Bilag til Indkaldelsescirkulæret

Til Økonomiudvalget

Schrems II-dommen og konsekvenser for Københavns Kommune

Resumé
EU-domstolens Schrems II-dom skærper kravene til myndigheder og virksomheder, som opbevarer og behandler persondata i en række lande uden for EU, herunder USA. Dommen påvirker derfor alle der anvender amerikanske cloudtjenester (fra fx Microsoft, Amazon eller Google) til persondata. De endelige konsekvenser af dommen er fortsat under afklaring hos myndighederne og der pågår forhandlinger mellem EU og USA. Såfremt der ikke findes en løsning, der muliggør fortsat brug af amerikanske cloudtjenester vil det kræve betydelige investeringer i ny it-infrastruktur. Sagen er til orientering.

Baggrund
EU-domstolen afsagde i juli 2020 dom i den såkaldte Schrems II-sag. Dommen fastslår at såfremt en virksomhed eller myndighed opbevarer eller behandler persondata uden for EU, skal en række forhold være opfyldt. Heriblandt skal det sikres, at data i al væsentlighed beskyttes på samme niveau, som hvis de var opbevaret eller behandlet inden for EU. Dommen betyder også, at USA nu betragtes som et såkaldt usikkert tredjeland ift. opbevare og behandle data. Dette betyder ikke, at persondata ikke kan opbevares eller behandles i USA, men dommen stiller nogle skærpede krav til måden, hvorpå det gøres.

På baggrund af dommen udsendte sammenslutningen af de europæiske datatilsyn (Det Europæiske Databeskyttelsesråd) i juni 2021 en række anbefalinger, hvoraf det fremgår, hvilke krav der gælder, hvis myndigheder og virksomheder fremadrettet vil opbevare eller behandle data i lande uden for EU, herunder USA.

Dommen har derfor blandt andet konsekvenser for myndigheder og virksomheder i Danmark, der anvender amerikanske cloudtjenester (fra fx Microsoft, Amazon eller Google). På trods af Det Europæiske Databeskyttelsesråds anbefalinger er der fortsat usikkerhed om, hvad der er muligt og hvilke konkrete tiltag, der er tilstrækkelige ved anvendelse af amerikanske cloudtjenester, da de nationale tilsynsmyndigheder og domstolene endnu ikke har truffet afgørelser på området. Dette har skabt usikkerhed på området, særligt i den offentlige sektor, og mange aktører afventer i

øjeblikket den snarligt forventede udgivelse af Datatilsynets vejledning til brug af cloud.

Problemstilling
I lighed med mange andre private og offentlige organisationer anvender Københavns Kommune amerikanske cloudtjenester og er derfor i høj grad berørt af denne problemstilling. Et eksempel på et system, der er baseret på en amerikansk cloudtjeneste, er Microsoft Office 365. Ud over de systemer der allerede er i brug, er der også en række systemer i pipeline, der afventer implementering.

Eksempelvis har Økonomiforvaltningen, på baggrund af en effektiviseringssag fra 2019, gennemført et udbud om at flytte kommunens it-infrastruktur til en cloudtjeneste. Udbuddet blev vundet af Atea, som anvender amerikanske Microsoft som underleverandør. På grund af Schrems II-dommen og den efterfølgende uklarhed om de præcise vilkår for at flytte kommunens it-systemer og it-infrastruktur til en amerikansk cloudtjeneste, blev projektet sat på pause i marts 2021. Økonomiforvaltningen har fremlagt et forslag til håndteringen af de økonomiske konsekvenser direkte afledt af projektforsinkelsen. Forslaget indgår i indkaldelsescirkulæret for 2023.

Derudover var der i kommunens It-Kreds enighed om ikke at igangsætte nye projekter, der indebærer at data opbevares eller behandles i bl.a. USA (se bilag 1A og 1B). Kommunens Databeskyttelsesrådgiver (DPO) har undervejs i hele forløbet løbende rådgivet forvaltningerne om Schrems II-problemstillingen, og Økonomiforvaltningen følger i fællesskab med kommunens DPO problemstillingen tæt og er i dialog med relevante myndigheder og leverandører om udviklingen på området.

Det er samtidig både KL's, Økonomiforvaltningens og DPO'en vurdering, at den overordnede problemstilling omkring lovligheden af at anvende amerikanske cloudtjenester ikke bør løses af den enkelte kommune, men at løsningen skal findes på nationalt eller EU-niveau, således at danske offentlige myndigheder har en fælles linje på området. Det er Økonomiforvaltningens forventning, at der vil blive fundet en løsning, da der efter forvaltningens opfattelse allerede er en høj grad af konstruktiv dialog med både leverandører og myndigheder på nationalt niveau og at alle parter har en interesse i at finde en løsning.

DPO'en har desuden d. 22. december 2021 fremsendt konkrete spørgsmål i relation til Schrems II-problematikken til Datatilsynet. Datatilsynet har efterfølgende kontaktet kommunen og meddelt, at den endelige vejledning om cloud er tæt på udgivelse og vil give svar på flere af kommunens spørgsmål. Hvis der er nogle af spørgsmålene, der ikke bliver besvaret i vejledningen, vil de blive besvaret særskilt. Det er forventningen,

at der kommer svar inden udgangen af januar, og Økonomiforvaltningen afventer derfor ligesom mange andre organisationer den kommende vejledning.

Sideløbende med drøftelserne med leverandører, forhandler EU-Kommissionen og USA om indgåelse af en ny politisk aftale, som fastlægger vilkårene for opbevaring og behandling af data i USA. Der er dog ikke sat en deadline for disse forhandlinger.

Økonomiske og forretningsmæssige konsekvenser
Det samlede billede af de potentielle økonomiske og forretningsmæssige konsekvenser af Schrems II er ikke endeligt opgjort. Der er dels igangværende projekter, der i lighed med cloudprojektet har måtte standse eller omlægge sine aktiviteter samt planlagte projekter, som er standset. Hvis eksisterende idriftsatte løsninger skal omlægges, er det vurderingen, det vil kræve meget store investeringer i både projektudgifter og infrastruktur. Dertil kommer konsekvenserne af et lavere/ændret it-sikkerhedsniveau, mindre forretningsmæssig agilitet og øget kompleksitet i infrastrukturen. Der er således også fra et it-sikkerhedsmæssigt synspunkt en række udfordringer ved at fravælge flere cloudtjenester, idet mange moderne løsninger kun udbydes som cloudtjenester, der i praksis indebærer behandlingen af persondata i USA.

Økonomiforvaltningen og kommunens DPO er løbende i dialog med forvaltningerne, da en række projekter er sat på hold, annulleret eller på anden måde berørt af problematikken. Økonomiforvaltningen er sammen med forvaltningerne i gang med at undersøge konsekvenserne yderligere og vil afrapportere om de økonomiske og forretningsmæssige konsekvenser til Økonomiudvalget forud for overførselssagen.

Hvad gør andre organisationer?
Generelt gælder det for offentlige myndigheder, at man på baggrund af en konkret vurdering af de enkelte systemer, fortsætter med at anvende nuværende systemer, men samtidig forholder sig afventende ift. at etablere nye systemer, der opbevarer eller behandler persondata i amerikanske cloudtjenester. Der er dog både i staten, kommuner og regioner eksempler på at nye systemer sættes i drift, da det i nogle tilfælde vurderes at den samfundsopgave myndigheden løser, ikke kan løses på en god måde uden at bruge amerikanske cloudtjenester.

Videre proces
Økonomiforvaltningen følger fortsat udviklingen i samarbejde med kommunens DPO. Der pågår endvidere fortsat erfaringsudveksling og sparring med andre offentlige organisationer samt kommunens leverandører.

På baggrund af de igangværende forhandlinger mellem EU og USA samt de ændringer, som cloudleverandørerne løbende laver, er det

Økonomiforvaltningens samlede vurdering, at en løsning på problemstillingen bør forventes at være på plads løbet af 2022, således at der igen under en række praktisk anvendelige forholdsregler vil kunne opbevares og behandles data i amerikanske cloudtjenester.

Bilag
Bilag 1A og 1B – DPO'ens notater omkring Schrems II

Notat

10. september 2021

Sagsbehandler

Databeskyttelsesrådgiveren

Schrems II-dommen

EU-domstolen har med Schrems II-dommen, underkendt den aftale der har dannet grundlaget for udveksling af personoplysninger mellem EU og USA. Aftalen hedder Privacy shield og måtte lide samme skæbne som sin forgænger, Safe Harbour, der i 2015 også blev erklæret ugyldig ved EU-domstolen. Dommen slår fast, at USA - på grund af sine vidtgående rammer for statslig overvågning - ikke kan stille et niveau af databeskyttelse, der svarer til det vi kender inden for EU med GDPR. Den beskyttelse som personoplysninger nyder inden for EU, skal følge personoplysningerne, uanset hvor i verden de befinder sig. Grundtesen er, at borgerne ikke skal have forringet deres databeskyttelse, blot fordi kommunen vælger en leverandør til at bistå os med fx et system.

EU-dommen betyder at USA nu betegnes som et *usikkert tredjeland*. Kommunen skal derfor selvstændigt foretage en vurdering af modtagerlandets lovgivning, for at fastlægge om de europæiske garantier for databeskyttelse er de samme, som dem der følger af GDPR – også kaldet en TIA (Transfer Impact Assessment). Det er netop denne vurdering som EU-domstolen har foretaget af USA's lovgivning, og er kommet frem til at niveauet af databeskyttelse og rettigheder for de registrerede for USA's vedkommende, ikke lever op til niveauet af beskyttelse som følger af GDPR.

Amerikansk lovgivning tillader deres efterretningstjenester, disproportionalt, at indsamle personoplysninger fra amerikanske selskaber og datterselskaber, også selvom datterselskabet har hovedsæde i EU. Dette desuagtet at personoplysningerne er "kommunens" samt at virksomhedens infrastruktur, eller serverer, eventuelt, står i EU. Lovgivningen er ligeledes skruet sådan sammen, at kommunen aldrig ville kunne blive oplyst om, hvorvidt personoplysningerne var blevet givet til en efterretningstjeneste fordi virksomhederne underlægges tavshedspligt.

Intern Revision
Suhmsgade 4, 2. sal
1125 København K

EAN-nummer
5798009809964

Lande inden og udenfor EU

I databeskyttelsessammenhæng kategoriserer man lande i tre kategorier:

- lande indenfor den europæiske union og EØS
- "sikre" tredjelande og
- "usikre" tredjelande.

Lande indenfor den europæiske union skal følge reglerne i databeskyttelsesforordningen (GDPR). Her er borgerne sikret en god databeskyttelse, som følge af reglerne i GDPR.

Sikre tredjelande, er lande, hvor EU-Kommissionen har godkendt det pågældende tredjeland som "sikkert" ved en såkaldt "tilstrækkelighedsafgørelse". Det betyder, at EU-Kommissionen har foretaget en juridisk vurdering af landets nationale lovgivning og derved sikret, at der ikke sker forringelse af EU-borgernes databeskyttelse i forhold til reglerne i GDPR. Har et land status af "sikkert tredjeland" kan man som udgangspunkt overføre personoplysninger til landet uden problemer.

Usikre tredjelande er lande, hvor Europa-Kommissionen ikke har truffet en tilstrækkelighedsafgørelse. Derfor er det op til dataansvarlige selv at vurdere tredjelandets beskyttelsesniveau. Det er et omfattende arbejde og udgangspunktet er, at det er den dataansvarlige, der har bevisbyrden. Har et land status af "usikkert tredjeland" – kan man ikke overføre personoplysninger til landet, inden man har sikret et såkaldt effektivt overførselsgrundlag.

TIA (transfer impact assessment)

Hvis man foretager en overførelse til et "usikkert" tredjeland, skal man vurdere, hvorvidt landet har et tilstrækkeligt beskyttelsesniveau, som det der er gældende indenfor EU/EØS. Den undersøgelse kaldes en TIA (transfer impact assessment).
Undersøgelsen betragtes som meget omfattende og det er ikke noget man laver på 2xA4-sider eller en serviet.
Et tredjelands lovgivning kan fx godt indikere, at der ikke umiddelbart er nogen problemer i den nationale lovgivning, men undersøgelsen skal også vise, om den reelt set efterleves.

Når du har udarbejdet din TIA, vil du stå med to muligheder:

1. Overførelsen kan igangsættes eller fastholdes
2. Eller forsøg at træffe supplerende foranstaltninger.

Supplerende foranstaltninger

Supplerende foranstaltninger betyder, at man forsøger at afhjælpe eventuelle utilstrækkeligheder i beskyttelsesniveauet i et usikkert tredjeland. Det kan fx være tekniske, organisatoriske eller kontraktuelle foranstaltninger, der højner databeskyttelsesniveauet til det der er gældende indenfor EU/EØS. Dette gælder f.eks. hvis man har leverandører fra USA. Det er vigtigt at pointere, at foranstaltningerne skal være effektive i praksis og ikke blot på papiret.
Hvis der ikke kan træffes tilstrækkelige effektive supplerende foranstaltninger, skal overførslen stoppes.

Databeskyttelsesrådgiverens anbefaling

Det er vores opfattelse, at problematikken i KK kan deles i tre grupper:

1. Igangværende overførsler til usikre tredjelande
2. Igangsættelse af nye overførsler, nye behandlinger og ændringer, eller udvidelser af eksisterende overførelser.
3. KK´s Cloudprojekt.

Den videre proces i KK i forhold til de tre grupper er efter vores opfattelse:

1. Der udarbejdes TIAére jævnfør henstillingerne fra Datatilsynet. KIT og Databeskyttelsesrådgiveren tilrettelægger en proces i overensstemmelse med drøftelserne i IT-kredsen. Forvaltningerne bør afvente denne proces.
2. KK bør ikke påtage sig yderligere risici ved foretage ændringer, eller udvidelser, af eksisterende overførelser eller igangsætte nye behandlinger, der medfører en forøgelse af risikoen ved overførsel til usikre tredjelande. Det er Databeskyttelsesrådgiverens opfattelse, at det vil være uansvarligt såfremt forvaltningerne bevidst øger risikoen ved yderligere overførsel eller behandling i usikre tredjelande. Det henstilles, at forvaltningerne, samt KIT inddrager eller orienterer Databeskyttelsesrådgiveren såfremt forvaltningerne mod forventning øger kommunens risiko i forbindelse med overførsel til tredjelande.
3. Cloudprojektet er ganske fornuftigt sat på hold, indtil videre.

Endelig anbefales, at der udarbejdes en "defence file" der beskriver, hvordan KK har forholdt sig ansvarligt til Schrems II problematikken.

Notat til IT- Kredsen

25. november 2021

Sagsbehandler

Databeskyttelsesrådgiveren

Schrems II-status i Københavns Kommune

EU-dommen udfordrer mange af kommunens nye tiltag på digitaliseringsområdet. I flere tilfælde kan de ikke gennemføres, da leverandørerne overfører data til USA og ikke kan sikre et tilstrækkeligt beskyttelsesniveau. Selvom det er udfordrende på mange måder, skal der være tillid til at Københavns Kommune, som offentlig virksomhed, kan passe på borgernes data.

Efter aftale med ØKF har vi udarbejdet dette notat for at give en status og beskrive omstændighederne og mulighederne som følge af Schrems II.

Den 16. september henstillede Databeskyttelsesrådgiveren overfor ITK, at

- Københavns Kommune ikke, påtager sig yderligere risici ved at foretage ændringer, eller udvidelser, af eksisterende overførelser eller igangsætte nye behandlinger, der medfører en forøgelse af risikoen ved overførsel til usikre tredjelande.

Det blev ligeledes anbefalet, at

- der udarbejdes en *defence file*, som beskriver, hvordan Københavns Kommune har forholdt sig ansvarligt til Schrems-II-sagen.

Endelig blev det aftalt, at

- at forvaltningerne samt KIT inddrager eller orienterer DPO'en, såfremt forvaltningerne mod forventning øger Københavns Kommunes risiko i forbindelse med overførsel til tredjelande.

- På baggrund af notatet i ITK den 16. september 2021, blev Schrems problematikkerne berørt meget overordnet og det var grundlaget for, at Københavns Kommune fik indført mere bestemte retningslinjer.

Intern Revision
Suhmsgade 4, 2. sal
1125 København K

EAN-nummer
5798009809964

Nuværende status
På baggrund af mødet i ITK den 16. september godkendte DCK den 11. oktober, forretningsgangen for vurderinger af overførsler til usikre tredjelande som følge af Schrems II.

Forretningsgangen sikrer, at Databeskyttelsesrådgiveren, bliver involveret i forvaltningernes overvejelser og vurderinger, inden de foretager sig noget konkret.

På nuværende tidspunkt er Databeskyttelsesrådgiveren blevet involveret i 10 tilfælde, hvor forvaltningerne ønskede en vurdering af hvorvidt det var muligt at foretage overførelser af personoplysninger til et usikkert tredjeland, udelukkende USA.

I alle tilfældene har Databeskyttelsesrådgiveren anbefalet at man på nuværende tidspunkt ikke igangsætter overførslen.

Proces hos Databeskyttelsesrådgiveren
Databeskyttelsesrådgiveren vurderer alle sager på objektivt grundlag. Vi ser således på:

1) Overføres der personoplysninger
2) Hvorvidt der er udarbejdet en sandsynlighedsvurdering, eller om
3) Der truffet tilstrækkeligt supplerende foranstaltninger og eventuelt

Hvis der overføres personoplysninger, er der to muligheder, hvor én skal være opfyldt, før en overførelse til et usikkert tredjeland, kan ske.

1) Man kan på baggrund af en omfattende sandsynlighedsvurdering redegøre for, hvorfor eventuelt problematisk lovgivning ikke har praktisk betydning ift. den behandling man ønsker at igangsætte
2) Der skal være truffet tilstrækkeligt supplerende foranstaltninger, eller

Vi har endnu ikke set tilfælde, hvor der bekræftende har kunnet svares "ja" til punkt 2 eller 3.

Ad. 1.
Denne vurdering er anses for meget omfattende og kræver udførlig dokumentation på baggrund af objektive kriterier og pålidelige kilder. Vurderingen må således ikke udelukkende være kommunens egen, leverandørens, eller begges i sammenslutning. I forhold til USA betyder det, at vurderingen skal kunne udelukke fx at en amerikansk efterretningstjeneste aldrig har haft, eller vil kunne tænkes af få interesse i de personoplysninger man ønsker at overføre til USA. Det er en svært beviselig øvelse, hvor man vil derfor blive nødt til at se på tidligere og nuværende praksis, nationens lovgivning, inddragelse af uvildige rapporter m.v.

I forhold til USA betragter databeskyttelsesrådgiveren det meget problematisk at lave denne vurdering og vi har endnu ikke set eksempler på en vurdering, som løfter opgaven. De eksempler vi har stiftet bekendtskab med, har alene været en risikovurdering understøttet af leverandørens mening og holdninger. Det er vigtigt at understrege, at en risikovurdering aldrig vil kunne opfylde de nødvendige kriterier af, hvorvidt problematisk lovgivning ikke har praktisk betydning ift. den behandling man ønsker at igangsætte. En sandsynlighedsvurdering og risikovurdering er to forskellige ting.

Ad. 2.
Supplerende foranstaltninger betyder, at man forsøger at afhjælpe eventuelle utilstrækkeligheder i beskyttelsesniveauet i et usikkert tredjeland. Det kan fx være tekniske, organisatoriske eller kontraktuelle foranstaltninger, der højner databeskyttelsesniveauet til det der er gældende indenfor EU/EØS

Ud fra de konkrete sager, hvor vi har været involveret, viser det tydeligt, at mange leverandører tror at det er tilstrækkeligt, at der bliver foretaget kontraktuelle foranstaltninger mellem kommunen og leverandøren. Dette er ikke tilfældet og kontraktuelle foranstaltninger vil aldrig kunne stå alene. De binder nemlig kun eventuelle aftaleparter, og vil, i tilfælde som med USA, ikke kunne påvirke en national myndighed.

Det er Databeskyttelsesrådgiverens vurdering, at der således skal være etableret tilstrækkeligt tekniske foranstaltninger før man kan overføre personoplysninger til et usikkert tredjeland. De eneste tekniske foranstaltninger vi på nuværende tidspunkt ser mulige, er igennem tilstrækkelig kryptering. Vi har endnu ikke set nogle løsninger, hvor det er muligt at kryptere oplysninger i så tilstrækkelig grad, at løsningen anses for mulig.

Idet de tekniske foranstaltninger er meget begrænset, og ofte ikke mulige, bliver den eneste tilbageværende mulighed at vurdere den praktiske betydning af problematisk lovgivning.

Andet

Vi erfarer ofte, at det bliver nævnt "at andre må, hvorfor kan vi så ikke"? Dette kan der være mange grunde til, dels at dem der gør det, kan være private virksomheder, som bl.a. kan overføre personoplysninger til fx USA på baggrund af samtykke eller at det mellem en eller flere koncern sammenhængende enheder.

Vi hører ligeledes, "at andre kommuner gør det". Dette kan der også være gode grunde til, dels at:

- overførslen er sket før Schems II afgørelsen 16. juni 2020
- der ikke har været tilstrækkeligt styr på interne retningslinjer
- man har ikke forholdt sig til databehandlerkonstruktionen m.v. inden aftale indgåelsen

Vi har endnu ikke hørt om en årsag der er forbundet med, at man har løst den overordnede problematik ift. tredjelandsoverførelser.

Det man ligeledes skal være opmærksom på er, at blot forbi man i nogle situationer allerede overfører personoplysninger til fx USA vil det ikke være ensbetydende med, at man kan forsætte med det. Alle eksisterende løsninger, systemer m.v., hvor der sker overførelse af personoplysninger til et usikkert tredjeland, skal opfylde samme krav, som hvis der foretager ændringer, eller udvidelser af eksisterende overførelser eller igangsættelse nye behandlinger. Det betyder at de skal opfylde præcis de samme krav til tredjelandsoverførelser og at de på nuværende tidspunkt ikke er ulovlige. Da vi indgik disse aftaler, var vi i god tro. Det er vi ikke længere, derfor vil det også være forbundet med stor kritikalitet, hvis vi fx begynder at lægge nye løsninger hen over eksisterende systemer eller gør noget, der ændre på det oprindelige udgangspunkt, idet man bygger oven på en allerede ulovlig overførelse.

Det er ligeledes værd at holde for øje, at informationen omkring tredjelandsoverførelser skal indgå i oplysningspligten til de registrerede. Er de derfor blevet oplyst, at kommunen ikke overfører deres personoplysninger til fx USA, og begynder man pludselig på det, så skal de registrerede oplyses om det.

Orientering ift. Datatilsynet

Indledningsvist kan vi oplyse, at Datatilsynet er påbegyndt deres tilsyn med tredjelandsoverførelser. Vi har fået indsigt i deres umiddelbare spørgeramme, det er bl.a.:

- En beskrivelse af deres retningslinjer / procedurer m.v. for deres efterlevelse af forordningens kapitel 5,
- En oversigt over de overførsler af personoplysninger til tredjelande som de foretager, herunder hvilke kategorier af personoplysninger samt destinationerne for de overførte oplysninger
- En oversigt over hvilke overførselsgrundlag i forordningens kapitel 5, de anvender til brug for de enkelte overførsler.

Vi har på nuværende tidspunkt hørt at Varde og Esbjerg kommune er omfattet af tilsynet.

Databeskyttelsesrådgiveren følger udviklingen omkring Schrems II på tæt hold og vurderer løbende hvis der kommer ny viden og holder kredsen af it-direktører opdateret.