Debatten om cloud er præget af misforståelser

Dette indlæg er først bragt** i Altinget **den 17. juni 2022: Indlægget nedenfor indeholder enkelte juridiske uddybninger af de holdninger, der fremgår af indlægget i Altinget.

Debatten om GDPR og brug af cloud-tjenester er i øjeblikket omgærdet af en vis mystik og forskellige udlægninger, der giver anledning til misforståelser. Jeg forsøger i dette indlæg at udrede trådene og sætte nogle ord på, hvordan jeg mener, at man skal forholde sig til brug af cloud-tjenester.

GDPR-reglerne om overførsel af personoplysninger til lande uden for EU/EØS (tredjelande) har givet anledning til en del "juridisk uro" siden den 16. juli 2020, hvor EU-domstolen afsagde dom i Schrems II-sagen.

Dette indspark i debatten tager udgangspunkt i, hvordan *jeg* ville rådgive en dansk virksomhed, der ønsker at anvende en global cloud-leverandør. Samtidig kan jeg forhåbentlig korrigere en række misforståelser om tredjelandsoverførsler og cloud-tjenester, som jeg mener er opstået på det seneste.

GDPR og cloud

Først en kort introduktion i tilfælde af, at GDPR ikke fylder hele din hverdag: Lidt firkantet sagt regulerer GDPR al indsamling, opbevaring, overførsel, deling osv. af personoplysninger (dvs. data om mennesker). GDPR indeholder blandt andet nogle meget restriktive regler for, hvornår sådanne personoplysninger må overføres til lande uden for EU/EØS, herunder USA.

Disse regler er relevante i forhold til store globale cloud-leverandører som Microsoft, Google, Amazon Web Services (AWS), Zendesk, Mailchimp og lignende. Der er dermed tale om regler, som næsten alle danske virksomheder er nødt til at tage stilling til, da det er vanskeligt (men ikke umuligt) at drive virksomhed i dag, uden at gøre brug af cloud-tjenester. Dertil kommer, at virksomheder er glade og tilfredse med de løsninger, som disse cloud-tjenester leverer.

Reglerne for overførsel af personoplysninger er imidlertid også præget af uklarheder og misforståelser. Domstole og myndigheder præciserer og justerer løbende på, hvordan reglerne skal forstås. Der allerede en proces i gang mellem EU og USA, der har til formål at gøre det hele lidt nemmere, men det betyder ikke nødvendigvis, at danske virksomheder er afskåret fra at bruge amerikanske cloud-tjenester i mellemtiden.

Kend dine dataoverførsler

Når man taler om overførsel af data til tredjelande, er første skridt, at du skal vide hvilke dataoverførsler der er tale om. Du skal med andre ord holde styr på, hvilke data du indsamler, hvordan du opbevarer dem og hvordan du forhindrer, at uvedkommende får adgang til dem.

Dette udgangspunkt gælder som sådan altid inden for GDPR, men er særligt relevant, når man taler om taler om overførsler til tredjelande uden for EU.

De fleste globale cloud-leverandører tilbyder i dag, at kunderne frit kan vælge, hvor i verden deres data opbevares. Det er altså dig – kunden – der bestemmer, om dine data skal opbevares inden for eller uden for EU's grænser. Det er dog allerede her, at billedet bliver mudret.

At overføre eller ikke at overføre...

Hvis du har valgt, at dine data opbevares inden for EU's grænser, skal du også undersøge, om cloud-leverandøren alligevel kan finde på at overføre dine data til lande uden for EU. Dette rejser et centralt spørgsmål, nemlig: Hvad er en "overførsel" af personoplysninger?

Den mest almindelige forståelse er, at data overføres, når det flyttes fra ét sted til et andet. Men i GDPR-sammenhæng anses det også for en overførsel, når data bliver *tilgået* (læst) fra en anden lokation. For eksempel, hvis en cloud-leverandørs teknikere i USA eller Indien tilgår data i forbindelse med support eller udvikling af cloud-tjenesten. Årsagen er, at data (teknisk set) også her flyttes midlertidigt fra eksempelvis en server til læserens computer. Disse overførsler kan vi kalde for "faktiske overførsler".

Hertil kommer de såkaldte "juridiske overførsler". En juridisk overførsel opstår, hvis en cloud-leverandør juridisk forbeholder sig retten til at overføre de pågældende data til lande uden for EU, for eksempel hvis dette er påkrævet af lovgivning eller en anmodning fra myndigheder – uanset om de pågældende data i praksis bliver overført.

Uro om overførsler

Disse juridiske overførsler har skabt en del uro på det seneste, blandt andet i kølvandet på Datatilsynets udtalelse vedrørende tilsigtede eller utilsigtede overførsler til tredjelande.

Udtalelsen er blevet udlagt i medierne af flere omgange, herunder i Computerworld den 13. april 2022, hvor udtalelsen bliver taget til indtægt for følgende: En "juridisk overførsel" svarer til en faktisk overførsel af personoplysninger, hvilket betyder, at der sker en overførsel af personoplysninger til et tredjeland i det øjeblik man anvender en cloud-leverandør, der forbeholder sig retten til at overføre disse data – uanset om data i praksis bliver overført.

Dette mener jeg dog ikke, at Datatilsynets udtalelse kan tages til indtægt for. Udtalelsen er alene en præcisering af, at hvis en databehandler overfører personoplysninger til et tredjeland, er der taler om en "overførsel" – og ikke et sikkerhedsbrud – hvis databehandleren har forbeholdt sig retten til at foretage en sådan overførsel.

Udtalelsen siger derimod ikke, at et sådan forbehold i sig selv udgør en overførsel af personoplysninger. Tværtimod fremgår det af udtalelsen, at der vil være tale om en overførsel, "*hvis og i det omfang [databehandleren] imødekommer en anmodning fra en offentlig myndighed i et tredjeland*", og at reglerne i GDPR kapitel V (om overførsler til tredjelande) skal overholdes "*hvis eller når [databehandleren] i henhold til instruksen foretager sådanne overførsler*" [mine understregninger].

Jeg finder det svært at læse ovenstående på andre måder, end at der skal ske en faktisk overførelse af personoplysninger, før der er tale om en "overførsel". Jeg mener derfor, at man – indtil Datatilsynet kommer en anden officiel udmelding – kan lægge til grund, at en "juridisk overførsel" ikke er en overførsel.

Kan du så bare lade stå til?

Nej – det kan du ikke. Anvender du en cloud-leverandør, skal du sikre dig, at leverandøren kan stille "nødvendige garantier" for, at der vil blive implementeret passende foranstaltninger der sikrer, at GDPR bliver overholdt.

Modsat udlægningen i visse medier, er der ikke tale om firkantede kontraktuelle garantier. Som det fremgår af vejledningen om dataansvarlige og databehandlere fra det Europæiske Databeskyttelsesråd, drejer spørgsmålet sig derimod om databehandlerens *ekspertviden*, *pålidelighed* og *ressourcer*, hvortil databehandlerens omdømme også kan tages i betragtning.

Du skal med andre ord foretage en risikovurdering af databehandleren, baseret på behandlings karakter, omfang, sammenhæng og formål, samt risikoen for fysiske personers rettigheder og frihedsrettigheder. Det er netop det Datatilsynet siger, når de henviser til artikel 28 i GDPR i de tre punkter, der fremgår til sidst i deres udtalelse. Dette betyder også, at sandsynligheden for og konsekvenserne ved, at databehandleren faktisk overfører personoplysninger om den registrerede, skal vurderes.

Hvis risikovurderingen viser, at der foreligger en ikke-acceptabel risiko, skal risikoen begrænses. Jeg gør i den forbindelse opmærksom på, at flere globale cloud-leverandører har indskrevet en nøjagtig procedure i deres databehandleraftaler for, hvordan anmodninger om udlevering af data håndteres. Jeg anbefaler at disse inddrages i risikovurderingen.

Det er således først hvis denne risiko ikke kan begrænses tilstrækkeligt, at du er forpligtet til at indstille brugen af cloud-tjenesten.

Hvad så nu?

Som sagt, så er det første vigtige skridt at få kortlagt dine dataoverførsler – og i relation til cloud-leverandører skal du kortlægge, hvilke cloud-leverandører du anvender, og hvordan du anvender dem.

Når du frem til, at cloud-leverandøren *faktisk* overfører ens data til lande uden for EU, skal du i gang med en større juridisk vurdering af disse dataoverførsler – nemlig en Transfer Impact Assessment (eller en "TIA", som beskrevet i EDBP's vejledning om tredjelandsoverførsler).

Men hvis cloud-leverandøren ikke foretager nogen faktiske overførsler til tredjelande, mener jeg, at du kan nøjes med at foretage en risikovurdering af cloud-leverandøren, hvor risikoen for sådanne overførsler tages i

betragtning.

Fagområder	IP og teknologi
Sektorer	Technology