2021 revideret sin vejledning om overførsel af personoplysninger til tredje-lande, som gennemgår kravene mere i dybden.

Når du påtænker at overlade en eller flere behandlingsaktiviteter til en cloudleverandør, kan du med hensyn til overholdelse af de særlige krav – reglerne i databeskyttelsesforordningens kapitel V – med fordel tage udgangspunkt i den køreplan, der fremgår af Det Europæiske Databeskyttelsesråds anbefalinger om supplerende foranstaltninger[11].

Det betyder, at du skal:

1) Identificere dine tredjelandsoverførsler
2) Identificere eller etablere det relevante overførselsgrundlag
3) (Hvis overførselsgrundlaget findes i artikel 46) Vurdere, hvorvidt det omhandlede overførselsgrundlag er effektivt i lyset af alle omstændighederne ved overførslen, og i benægtende fald
4) Træffe supplerende foranstaltninger
5) Iagttage eventuelle proceduremæssige krav
6) Reevaluere overførslerne med passende intervaller

Særligt ad pkt. 1)

Når du skal identificere, om der i forbindelse med din brug af den omhandlede cloudleverandør vil blive overført personoplysninger til tredjelande, og i bekræftende fald hvilke lande det drejer sig om, kan du med fordel tage udgangspunkt i den kortlægning af, hvor personoplysninger behandles, som du har foretaget i forbindelse med din screening af den pågældende leverandør. Se nærmere om denne kortlægning ovenfor i afsnit 3.2.1.

Kortlægningen skal bl.a. besvare, om personoplysninger bliver behandlet af en eller flere databehandlere i tredjelande, og om personoplysninger bliver eller vil blive tilgået af databehandlere i tredjelande. I givet fald skal du – foruden at indgå en databehandleraftale med instruks om at overføre personoplysninger til disse databehandlere i de pågældende tredjelande – også etablere et gyldigt overførselsgrundlag.

Vær særligt opmærksom på, at alle overførsler af personoplysninger kræver et overførselsgrundlag. Det gælder alt fra behandling af personoplysninger i forbindelse med service- og supportfunktioner til overførsel af personoplysninger til brug for afregning af eller fejlsøgning på cloudservicen.

Det er ikke ualmindeligt, at der blandt cloudleverandørers dokumentation alene findes en generel oversigt over alle underdatabehandlere, som den pågældende leverandør benytter til levering af sine services. Hvis du kun bruger enkelte af de cloudservices, som leverandøren tilbyder, er det derfor ikke sikkert, at alle de pågældende underdatabehandlere er relevante for dig. Du kan derfor med fordel indgå i en dialog med cloudleverandøren om, hvilke specifikke underdatabehandlere der er relevante for de services, som cloudleverandøren leverer til dig.

Det er dog dit ansvar som den dataansvarlige at kunne dokumentere dette over for Datatilsynet. Hvis det ikke er muligt at indgå i en dialog med cloudleverandøren, eller hvis din dialog med leverandøren ikke giver dig tilstrækkelig information til, at du over for Datatilsynet vil kunne dokumentere hvilke specifikke underdatabehandlere, der er relevante for de services, du benytter, skal du efter Datatilsynets opfattelse lægge til grund, at alle de underdatabehandlere, der fremgår af cloudleverandørens generelle oversigt, benyttes til levering af dine cloudservices.

Særligt ad pkt. 2)

Hvis cloudleverandøren eller dennes underdatabehandler(e) befinder sig i et af de lande, som EU-Kommissionen har vurderet som et sikkert tredjeland, er det tilstrækkeligt for så vidt angår dit overførselsgrundlag at henvise til EU-Kommissionens tilstrækkelighedsafgørelse.

11 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Hvis leverandøren eller dennes databehandler(e) ikke befinder sig i et sådant tredjeland, vil du oftest tilvejebringe det nødvendige overførselsgrundlag ved at indgå en standardkontrakt, som er vedtaget af EU-Kommissionen, med cloudleverandøren m.fl.

Hvis cloudleverandøren benytter sig af en eller flere underdatabehandlere i tredjelande, vil cloudleverandøren oftest allerede have indgået en standardkontrakt med den pågældende underdatabehandler, som vil udgøre det nødvendige overførselsgrundlag.

Det er dog fortsat dig som den dataansvarlige, der skal påse – og kunne dokumentere over for Datatilsynet – at der foreligger et overførselsgrundlag til det pågældende tredjeland.[12]

Standardbestemmelser om databeskyttelse

Et af de måske mest brugte overførselsgrundlag er EU-Kommissionens standardbestemmelser om databeskyttelse – også kaldet standardkontrakter – der fungerer som en skabelon, der udfyldes og underskrives af dataeksportøren og dataimportøren. Både EU-Kommissionen og de nationale tilsynsmyndigheder har mulighed for at vedtage standardbestemmelser, men indtil videre er det kun EU-Kommissionen, der har udnyttet muligheden.

EU-Kommissionen har den 4. juni 2021 vedtaget nye standardbestemmelser til brug for overførsel til tredjelande. De nye standardbestemmelser består af flere særskilte moduler, som skal kombineres alt efter, hvilken overførselssituation man befinder sig i. Det har siden den 27. juni 2021 været muligt at benytte de nye standardbestemmelser i følgende fire overførselssituationer:

- Modul 1: Overførsel fra dataansvarlig til dataansvarlig
- Modul 2: Overførsel fra dataansvarlig til databehandler
- Modul 3: Overførsel fra databehandler til databehandler
- Modul 4: Overførsel fra databehandler til dataansvarlig

Hvis du ønsker at benytte standardbestemmelser som overførselsgrundlag, skal du ikke have en forudgående godkendelse fra Datatilsynet. Du bør dog altid sikre dig, at du som dataeksportør har anvendt standardbestemmelserne korrekt, og at du og dataimportøren i øvrigt er i stand til at leve op til de forpligtelser, der følger med brugen af standardbestemmelserne.

De nye standardbestemmelser indeholder en såkaldt "docking clause", hvilket gør det muligt løbende at udskifte eller tilføje parter til aftalen, hvilket særligt kan være relevant for mere komplekse behandlingsaktiviteter.

Du kan derudover lade standardbestemmelserne indgå som en del af en bredere kontrakt mellem dig og dataimportøren samt tilføje andre klausuler eller yderligere garantier, forudsat at de ikke direkte eller indirekte er i strid med standardbestemmelserne. Det vil eksempelvis være muligt at inkludere bestemmelser om anvendelse af supplerende foranstaltninger, uden at det kræver en godkendelse fra Datatilsynet.

Hvis du ændrer i standardbestemmelserne i strid med deres indhold, skal du være opmærksom på, at de hermed vil ændre karakter og blive til en såkaldt ad hoc aftale, som kræver godkendelse fra Datatilsynet.

Særligt ad pkt. 3) og 4)
I juli 2020 fastslog EU-Domstolen i den såkaldte Schrems II-dom, at en overførsel, der sker på baggrund af fornødne garantier såsom EU-Kommissionens standardkontrakter, skal sikre den

[12] Se databeskyttelsesforordningens artikel 44, der indeholder det generelle princip om overførsel af personoplysninger til tredjelande. Det følger heraf, at overførsel kun må finde sted "hvis betingelserne i [kapitel V] med forbehold af de øvrige bestemmelser i denne forordning opfyldes af den dataansvarlige og databehandleren." (Datatilsynets fremhævning)

registrerede en beskyttelse af vedkommendes personoplysninger, som i det væsentlige svarer til beskyttelsesniveauet i EU/EØS.

Det betyder, at du skal vurdere, om der er lovgivning og/eller praksis i de(t) pågældende tredjeland(e), der påvirker effektiviteten af de(n) indgåede standardkontrakt(er). Det vil eksempelvis være tilfældet, hvis der findes lovgivning og/eller praksis i tredjelandet, som tillader indsamling af eller adgang til de overførte oplysninger for retshåndhævende myndigheder på en måde, der ikke opfylder europæiske standarder.

Hvis dette er tilfældet, har du ifølge anbefalingerne fra Det Europæiske Databeskyttelsesråd tre muligheder.

Du kan **(i)** undlade at iværksætte eller suspendere overførslen, hvilket i praksis sandsynligvis vil betyde at undlade at benytte den pågældende cloudservice.

Alternativt kan du **(ii)** træffe supplerende foranstaltninger for at bringe beskyttelsesniveauet op på det påkrævede europæiske niveau. Det Europæiske Databeskyttelsesråd har i den forbindelse offentliggjort et sæt anbefalinger, der nærmere beskriver, hvordan du vurderer beskyttelsesniveauet i et tredjeland, og hvilke eventuelle supplerende foranstaltninger, du om nødvendigt skal træffe.

Hvis det er nødvendigt at træffe supplerende foranstaltninger vil det som regel skulle være tekniske supplerende foranstaltninger. Det skyldes, at kontraktuelle og organisatoriske foranstaltninger oftest ikke vil være tilstrækkelige for at imødegå den "problematiske" lovgivning og/eller praksis.[13] Dette beror dog på de konkrete omstændigheder ved den "problematiske" lovgivning og/eller praksis. Det Europæiske Databeskyttelsesråd anfører, at kombination af forskellige foranstaltninger på en sådan måde, at de understøtter og bygger på hinanden, kan bringe beskyttelsesniveauet op på et europæisk niveau.[14] Datatilsynet bemærker dog, at i tilfælde, hvor den "problematiske" lovgivning og/eller praksis tillader indsamling af og/eller adgang til personoplysninger for tredjelandes efterretningstjenester eller lignende retshåndhævende myndigheder på en måde, der ikke opfylder europæiske standarder, almindeligvis kun kan imødekommes ved supplerende tekniske foranstaltninger.

Det er ikke afgørende, om det er dig som den dataansvarlige eller din cloudleverandør, der træffer de supplerende foranstaltninger, forudsat foranstaltningerne er effektive. Der vil dog være typer af supplerende foranstaltninger, herunder navnlig implementering af effektiv kryptering, som kan være vanskelige for cloudleverandøren at træffe. Det er navnlig tilfældet, hvis leverandøren selv vil være i besiddelse af krypteringsnøglen, hvorved krypteringen ikke vil kunne anses som effektiv. I tilfælde, hvor cloudleverandøren kan træffe effektive foranstaltninger, er det dog fortsat dit ansvar som den dataansvarlige at sikre dig, at de supplerende foranstaltninger, som cloudleverandøren træffer, reelt er effektive og i kombination med det relevante overførselsgrundlag sikrer et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS.

Datatilsynet forstår, at det kan være en ganske omfangsrig øvelse at vurdere lovgivning og praksis i en lang række tredjelande, hvor din påtænkte cloudleverandør og dennes eventuelle underdatabehandlere befinder sig. Det er i den forbindelse Datatilsynets opfattelse, at du kan basere din vurdering på et "worst case scenario", dvs. at alle de omhandlede tredjelande har "problematisk" lovgivning og/eller praksis og på den baggrund nærmere vurdere, hvilke supplerende tekniske foranstaltninger der skal træffes for at sikre et beskyttelsesniveau, der i det væsentlige svarer til niveauet i EU/EØS.

Endelig kan du **(iii)** beslutte at fortsætte overførslen uden at træffe supplerende foranstaltninger, hvis du ikke har nogen grund til at tro, at den relevante "problematiske" lovgivning vil blive

13 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 53.

14 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 52.

anvendt i praksis for så vidt angår din cloudleverandør, herunder eventuelle underdatabehandlere, og/eller oplysningerne, som du overfører.

I så fald skal du i din vurdering, eventuelt i samarbejde med cloudleverandøren, påvise og dokumentere, at lovgivningen og/eller praksis ikke fortolkes eller anvendes på cloudleverandøren m.fl. og/eller de overførte oplysninger.[15] Det vil dog ikke være tilstrækkeligt som dokumentation at henvise til din egen – eller cloudleverandørens – subjektive vurdering af, at de personoplysninger, der vil blive overført, ikke har interesse for fx retshåndhævende myndigheder, hvis dette udsagn ikke er understøttet af objektiv, troværdig og tilgængelig information, fx fra de omhandlede myndigheder.

Nedenfor i afsnit 3.5 gennemgås – med udgangspunkt i USA – ovennævnte pkt. **(ii)** og **(iii)**.

3.5 Cloud og USA

I databeskyttelsesforordningens forstand betragtes USA som et tredjeland, hvorfor forordningens kapitel V skal iagttages ved overførsel af personoplysninger hertil.

Siden EU-Domstolens afgørelse af 16. juli 2020 i den såkaldte Schrems II-sag foreligger der ikke længere en afgørelse fra EU-Kommissionen om, at USA frembyder et tilstrækkeligt beskyttelsesniveau. For at overføre personoplysninger til USA i forbindelse med brug af cloudservices skal du derfor etablere fornødne garantier, fx indgå EU-Kommissionens standardkontrakt med cloudleverandøren.

For en generel gennemgang af Schrems II-dommen, og hvilken betydning dommen har for overførsel af personoplysninger til USA henvises til Datatilsynets nyhed om Schrems II-dommen, Det Europæiske Databeskyttelsesråds anbefalinger 02/2020 om de 4 essentielle garantier og anbefalinger 01/2020 om supplerende foranstaltninger.

Kort opsummeret vurderede EU-Domstolen i sagen med hensyn til USA, at hverken Foreign Surveillance Intelligence Act (FISA) sektion 702 eller E.O. 12 333, sammenholdt med Presidential Policy Directive-28 (PPD-28), opfylder EU-rettens proportionalitetskrav med den følge, at overvågningsprogrammer, der er baseret på disse bestemmelser, ikke kan anses for at være begrænset til det strengt nødvendige. Domstolen fastslog endvidere, at FISA 702 eller E.O. 12 333, sammenholdt med PDD-28, ikke giver de (europæiske) registrerede rettigheder, som kan håndhæves over for de amerikanske myndigheder ved domstolene.

Med andre ord opfylder ovennævnte amerikanske lovgivning ikke EU-rettens krav om proportionalitet ved indgreb i grundlæggende rettigheder, ligesom de (europæiske) registrerede ikke har adgang til effektive retsmidler, hvilket er blandt de fire essentielle europæiske garantier.

FISA 702 bemyndiger den amerikanske regering til at indhente oplysninger om "non-U.S. persons", der med rimelighed kan forventes at befinde sig uden for USA, med henblik på indsamling af "foreign intelligence information".[16] Det sker ved udstedelse af direktiver til "electronic communications service providers" om at udlevere eller foranstalte udlevering af personoplysninger, som leverandøren behandler.

Cloudleverandører anses typisk som "electronic communications service providers"[17] og kan derfor være genstand for sådanne direktiver i henhold til FISA 702.

For så vidt angår "U.S. persons" ("USP") er begrebet defineret i 50 U.S.C. § 1801(i) som:

> "A citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does

15 Se EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 43.3, 45-47 samt bilag 3 for nærmere om kravene til denne vurdering.

16 Se nærmere i 50 U.S.C. § 1881a.

17 Som defineret i 50 U.S.C. § 1881(b)(4).

not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

Med henblik på at iagttage kravet om indsamling af oplysninger om non-USP's "reasonably believed to be located outside the United States" har de relevante amerikanske retshåndhævende myndigheder udarbejdet målretningsprocedurer.

Af tidligere, afklassificerede målretningsprocedurer fremgår det, at myndighederne i sin vurdering af status som USP inddrager en række oplysninger fra egne og andre myndigheders datasæt. Det fremgår imidlertid også, at myndighederne – i mangel på specifik information (i) om målets status som en USP, (ii) om målet befinder sig uden for USA, eller (iii) i tilfælde hvor målets lokalitet er ukendt – vil antage, at målet er en non-USP, der befinder sig uden for USA.[18]

Idet en dansk organisation normalt vil behandle oplysninger om non-USP's, er det derfor Datatilsynets umiddelbare opfattelse, at en dansk organisations brug af cloudleverandører i USA normalt vil være inden for anvendelsesområdet af FISA 702 – og dermed omfattet af såkaldt "problematisk" lovgivning.

Du har herefter to muligheder, hvis du fortsat ønsker at benytte den pågældende cloudleverandør og dermed overføre personoplysninger til USA. Du skal enten **(i)** træffe supplerende foranstaltninger, der imødegår denne problematiske lovgivning, eller **(ii)** vurdere, om den pågældende lovgivning vil blive anvendt i praksis med hensyn til de oplysninger, du ønsker at overføre til leverandøren.

Ad supplerende foranstaltninger

Idet en amerikansk cloudleverandør almindeligvis vil være omfattet af FISA 702, er din første mulighed at træffe supplerende foranstaltninger som tillæg til det etablerede overførselsgrundlag i form af EU-Kommissionens standardkontrakt.

Det bemærkes i den forbindelse, at kontraktuelle og organisatoriske foranstaltninger almindeligvis ikke vil imødegå adgang til eller indsamling af personoplysninger af amerikanske retshåndhævende myndigheder til overvågningsformål.[19] Det vil derfor være nødvendigt at træffe supplerende tekniske foranstaltninger.

Af anbefalingerne fra Det Europæiske Databeskyttelsesråd fremgår en række eksempler på supplerende tekniske foranstaltninger, du kan træffe, samt tilhørende cases, der gennemgår implementering af disse foranstaltninger.[20]

Datatilsynet bemærker, at der alene er tale om eksempler. Du kan som den dataansvarlige frit implementere andre supplerende tekniske foranstaltninger forudsat, at du kan påvise og dokumentere, at foranstaltningerne sammen med overførselsgrundlaget samlet set sikrer den registrerede et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS.

Blandt de nævnte eksempler på supplerende tekniske foranstaltninger er det navnlig kryptering, pseudonymisering og såkaldt opsplittet behandling, der er relevante ved brug af cloudservices.

Hvis du benytter en cloudservice, hvor leverandøren er nødt til at have adgang til de overførte oplysninger i klartekst, kan Det Europæiske Databeskyttelses-

18 NSA Targeting Procedures (2019): https://www.intel.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Targeting_17Sep19_OCR.pdf

19 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 53.

20 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 79-97.

råd imidlertid for nuværende ikke anvise supplerende tekniske foranstaltninger, der effektivt vil sikre et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU.

Eksempel 6

En dansk virksomhed ønsker at benytte en SaaS-service fra en cloudleverandør i USA. Cloudleverandøren anses som en "electronic communications service provider" og er dermed omfattet af FISA 702.

Virksomheden har derfor vurderet, at det er nødvendigt at træffe supplerende tekniske foranstaltninger i tillæg til etablering af et overførselsgrundlag i form af indgåelse af EU-Kommissionens standardkontrakt.

Det fremgår af cloudleverandørens dokumentation, at personoplysningerne er krypteret, når de behandles af leverandøren. Virksomheden finder imidlertid anledning til at stille uddybende spørgsmål til implementeringen af denne kryptering.

Cloudleverandøren præciserer, at transmission af oplysningerne til og fra leverandøren er krypteret ("in transit"), ligesom oplysningerne er krypteret, når de opbevares af cloudleverandøren ("at rest").

På virksomhedens foranledning bekræfter cloudleverandøren, at oplysningerne ikke er krypteret, når virksomhedens medarbejdere aktivt benytter den pågældende SaaS-service ("in motion").

Der er i dette tilfælde ikke tale om en effektiv supplerende teknisk foranstaltning, idet cloudleverandøren, når SaaS-servicen benyttes, har adgang til oplysningerne i klartekst.

Eksempel 7

En dansk myndighed ønsker at udskifte sit eksisterende økonomisystem med et cloudbaseret system, der leveres af en finsk virksomhed.

For at kunne levere systemet benytter virksomheden en cloudbaseret infrastruktur fra en global hyperscale public cloudleverandør. Virksomheden har herunder indført supplerende tekniske foranstaltninger i form af filtrering af IP-adresser således, at oplysningerne, der behandles i systemet reelt ikke kan tilgås fra IP-adresser, der hidrører fra lande uden for EU/EØS. Det gælder såvel for data i hvile, i transit og i bevægelse. Denne type af foranstaltning kendes også som "geoblocking" eller "geofencing" og er traditionelt blevet benyttet til at begrænse adgangen til websites og tjenester til udvalgte lande.

Det fremgår af aftalevilkårene mellem den finske virksomhed og cloudleverandøren, at der kan ske overførsel af personoplysninger til en lang række tredjelande bl.a. i forbindelse med leverandørens servicering og support af infrastrukturen.

Der er i dette tilfælde ikke tale om en effektiv supplerende teknisk foranstaltning, idet virksomheden som kunde hos cloudleverandøren alene har adgang til og kontrol med sin egen infrastruktur, dvs. økonomisystemet, der er udviklet af virksomheden. Kontrollen med den underliggende infrastruktur er fortsat hos cloudleverandøren. Det er

dermed ikke udelukket, at cloudleverandøren i forbindelse med sin servicering af infrastrukturen kan få adgang til personoplysninger, der findes i økonomisystemet, fra et eller flere tredjelande, hvorfra serviceringen foretages.

Det kan også tænkes, at myndigheden i forbindelse med sin gennemgang af virksomhedens dokumentation konstaterer, at virksomheden har været opmærksom på denne problemstilling og derfor benytter sig af dedikeret infrastruktur hos cloudleverandøren, som er teknisk adskilt fra cloudleverandørens øvrige infrastruktur. Dette understøttes endvidere af aftalevilkårene med cloudleverandøren, hvoraf det fremgår, at kunden kan indgå aftale om dedikeret infrastruktur, som imidlertid indebærer en dårligere oppetidsgaranti, en højere pris og dårligere muligheder for support – med andre ord en "værre" SLA for kundens vedkommende.

Samlet set vil personoplysninger således i sidstnævnte tilfælde slet ikke blive overført til tredjelande, og kravene i databeskyttelsesforordningens kapitel V skal derfor ikke iagttages.

Eksempel 8

En dansk virksomhed har udviklet en applikation, hvor brugerne kan registrere og følge deres blodsukkerniveau. Virksomheden er en lille start-up og har ikke selv kapacitet til at imødekomme den kommende store efterspørgsel på applikationen, som virksomheden påregner. Virksomheden har derfor hostet applikationen hos en hyperscale public cloudleverandør. Cloudleverandøren garanterer, at oplysningerne vil blive opbevaret i EU, men kan ikke udelukke, at der vil ske overførsel af personoplysninger til tredjelande, fx i forbindelse med service og opgradering af infrastrukturen, som foretages af underleverandører i USA.

Virksomheden har derfor vurderet, at det er nødvendigt at træffe supplerende tekniske foranstaltninger i tillæg til etablering af et overførselsgrundlag i form af indgåelse af EU-Kommissionens standardkontrakt.

Virksomheden har vurderet, at kryptering er den mest passende supplerende foranstaltning og har tidligt i udviklingsprocessen taget højde for, at der skulle implementeres effektiv kryptering.

Kommunikationen er derfor krypteret hele vejen fra applikationen på tværs af alle servere, hvor oplysninger behandles ("in transit").

Derudover har virksomheden implementeret en særlig kryptering af oplysningerne i brug ("in motion") og i hvile ("at rest").

Virksomheden har indgået en separat aftale med en specialiseret svensk virksomhed, der har implementeret krypteringen og opbevarer krypteringsnøglen. Når brugeren registrerer oplysningerne i applikationen sker kommunikationen fra den danske virksomhed via den svenske leverandør, hvor de relevante behandlingsaktiviteter sker, inden oplysningerne krypteres og sendes videre til den amerikanske cloudleverandør i form af krypteret rådata. Når brugeren ønsker at læse oplysninger i applikationen, henter den svenske leverandør krypteret rådata fra cloudleverandøren og dekrypterer oplysningerne, hvorefter de sendes videre til brugeren.

I dette tilfælde er der efter Datatilsynets opfattelse tale om en effektiv supplerende teknisk foranstaltning, idet oplysningerne er krypteret ved hjælp af nøgler, der opbevares i EU, hvor oplysningerne krypteres, og det er alene krypteret rådata, der sendes til og fra cloudleverandøren i USA. Cloudleverandøren har dermed på intet tidspunkt adgang til oplysningerne i klartekst – heller ikke når brugeren aktivt bruger applikationen.

Ad anvendelse af loven i praksis

Alternativt kan du vælge at overføre personoplysninger til USA uden at implementere supplerende foranstaltninger, hvis du "ikke har nogen grund til tro, at den relevante problematiske lovgivning vil blive anvendt i praksis for så vidt angår de oplysninger, du overfører, eller den organisation, du overfører oplysningerne til."[21]

Som beskrevet ovenfor betragtes cloudleverandører i USA typisk som "electronic communications service providers", og en dansk organisations brug af sådanne cloudleverandører vil almindeligvis være omfattet af anvendelsesområdet for FISA 702.

Spørgsmålet er herefter, om de specifikke oplysninger, som du ønsker at overføre, i praksis vil være omfattet af FISA 702 mv.

Under de overvågningsprogrammer, der er autoriseret under FISA 702, sker indsamling af oplysninger om de relevante målpersoner ved hjælp af "selectors". Ofte fremhævede eksempler på "selectors" er e-mailadresser og telefonnumre.[22]

Derudover følger det af FISA 702, at oplysningerne, der kan indsamles i medfør af bestemmelsen, skal være "foreign intelligence information", der defineres[23] som:

> "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
> (B) the conduct of the foreign affairs of the United States."

Det fremgår derudover af tidligere, afklassificerede målretningsprocedurer for så vidt angår "foreign intelligence purpose", at myndighederne "med rimelighed skal vurdere – baseret på alle omstændigheder – at målet forventes at besidde, modtage og/eller sandsynligvis vil kommunikere udenlandsk efterretningsinformation vedrørende en fremmed magt eller fremmed territorium". Vurderingen skal foretages af en særligt uddannet medarbejder og skal være specifik, informeret og baseret på faktuelle omstændigheder.[24]

For så vidt angår "selectors" har Datatilsynet ikke været i stand til at identificere en udtømmende oversigt over, hvilke typer af "selectors" der benyttes af amerikanske retshåndhævende myndigheder.

Derudover er det med hensyn til definitionen af "foreign intelligence information" Datatilsynets opfattelse, at der er tale om en bred afgrænsning, og en dansk organisation vil – med få forbehold – almindeligvis ikke besidde de nødvendige forudsætninger for at vurdere, i hvilket omfang en eller flere typer af personoplysninger udgør "foreign intelligence information". Dette moment bidrager dermed efter tilsynets opfattelse ikke i sig selv til fastlæggelsen af, hvilke

21 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 43.3.

22 U.S. Privacy and Civil Liberties Oversight Board's report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, s. 7.

23 Se 50 U.S.C. § 1801(e)

24 NSA Targeting Procedures (2019): https://www.intel.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Targeting_17Sep19_OCR.pdf

typer af personoplysninger der vil være genstand for de overvågningsprogrammer, der er autoriseret under bl.a. FISA 702.

På den baggrund er det Datatilsynets umiddelbare opfattelse, at det vil være vanskeligt at dokumentere, at de konkrete typer af personoplysninger, som man ønsker at overføre til cloudleverandører i USA ikke vil være genstand for de overvågningsprogrammer, der er autoriseret under bl.a. FISA 702.

Datatilsynet udelukker ikke, at der kan være typer af personoplysninger, som i praksis ikke er genstand for de overvågningsprogrammer, der er autoriseret under bl.a. FISA 702. Datatilsynet forventer dog, at en dataansvarlig, der ønsker at overføre personoplysninger til cloudleverandører, der er omfattet af FISA 702 uden at træffe supplerende tekniske foranstaltninger, kan dokumentere, at de konkrete typer af oplysninger på baggrund af objektiv, troværdig og tilgængelig information ikke i praksis er genstand for de overvågningsprogrammer, der er autoriseret under FISA 702.[25]

Du kan i din dokumentation inddrage cloudleverandørens vurdering, men dette udsagn kan ikke stå alene og skal være understøttet af objektiv, troværdig og tilgængelig information.

Det er således ikke tilstrækkelig som dokumentation at henvise til sin egen – eller cloudleverandørens – subjektive vurdering af, at de personoplysninger, der vil blive overført, ikke kan målrettes via "selectors" eller har interesse for amerikanske retshåndhævende myndigheder, hvis dette udsagn ikke er understøttet af objektiv, troværdig og tilgængelig information, fx fra de omhandlede myndigheder.

Selv hvis de specifikke oplysninger, som du ønsker at overføre, reelt er omfattet af de overvågningsprogrammer, der er autoriseret under bl.a. FISA 702, kan du stadig – uden at træffe supplerende foranstaltninger – overføre oplysningerne til din cloudleverandør.

Det forudsætter dog, at din leverandør i praksis ikke tidligere har modtaget anmodninger fra amerikanske retshåndhævende myndigheder, eller hvis anmodningerne under alle omstændigheder ikke har omfattet de typer af oplysninger, som du påtænker at overføre.

Datatilsynet bemærker imidlertid, at du skal dokumentere, at (i) leverandøren ikke er underlagt et forbud om at oplyse om eksistensen af tidligere modtagne anmodninger, samt omfanget heraf, herunder med hensyn til typen af personoplysninger, der har været omfattet af anmodningerne.

Det er også dit ansvar som den dataansvarlige at kunne dokumentere, at eventuelle tidligere anmodninger, som din cloudleverandør har modtaget, ikke har omfattet de typer af personoplysninger, som du påtænker at overføre. Denne dokumentation skal ligeledes være baseret på objektiv, troværdig og tilgængelig information, og ikke alene din egen subjektive vurdering.

Eksempel 9

En dansk virksomhed ønsker at benytte en SaaS-service fra en cloudleverandør i USA. Cloudleverandøren anses som en "electronic communications service provider" og er således omfattet af FISA 702.

Der er tale om en SaaS-service, hvor cloudleverandøren til brug for levering af servicen har behov for adgang til oplysningerne i klartekst.

På baggrund af, at der hverken vil blive overført e-mailadresser eller telefonnumre, har virksomheden vurderet, at de overførte oplysninger sandsynligvis ikke vil være genstand for de overvågningsprogrammer, der er autoriseret under FISA 702. Virksomhedens vurdering er imidlertid ikke understøttet af yderligere dokumentation og

25 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, afsnit 44-46.

bygger derfor alene på virksomhedens subjektive vurdering af, at der er tale om oplysninger, der ikke vil blive målrettet af amerikanske retshåndhævende myndigheder.

Idet virksomheden har vurderet, at oplysningerne i praksis ikke er omfattet af "problematisk" lovgivning, har virksomheden undladt at træffe supplerende tekniske foranstaltninger.

Det vil i dette tilfælde ikke være lovligt for den danske virksomhed at overføre personoplysningerne til USA. Det skyldes navnlig, at virksomhedens vurdering af, hvorvidt oplysningerne vil være omfattet af overvågningsprogrammerne under FISA 702 alene er baseret på virksomhedens subjektive vurdering og ikke understøttet af yderligere objektiv, troværdig og tilgængelig information.

Eksempel 10

En dansk virksomhed ønsker at benytte en SaaS-service fra en cloudleverandør i USA. Cloudleverandøren anses som en "electronic communications service provider" og er således omfattet af FISA 702.

Der er tale om en SaaS-service, hvor cloudleverandøren til brug for levering af servicen har behov for adgang til oplysningerne i klartekst.

SaaS-servicen vil alene blive benyttet til at behandle oplysninger, der skal offentliggøres på virksomhedens hjemmeside.

Selvom oplysningerne formelt måtte være omfattet af anvendelsesområdet af de overvågningsprogrammer, der er autoriseret under FISA 702, er hovedformålet med overvågningsprogrammerne under FISA 702 at indhente signalefterretninger (SIGINT). Ved indsamling af offentligt tilgængelige oplysninger er der derimod tale om indsamling af open source efterretninger (OSINT).

Henset navnlig til, at oplysningerne er beregnet til at være offentligt tilgængelige, vil virksomheden efter Datatilsynets umiddelbare opfattelse kunne lægge til grund, at oplysningerne i praksis ikke vil være omfattet af anvendelsesområdet af de overvågningsprogrammer, der er autoriseret under FISA 702, og dermed lovligt kunne benytte den pågældende SaaS-service.

Det bemærkes dog, at der kan være behandling af personoplysninger, navnlig i SaaS-servicens back-end, som ikke vil være offentligt tilgængelige og dermed formelt og i praksis vil være omfattet af FISA 702.

Eksempel 11

En dansk virksomhed benytter en SaaS-service fra en cloudleverandør i et tredjeland. Virksomheden påtænker at overføre personoplysninger til cloudleverandøren på baggrund af EU-Kommissionens standardkontrakt. Cloudleverandøren er imidlertid omfattet af lovgivning i tredjelandet, der påvirker effektiviteten af den pågældende standardkontrakt.

Der er tale om en SaaS-service, hvor cloudleverandøren til brug for levering af servicen har behov for adgang til oplysningerne i klartekst.

Virksomheden har – på baggrund af de oplysninger, der påtænkes behandlet i servicen og dermed overført til cloudleverandøren – vurderet, at de konkrete overførte oplysninger ikke vil være genstand for den lovgivning, som cloudleverandøren generelt er omfattet af i tredjelandet.

Virksomhedens vurdering er understøttet af afklassificeret materiale fra tredjelandets retshåndhævende myndigheder, der udtømmende beskriver, hvilke oplysninger der er genstand for myndighedernes indsamling af oplysninger i henhold til den pågældende lovgivning, som cloudleverandøren er omfattet af.

I dette tilfælde vil virksomheden efter Datatilsynets opfattelse lovligt kunne overføre personoplysninger til cloudleverandøren uden at træffe supplerende tekniske foranstaltninger, da virksomheden kan dokumentere, at oplysningerne – på baggrund af objektive, troværdige og tilgængelige informationer – ikke er genstand for den problematiske lovgivning i tredjelandet.

Eksempel 12

En dansk virksomhed modtager et sæt helbredsoplysninger fra et amerikansk universitetshospital, som udelukkende vedrører amerikanske statsborgere. Virksomheder behandler oplysningerne ved at rense datasættet for datastøj (metodiske målefejl), hvorefter oplysningerne sendes krypteret tilbage til universitetshospitalet i USA med henblik på brug i patientbehandlingen.

Virksomheden behandler oplysningerne på vegne af universitetshospitalet som databehandler, og virksomheden er qua sin etablering i Danmark omfattet af databeskyttelsesreglerne. Virksomhedens "reeksport" af oplysninger til det amerikanske universitetshospital er derfor omfattet af forordningens kapitel V.

Virksomheden har som overførselsgrundlag indgået EU-Kommissionens standardkontrakt med det amerikanske universitetshospital. Virksomheden har derudover vurderet lovgivningen og praksis, som universitetshospitalet er omfattet af, og konkluderer, at universitetshospitalet generelt er omfattet af lovgivning, der påvirker effektiviteten af den indgåede standardkontrakt. Virksomhedens vurdering konkluderer imidlertid også, at den pågældende lovgivning ikke finder anvendelse for oplysninger om amerikanske statsborgere. Denne vurdering er understøttet af en rapport fra et anerkendt amerikansk universitet.

I dette tilfælde er det Datatilsynets opfattelse, at den danske virksomhed kan foretage "reeksport" af oplysningerne, da virksomheden har (i) etableret et overførselsgrundlag, og (ii) dokumenteret, at den lovgivning som universitetshospitalet er omfattet af – selvom lovgivningen i sig selv kan anses som problematisk – ikke i praksis anvendes på de oplysninger, der overføres til universitetshospitalet, og virksomhedens vurdering er underbygget af objektive, troværdige og tilgængelige informationer.

Eksempel 13

En dansk virksomhed benytter en cloudleverandør baseret i EU til brug for hosting af sit CRM-system. Cloudleverandøren er et datterselskab af et amerikansk moderselskab.

Af databehandleraftalen fremgår det, at cloudleverandøren behandler visse typer af metadata, som er personhenførbare, til egne formål (bl.a. kapacitetsfastlæggelse, sikkerhedshåndtering og forbedringer af servicen), herunder overfører oplysningerne til sit amerikanske moderselskab.

Cloudleverandøren er selvstændigt dataansvarlig for sin behandling af disse oplysninger til de ovennævnte formål og er derfor selv ansvarlig for at overholde databeskyttelsesforordningens kapitel V i forbindelse med sin overførsel af oplysningerne til USA.

Bemærk, at den danske virksomhed i dette tilfælde - inden behandlingen overlades til cloudleverandøren – skal vurdere, på hvilket retligt grundlag (videregivelseshjemmel)

virksomheden kan videregive de omhandlede metadata til cloudleverandøren til brug for leverandørens behandling af oplysningerne til egne formål.

3.6 Behandlinger, der foretages inden for EU/EØS af selskaber, der kan blive mødt med anmodninger fra myndigheder i tredjelande

I de tilfælde, hvor din cloudleverandør udelukkende behandler personoplysninger inden for EU/EØS, herunder også udelukkende benytter underdatabehandlere i EU/EØS, vil det som udgangspunkt ikke være nødvendigt for dig at forholde dig til reglerne i databeskyttelsesforordningens kapitel V.

Cloudleverandører, der er etableret i EU/EØS, kan dog – eksempelvis qua sin koncernstruktur – blive mødt med anmodninger fra tredjelandet, hvor virksomhedens moderselskab er etableret.

For cloudleverandører, hvor virksomhedens moderselskab er etableret i USA, vil det eksempelvis kunne være tilfælde ved anmodninger i henhold til US CLOUD Act.[26]

Det er ikke i sig selv ulovligt at bruge en cloudleverandør, der tilhører en koncern, hvor moderselskaber er underlagt lovgivning i sit etableringsland, som giver myndighederne kompetence til at kræve oplysninger udleveret fra de øvrige koncernforbundne selskaber, herunder selskaberne i EU/EØS.

For en konkretisering af problemstillingen henvises til et eksempel fra Datatilsynets vejledning om overførsel til tredjelande, som er gengivet nedenfor.[27]

Særligt om udlevering af personoplysninger efter anmodning fra myndigheder i tredjelande

En databehandler må kun behandle personoplysninger, herunder overføre oplysningerne til tredjelande, i det omfang den dataansvarlige har givet instruktioner om det i databehandleraftalen, eller det er krævet ifølge EU-ret eller medlemsstaternes nationale ret.

Hvis en databehandler i EU/EØS også er etableret i et tredjeland, kan databehandleren dog i nogle tilfælde blive mødt af en anmodning fra myndighederne i et tredjeland om udlevering af personoplysninger, som databehandleren behandler for den dataansvarlige.

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 anvendelse 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 overholdt. I den forbindelse bør den dataansvarlige anmode databehand-

26 Datatilsynet er bekendt med, at der er blevet fremført, at anden amerikansk lovgivning, herunder FISA 702, har ekstraterritorial virkning på samme vis som US CLOUD Act. Der er imidlertid for nuværende Datatilsynets opfattelse, at det ikke er klarlagt i praksis, om – og i hvilket omfang – bl.a. FISA 702 har ekstraterritorial virkning.

27 Datatilsynets vejledning om overførsel til tredjelande, s. 11.

leren om tydeligt 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 databehandleraftalen ved at overføre personoplysninger til et tredjeland mod den dataansvarliges 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.

Som det fremgår af pkt. 2 i ovenstående eksempel, er den ovennævnte problemstilling således efter Datatilsynets opfattelse et spørgsmål om passende behandlingssikkerhed, hvor du som den dataansvarlige bl.a. skal sikre, at personoplysninger ikke utilsigtet kommer til uvedkommendes kendskab.

Du skal i den forbindelse være opmærksom på, at hvis din (europæiske) cloudleverandør – som din databehandler – imødekommer en anmodning fra retshåndhævende myndigheder i et tredjeland, vil være tale om et brud på persondatasikkerheden for dit vedkommende. Det skyldes, at der i så fald sker en uautoriseret videregivelse af personoplysninger til den pågældende myndighed.

Det understreges imidlertid, at spørgsmålet om passende behandlingssikkerhed alene er begrænset til de tilfælde, hvor brugen af den pågældende cloudleverandør ikke i øvrigt på nogen måde indebærer tilsigtede overførsler af personoplysninger til tredjelande, herunder i forbindelse med service af leverandørens infrastruktur, levering af support til din anvendte cloudservice, adgang til infrastrukturen til brug for leverandørens kapacitetsstyring mv.

Eksempel 14

En dansk virksomhed ønsker at benytte en cloudservice til udsendelse af nyhedsbreve fra en amerikansk cloudleverandør.

Virksomheden vil i den forbindelse navnlig behandle oplysninger om de registreredes e-mailadresser samt oplysninger om de nyhedsbreve, der er blevet udsendt.

Servicen leveres af et europæisk datterselskab på baggrund af infrastruktur, der udelukkende befinder sig inden for EU/EØS. Der vil derved ikke ske nogen tilsigtet overførsel af personoplysninger til tredjelande.

I dette tilfælde er den amerikanske cloudleverandør omfattet af US CLOUD Act, hvorefter en cloudleverandør kan blive forpligtet til at *"preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or*

control, regardless of whether such communication, record, or other information is located within or outside of the United States."

Personoplysninger, der behandles af et europæisk datterselskab til en amerikansk cloudleverandør, betragtes i denne forbindelse som værende under det amerikanske selskabs "possession, custody, or control".

Virksomheden har derfor som led i sin generelle risikovurdering vedrørende behandlingssikkerhed forholdt sig til risikoen for de registrerede ved en eventuel udlevering af personoplysninger til amerikanske retshåndhævende myndigheder:

- Sandsynlighed: Virksomheden har konstateret, at cloudleverandøren i sine *Transparency Reports* har oplyst, at leverandøren årligt imødekommer et antal anmodninger i henhold til US CLOUD Act. På den baggrund har virksomheden vurderet, at det er SANDSYNLIGT (4)[28], at cloudleverandøren vil modtage en anmodning i henhold til US CLOUD Act.
- Konsekvens: Henset til typen af oplysninger, der vil blive behandlet ved hjælp af cloudservicen, er det virksomhedens vurdering, at konsekvensen for de registrerede ved, at amerikanske retshåndhævende myndigheder får udleveret oplysninger om e-mailadresse, og hvilke nyhedsbreve vedkommende har modtaget, vil være en oplevelse af stress og mistro/frygt. Konsekvensen vil dermed være LAV (2).

Virksomheden fastslår dermed, at den samlede risiko ved udlevering af personoplysninger i henhold til en US CLOUD Act anmodning er MIDDEL (8).

På den baggrund indgår virksomheden i en dialog med den europæiske cloudleverandør med henblik på, at der indføjes i aftalevilkårene, at cloudleverandøren, herunder det amerikanske moderselskab, skal anfægte anmodningen i videst muligt omfang i henhold til amerikansk lovgivning.

Virksomheden vurderer, at dette tillæg til aftalevilkårene vil udgøre en passende organisatorisk sikkerhedsforanstaltning, der nedbringer sandsynligheden for, at amerikanske retshåndhævende myndigheder faktisk modtager oplysninger i henhold til en US CLOUD Act-anmodning, til USANDSYNLIGT (2). Virksomheden vurderer herefter, at residualrisikoen for den pågældende hændelse er LAV (4).

I dette tilfælde vil virksomheden have fastsat passende sikkerhedsforanstaltninger med hensyn til den konkrete trussel og dermed opfylde sine forpligtelser i henhold til databeskyttelsesforordningens regler om behandlingssikkerhed.

28 Datatilsynet har i eksemplet taget udgangspunkt i evalueringskriterier på en skala fra 1-5 for så vidt angår både evalueringen af såvel sandsynlighed som konsekvens.

Vejledning om cloud

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk