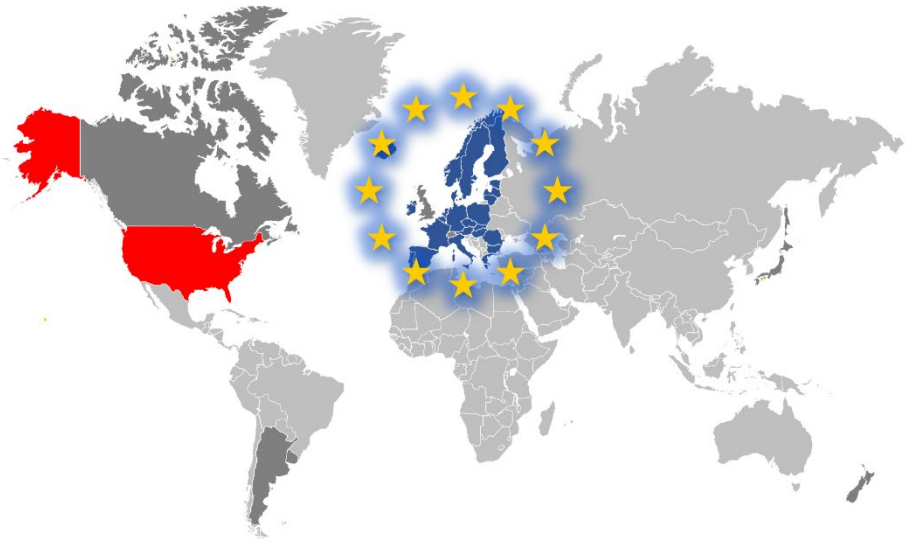


Overføring av personopplysninger utenfor EØS – hva gjør vi etter Schrems II?

I juli 2020 ble den såkalte Schrems II-dommen avsagt i EU-domstolen. Dommen fastslo at Privacy Shield var ugyldig som overføringsgrunnlag til land utenfor EØS (såkalte tredjeland). I tillegg ble det stilt krav til bruk av EUs standard kontraktsbestemmelser (EC Standard Contract Clauses eller SCC) som overføringsgrunnlag til tredjeland.

For Privacy Shield var det enkelt; her var det full stopp. Om og hvordan dagens SCC kan brukes som overføringsgrunnlag etter dommen, er langt mer vanskeligere. I november 2020 kom EUs personvernråd (EDPB) med veiledere for bruk av SCC, som ikke gjorde det så mye enklere. Nedenfor skal det gis en oversikt over bruk av SCC etter dommen og veilederen, og også forslag til nye SCCer skal gjennomgås.

1 Bakgrunn og oversikt

Schrems II-dommen gjaldt kun overføring til USA, men siden dommen også behandlet bruk av EUs standard kontraktsbestemmelser (SCC) som overføringsgrunnlag får dommen også betydning for overføring til andre land utenfor EØS (tredjeland).

Ved overføring av personopplysninger til tredjeland, kreves det et eget grunnlag for overføringen, som finnes i GDPR kapitel V. Det er altså *ikke* tilstrekkelig med kun databehandleravtale om overføring til tredjeland skal skje.

SCC er det mest praktiske grunnlaget for overføring, og siden så godt som alle virksomheter i Europa benytter en leverandør/databehandler i tredjeland, så vil Schrems II-dommen ha meget stor betydning.

Etter dommen kreves det at om en overføring til tredjeland skal være lovlig, så må det vurderes om overføring kan skje ut fra hvilken beskyttelse landets lovgivning gir for

personopplysningene som overføres. Gir ikke landet tilstrekkelig beskyttelse, så må det iverksettes nødvendige tiltak for å sikre personopplysningene.

EDPB har laget veiledninger for vurderingen av lovgivningen i tredjelandet og om de tiltakene som kan være aktuelle for å sikre personopplysninger i tredjelandet. Denne artikkelen går gjennom kravene etter dommen og veiledningene fra EDPB.

2 Prosedyre – vurdering om overføring kan skje

I veiledning fra EDPB er det tatt anbefalt en prosedyre for å sikre at overføring skjer etter på riktig måte og at de nødvendige vurderinger gjøres. Nedenfor er en oversikt over prosedyren og nødvendige vurderinger, samt eventuelle tiltak som må gjøres.

Gjennomføring av enkelte ledd i prosedyren og vurderinger som gjøres etter denne, må dokumenteres (dvs. det må kunne vises at det er gjennomført, og den beste måten er å gjøre vurderingen skriftlig). Som et hjelpemiddel for gjennomføring av prosedyren og vurderingen har jeg tatt laget et arbeidsdokument, som finnes her. Arbeidsdokumentet er kun et eksempel og andre måter å dokumentere prosedyren kan velges.

Merk at EDPB anbefaler at vurdering om overføring skal foretas for *hver* overføring, og skal fortrinnsvis gjøres *før* overføring gjennomføres, om mulig, eller før overføring fortsetter (innen en rimelig tid).

I det følgende benyttes det «databehandler» for den som behandler personopplysninger i tredjeland som fellesbegrep som også omfatter «dataimportør», «leverandør», «tredjelandsmottaker» mv., og selv om det også kan foretas overføring av personopplysninger til andre behandlingsansvarlige.

For den som overfører personopplysninger til tredjeland fra EØS, brukes «behandlingsansvarlig», som også omfatter «dataeksportør», «kunde» mv.) og selv om det også kan skje eksport fra databehandler lokalisert innenfor EØS (etter fullmakt eller etter de nye SCCene).

2.1 Hvilke personopplysninger overføres til tredjelandet?

For å kunne vurdere overføringene til tredjelandene, er det nødvendig å få en oversikt over hvilke personopplysninger som overføres, til hvilken mottaker og til hvilket tredjeland det overføres til.

En slik kartlegging kan ta utgangspunkt i databehandleravtaler som er inngått, samt behandlingsoversikten (protokollen) som skal lages etter GDPR artikkel 30. I tillegg bør det undersøkes dataflyt som skjer i virksomheten, hvor det kan avdekkes overføringer som ikke er dekket av databehandleravtaler eller behandlingsoversikten. Det kan her være nødvendig å kontakte databehandlerne for å avklare hvordan og hvor personopplysningene behandles.

Også underdatabehandlere (underleverandører) til databehandlere som også behandler personopplysninger er bør kartlegges, siden det er *alle* overføringer til tredjeland av ens egne personopplysninger som behandlingsansvarlig som omfattes. Er man databehandler, så er det sannsynlig at behandlingsansvarlige vil ønske en oversikt over overføring til tredjeland, så databehandlere bør også gjøre kartleggingen for egen del og knyttet til kunder.

Foretas behandlingen innenfor EØS, dvs. personopplysningene lagres og behandles uten å bli overført til tredjeland, så vil det ikke være nødvendig å foreta resten av prosedyren nedenfor. Men man skal være klar over at mange databehandlere forutsetter overføring til tredjeland selv om de hevder at det ikke skal skje (sjekk databehandleravtalene og

personvernerklæringene til databehandler). Er det tatt inn i databehandleravtalen at overføring skal kunne skje etter lovlig grunnlag som SCC, og databehandleravtalen inneholder andre referanser til SCC eller overføring, som at SCC er et bilag til avtalen, bør det undersøkes nærmere om overføring skjer selv om databehandler hevder noe annet.

Også tilgang (som fjerntilgang) til personopplysninger fra tredjeland anses som overføring, selv om opplysningene er innenfor EØS. Har f.eks. support mulighet til å gå inn i systemet hvor personopplysningene lagres innenfor EØS, er dette også en overføring til tredjeland.

Man må derfor også vurdere selskap som har infrastruktur (som at support håndteres fra tredjelandet). Dette følger av kravene til valg av forsvarlig databehandler etter GDPR artikkel 28. Lokalisering av personopplysningen kan derfor ha liten betydning. Se mer om Datatilsynets forståelse.

Skjer all behandling innenfor EØS, kan følgende punkter være til veiledning om overføring og bruk av leverandør kan benyttes:

1. Alle personopplysninger behandles (virkelig) innenfor EØS. Det må ikke være noen metadata eller annet som overføres ut av EØS.
2. Leverandøren er selskap som er registrert og etablert innenfor EØS (selv om det er eid av amerikansk selskap)
3. Det er ingen tilganger til personopplysninger eller administrasjonstilganger til systemer som behandler personopplysninger fra tredjeland
4. Det foretas revisjon av ekstern og uavhengig at ovennevnte overholdes.

Trolig trengs ikke alle punktene ovenfor, men de kan gi en viss veiledning.

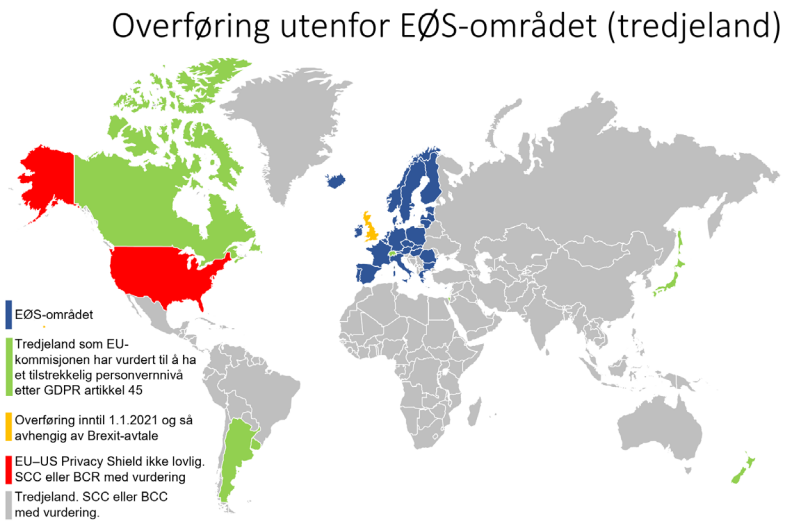
For å få full oversikt, kan det være nødvendig å kontakte databehandlerne for å avklare bl.a. hvor data overføres og hvor data behandles og lagres. Dette kan være en vanskelig overfor de store databehandlerne, og man må ofte basere seg på informasjon på databehandlernes nettsider. Her er det til gjengjeld mye informasjon, og vanskelig å finne det som har betydning. Enkelte databehandlere har heller ikke forståelse for at det skal iverksettes tiltak, og enkelte mener til og med at Privacy Shield er tilstrekkelig siden amerikanske myndigheter har fortsatt med ordningen, som kan skape ekstra utfordringer.

2.2 Hvilket grunnlag skjer overføringen på?

Som en del av kartleggingen ovenfor, så må det også avdekkes hvilket grunnlag etter GDPR artikkel 46 overføringen skjer etter.

Er det Privacy Shield, så må overføringen stanses umiddelbart ifølge dommen. Er det SCC, så må man gå gjennom prosedyren og foreta vurderingen som beskrevet her. Merk at det er foreslått nye SCCer, se punkt 3.2 nedenfor. Gjennomgang av prosedyren og vurderinger gjelder også for bindende virksomhetsregler (BCC) og enkelte andre grunnlag, hvor det også kreves vurderinger, men det gjennomgås ikke her.

Er det overføring til godkjent tredjeland, så kan overføringen fortsette. Se oversikt over godkjente tredjeland her:



2.3 Tilstrekkelig sikringen av personopplysninger etter lovgivningen i tredjelandet?

Det skal gjøres en vurdering av om lovgivningen i tredjelandet sikrer personopplysninger i tilstrekkelig grad. Gullstandarden dette skal vurderes opp mot er nivået i EØS, og da selvsagt GDPR.

Det er kommet en egen veileder fra EDPB om dette temaet, og momenter som kan benyttes i denne vurderingen er tilsvarende som de momentene som er tatt inn nedenfor under punkt 2.4 om aktuelle tiltak. I tillegg er det oppstilt fire grunnleggende krav til personvern som gjelder ved vurdering av behandlingen i tredjelandet:

- Behandlingen skal baseres på klare, presise og tilgjengelige reguleringer i lov mv.
- Behandlingen skal være nødvendig og proporsjonal knyttet til de legitime formål som forfølges.
- Det skal være en uavhengig kontrollmyndighet i landet som fører tilsyn med behandlingen.
- Den registrerte (dvs. den personopplysningene gjelder) skal ha rett til at få prøvet sine rettigheter, som ved en domstol.

For denne vurderingen så kan kontakt med databehandler i tredjeland også være aktuelt, men databehandlerne er normalt heller ikke i stand til å vurdere nivået på personvernlovgivningen (og i enda mindre grad mot nivået innenfor EØS).

En slik vurdering er veldig vanskelig, som de færreste (selv de som arbeider mye med personvern) vil klare å gjøre. Det er illustrerende at EU-kommisjonen brukte selv over to år på å vurdere personvernnivået i Japan, slik at behandlingsansvarlige eller databehandleren selv skal foreta en forsvarlig vurdering er nær utenkelig. Det er derfor merkelig at det ikke er gjort en vurdering av enkelte aktuelle lands lovgivning hvor det er store databehandlere (som India, Australia, Brasil mv.), men EDPB/EU-kommisjonen har kanskje funnet at dette er en for stor jobb, så den er skjøvet over på de som skal overføre personopplysningene. Det kan være at en slik liste kommer senere.

En vurdering er imidlertid klar: Etter Schrems II-dommen, så ble USA ansett for å ikke ha et tilstrekkelig personvernnivå, så her må vurderingen nedenfor uansett gjennomføres.

Det skal kun gjøres en objektiv vurdering, som om at det foreligger lovgivning som gjør at myndighetene kan pålegge utlevering av opplysninger eller det har skjedd at myndighetene har krevd utlevering, enten fra den aktuelle databehandler, av denne typen databehandler eller generelt i landet som er relevant for overføringen. Subjektive forhold har ikke betydning, som om det er sannsynlig at det kan kreves utlevering fra den som mottar opplysningene i tredjelandet (som en databehandler).

Er lovverket praktisk sett tilsvarende som på EØS-nivå, så kan overføring skje. Finner man at tredjelandet ikke har tilstrekkelig personvernnivå, så skal man fortsette prosedyren nedenfor. Vurderingen av landets personvernnivå er som sagt vanskelig, så som regel er det eneste alternativ å gå videre i prosedyren nedenfor.

2.4 Vurdere ytterligere tiltak

Er sikringen av personopplysningene etter lovgivningen i tredjelandet ikke tilstrekkelig, så skal det som nevnt vurderes om kan gjøres tiltak som i praksis kan sikre behandlingen tilvarende som innenfor EØS.

Tiltakene kan enten gjennomføres av behandlingsansvarlig, som da er innenfor EØS, og/eller mottakeren i tredjeland. Det er imidlertid mest sannsynlig at tiltakene må gjøres hos mottakeren i tredjelandet, som innebærer det må undersøke eller samarbeides med mottakeren i tredjelandet om tiltakene som må iverksettes.

For å vurdere hvilke tiltak som kan være aktuelle, så kan disse momentene ha betydning:

- Hvilke kategorier personopplysninger som skal overføres, og hvor sensitive opplysningene er vil ha betydning (som at de er særlige kategorier personopplysninger som stiller ekstra krav til og grunnlag for overføring).
- Hvem er de registrerte, dvs. hvem gjelder opplysningene, som f.eks. ansatte, kunder, sluttbrukere (privatpersoner), barn, pasienter mv.
- Hvor omfattende opplysningene er, enten ved at det gjelder mange personer og/eller det er omfattende opplysninger per person.
- I hvor lang periode skal behandlingen skal skje, når opplysningene da skal slettes og hvor sikker slettingen er.
- Hva formålet med overføringen er, som f.eks. markedsføring, HR, teknisk (som sikkerhetskopier, redundans), support, mv.
- Forholdet mellom behandlingsansvarlig innenfor EØS og databehandler i tredjelandet, som at de er del av samme konsern, samarbeid over tid, bundet av avtaler med sanksjoner som forplikter mv.
- Hvor kompleks er overføringen er, som om overføring skal gjøres av flere leverandører/-databehandlere, gå gjennom flere tredjeland, om det er sannsynlig at opplysningene videreoverføres fra tredjelandet som antas å være destinasjonen mv.
- Hvor kompleks er behandlingen i tredjelandet, som at det skal skje en sammenstilling av opplysninger, innhenting av ytterligere opplysninger basert på opplysningene som overføres mv.
- Hvor mange aktører er involvert i selve behandlingen, som at det er flere behandlingsansvarlige, flere databehandlere, underleverandører i flere ledd, om det er sannsynlig med videreoverføring til andre aktører mv.

- Hvilket format overføres og behandles personopplysningene i (klartekst, pseudonymisert, kryptert (ende-til-ende, eller bare delvis).

Ifølge veilederen fra EDPB kan tiltak være aktuelle innenfor tre hovedområder:

- Kontraktuelle tiltak
- Organisatoriske tiltak
- Tekniske tiltak

Under punkt 3 nedenfor er konkrete tiltak som kan være aktuelle tatt inn.

Desto flere tiltak som kan iverksettes, desto mindre risiko er det for at overføringen ikke er tillatt og desto tryggere vil er personopplysningene kunne være. Etter veilederen vil kontraktuelle og organisatoriske tiltak i seg selv vil trolig ikke være tilstrekkelig uten at det også iverksettes tekniske tiltak.

Behandlingsansvarlig må så vurdere om tiltakene i praksis er tilstrekkelige for å sikre at behandlingen er tilvarende som innenfor EØS. Anses det for å være det, så kan overføringen til tredjelandet gjennomføres.

Er ikke nivået nådd, så må enten overføringen stanses eller nye tiltak vurderes. Gjennomføres overføringen til tross for at tiltakene anses for å ikke være tilstrekkelig, så må tilsynsmyndigheten, som Datatilsynets, varsles.

2.5 Iverksettelse av tiltakene

Når tiltakene er vurdert, så skal disse gjennomføres. Slik implementering kan skje både hos behandlingsansvarlig og databehandler avhengig av tiltakene.

Implementering bør følge rutinene for internkontroll som skal etableres hos behandlingsansvarlig og databehandler, og implementeringen skal dokumenteres (nedtegnes og bekreftes skriftlig).

Det kan være hensiktsmessig at behandlingsansvarlig undersøker og får bekreftet fra databehandleren at tiltakene er iverksatt.

2.6 Regelmessige vurderinger

Det skal foretas regelmessige vurderinger av om tiltakene gjennomføres, om disse har tilstrekkelig virkning, eller om det må foretas nye vurderinger og påfølgende endrede eller nye rutiner. Her kan det være nyttig å ha man har rutiner for regelmessig vurdering av om tiltakene er tilstrekkelig og at de utføres som en del av internkontrollrutinene/-systemet.

Vurderingene bør som nevnt foretas ved iverksettelse av ny overføring eller endring i overføringer til tredjeland. I tillegg bør vurderingen skje regelmessig, f.eks. hvert kvart-, halv- eller helår avhengig av overføringen (momentene under punkt 2.4 kan også brukes her).

De regelmessige vurderingene kan også gjøres sammen med databehandler, om det lar seg gjøre. Behandlingsansvarlig bør også følge med på om det skjer endringer hos databehandler, som på informasjonssikkerhet, bruk av nye databehandlere, overføringer til tredjeland (videreoverføring), mv.

3 Tiltak

EDPB har også i sin veileder en liste over tiltak som kan implementeres i Annex 2 til veilederen. Nedenfor er en oppsummering av tiltak som følger av selve veiledningen, Annex 2 og andre tiltak som kan vurderes.

Merk at denne listen er kun eksempler, og andre tiltak kan iverksettes. Slike tiltak kan følge av standarder for internkontroll, informasjonssikkerhet mv. eller annen informasjon knyttet til informasjonssikkerhet. Merk også at tiltakene bør vurderes innenfor ekspertise på området, f.eks. ekspertise på tekniske forhold vurderer de tekniske tiltakene. Men til slutt er det ledelsen i behandlingsansvarlig som er ansvarlig for om overføringen skal gjennomføres.

3.1 Organisatoriske tiltak

Organisatoriske tiltak vil kunne være tiltak som:

- Etablere rutiner for medarbeidere, som å begrense den enkeltes tilgang til opplysningene, som regulerer bl.a. det som følger nedenfor og ta inn rutinene i internkontrollen.
- Regulere hvem som har ansvar i organisasjonen knyttet til forhold vurdering av om utlevering skal skje og selve utleveringen av personopplysningene, som utlevering til myndighetene.
- Rapportering i organisasjonen som sikrer at uregelmessigheter ved behandlingen (som tegn på avlytting eller utlevering), innsynskrav og utleveringer rapporteres offentlig (om mulig) mv.
- Krav om at personopplysninger ikke skal videreføres/viderebehandles uten at underdatabehandler blir pålagt samme krav til organisatoriske tiltak.
- Krav fra myndighetene skal rapporteres til behandlingsansvarlig, om da ikke databehandleren er pålagt konfidensialitet om forholdet («gag order»).
- Ved pålegg om utlevering fra myndighetene, så skal databehandleren søke å motsette seg utleveringen med alle mulige rettslige virkemidler for å forhindre utleveringen, og i tilfelle utlevering, minimere hva som utleveres av personopplysninger. Dette er noe som de fleste større skyleverandører påtar seg og gjennomfører.
- Personvernombudet involveres i alle saker om overføring til tredjelandet, som bør gjøres både hos behandlingsansvarlig og databehandler, samt i saker om utlevering til myndighetene.
- Rutinemessig gjennomgang av rutiner og hvordan disse fungerer, se også punkt 2.6 ovenfor.

Det kan benyttes standarder eller best practice innenfor det område som det drives virksomhet eller som opplysningene behandles, som noen av sertifiseringene som benyttes innfor informasjonssikkerhet.

Tiltakene bør tas inn i interne policyer som dokumenterer tiltakene (dvs. det kan vises at tiltakene gjennomføres), og tiltakene bør være del av internkontrollen hos virksomheten for å sikre implementering og kontroll på etterlevelse.

3.2 Kontraktuelle tiltak og nye standardbestemmelser (SCC)

Kontraktuelle tiltak kan være regulering i avtaler om at mottakeren skal opplyse om hvilke regler denne er underlagt som kan medføre at opplysninger må utleveres til myndighetene. Slike avtaler binder imidlertid ikke myndighetene, og mottakeren kan også være pålagt å ikke opplyse om at denne er underlagt slik lovgivning eller at den har fått krav om utlevering (som er tilfelle i bl.a. USA). Det er imidlertid viktig å huske at kontrakter gjelder kun mellom partene, som behandlingsansvarlig og databehandler, og har normalt ikke virkning for tredjeparter, som myndighetene.

Kontraktuelle tiltak som kan pålegges følger til en stor grad av databehandleravtaler som inngås i dag og kravene etter GDPR artikkel 28 og artikkel 32, som at databehandler skal dokumentere etterlevelse av tiltak, gi rapporter på avvik og eventuelt eksterne revisjoner, sertifiseringer mv.

EDPB har en rekke eksempler på kontraktregulering som kan være aktuelle (se Annex 2 til veiledningen):

- Databehandler forplikter seg til bestemte tekniske foranstaltninger i tillegg til de som ellers er avtalt og som følger av lovverket.
- Databehandlere skal informere om myndighetenes krav om tilgang til opplysningene, samt om utlevering, dersom databehandler har anledning til dette. Se også dette i punkt 3.1 ovenfor om organisatoriske tiltak. Databehandler skal også bekrefte på forespørsel om at denne ikke har utlevert opplysninger til myndighetene (vil kunne være et effektivt tiltak siden databehandler må da enten avkrefte eller ikke kunne uttale seg, men må da gjentas med en viss hyppighet).
- Databehandler skal gi informasjon om denne er underlagt lovgivning om å utlevere opplysninger til myndighetene, og om dennes erfaringer med krav om og tilgang til opplysninger fra myndighetene. Databehandler skal også informere om endringer av regelverk som pålegger overvåking mv. og som databehandler er underlag.
- Databehandler skal forplikte seg til å forhindre at det foreligger bakdører eller tilsvarende som gir tilgang til databehandlerens systemer for f.eks. myndighetene, og at systemet ikke er tilrettelagt for tilgang til personopplysninger uautorisert, samt at krypteringsnøkler oppbevares sikkert og ikke tilgjengelig for myndighetene.
- Databehandler skal gi rett til tilsyn og revisjon fra behandlingsansvarlig samt tilgang til logger og annet som kan vise tilgang til opplysningene av myndighetene.
- Databehandleren skal benytte rettslige midler for å avvise kravet fra myndighetene, se også nedenfor om organisatoriske tiltak, herunder informere myndighetene om at utlevering av personopplysningene er et brudd på GDPR, og spesielt artikkel 46, samt å informere behandlingsansvarlig.
- Databehandler skal være forpliktet til å innhente samtykke fra den registrerte i saker hvor vedkommendes personopplysninger vil eksponeres for databehandler (som ved support).
- Databehandler skal bistå med å hjelpe den registrerte (dvs. den person opplysningene gjelder) til å ivareta sine rettigheter.

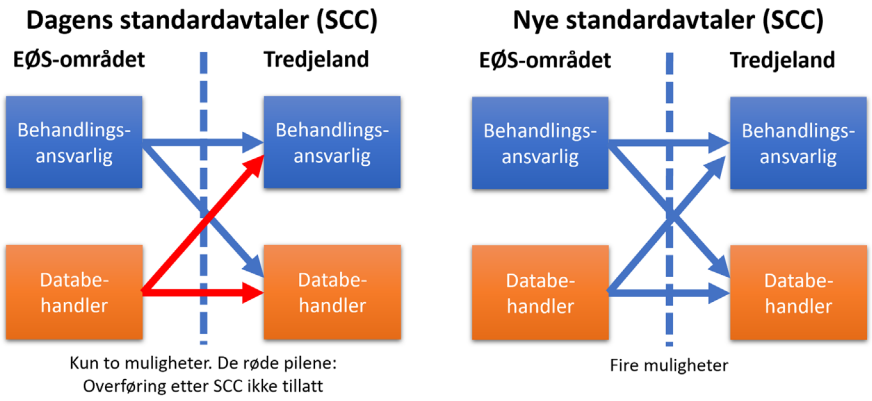
I veiledningen har EDPB tatt inn eksempler på forutsetninger for at ovennevnte kontaktregulering skal være effektive som tiltak.

De kontraktuelle tiltakene kan tas inn eller vedlegges databehandleravtalen mellom behandlingsansvarlig og databehandler, i SCCene som er inngått eller i nye SCCer som skal inngås, se nedenfor. Det som er utfordringen med å endre SCCene er at dersom disse endres, eller det inngås avtale som strider mot SCCene, så må de forelegges Datatilsynet for godkjennelse. Det kan derimot ta inn bestemmelser i tillegg til standardteksten i SCCene dersom disse ikke strider mot SCCenes standardtekst.

Nye Standard kontraktsbestemmelser (SCC)

Som ett av tiltakene fra EU-kommisjonen for å bedre personvernet ved overføring til tredjeland, er det nylig kommet utkast til nye standard kontraktsbestemmelser (SCC). De nye SCCene er en oppdatering som det har vært arbeidet med lenge, men som har fått noen tilpasninger til Schrems II-avgjørelsen. Bestemmelsene er kun utkast, men vil trolig ha stort sett samme oppbygning når de vedtas. Etter vedtakelse vil det bli en overgangsperiode på ett år hvor dagens SCCer skal erstattes med de nye. Inngås det nye avtaler om overføring eller eksisterende SCCer byttes ut endres etter vedtakelsen av nye SCCer, skal de nye SCCene benyttes.

En viktig endring med de nye SCCene er at dagens SCCer dekker kun overføring mellom behandlingsansvarlig innenfor EØS og enten behandlingsansvarlig i tredjeland eller databehandler i tredjeland. I de nye SCCene er det lagt opp til at man skal dekke alle de fire alternativene:



Det er også gjort enklere at flere parter knytter seg til overføringsavtalen (SCC), som gjør forvaltningen av avtalen enklere. Dette passer med at avtalen kan benyttes i flere konstellasjoner som vist ovenfor.

I de nye bestemmelsene skal også overføringen og behandlingen beskrives nærmere enn tidligere, herunder bl.a. sikkerhetstiltakene. Dette kan sees på som en tilnærming til kravene etter Schrems II-avgjørelsen.

Noe nytt er også at de nye SCCene dekker også kravene til databehandleravtale etter GDPR artikkel 28 etter tydelig inspirasjon av de nye standard databehandleravtalene fra EDPB. Dette innebærer at de nye SCCene står på egne ben som databehandleravtale slik at det ikke er nødvendig med både databehandleravtale og SCC, som i dag. Men det vil nok i enkelte tilfelle inngås en databehandleravtale i tillegg til SCC, men SCC vil da gå foran databehandleravtalen. Dette vil trolig redusere «databehandleravtalekrigen» ytterligere i tillegg til at det er kommet ny standard databehandleravtalen fra EDPB.

Noe som også er interessant er at lovgivningen til land innenfor EØS skal regulere avtalen (lovvalg), som f.eks. kan være behandlingsansvarliges land og lovgivning. Kombinert med at

databehandleravtaledelen i SCCene skal gå foran eventuell annen databehandleravtale, vil det medføre at lovreguleringen i denne skal gjelde, med den følge at databehandler i tredjeland ikke kan kreve sin egen lovgivning skal gjelde.

3.3 Tekniske tiltak

Tekniske tiltak vil være knyttet til den tekniske behandlingen av personopplysninger og tiltak som kan iverksettes her for å øke sikkerheten for personopplysningene i tredjelandet. Tiltak som kan være aktuelle er f.eks. kryptering, pseudonymisering, spesielle vern, splitte opp behandlingen til flere aktører mv. Enkelte av tiltakene er det gått nærmere inn på nedenfor.

3.3.1 Kryptering

Kryptering kan benyttes som tiltak for å sikre personopplysningene. Kryptering skal gjøres enten ved overføring (i transitt) eller der hvor behandling skjer (i tredjelandet).

EDPB anbefaler at følgende gjelder for krypteringen som benyttes og som er på plass *før* overføringen skjer:

- Krypteringen skal være tilstrekkelig sterk og robust mot dekrypteringsløsninger og andre forsøk på å knekke krypteringen (som kan forsøkes fra myndighetene)
- Krypteringen må hensynta den periode krypteringen skal anvendes for, dvs. om det kan komme dekrypteringsmåter i fremtiden.
- Kryptering må være tilstrekkelig godt implementert («flawless implemented») av tilstrekkelig vedlikeholdte krypteringsløsninger.
- Krypteringsnøklene skal oppbevares innenfor behandlingsansvarliges kontroll i EØS eller andre som er under behandlingsansvarliges kontroll også innenfor EØS.

Er ovennevnte gjennomført, så vil det med høy grad av sikkerhet kunne sies at tiltakene er tilstrekkelig. Det må trolig i tillegg være inntatt i kontrakt (se kontraktuelle tiltak under punkt 3.2 ovenfor) med databehandler at kryptering etter ovennevnte krav skal etterleves, og at det er iverksatt organisatoriske tiltak for at kravene gjennomføres. EDPB bruker som eksempel at ved av bruk av databehandler i tredjeland (som skyleverandører) hvor personopplysninger behandles i klartekst (dvs. ikke kryptert), så må behandlingen opphøre. Dette er trolig et for spisset eksempel, se nedenfor, men viser noe om tiltakene som kan gjennomføres.

Det kan også være at dataene er kryptert, men at dekryptering av en begrenset mengde data kan skje dersom dette er nødvendig for f.eks. support fra tredjeland.

3.3.2 Pseudonymisering

Pseudonymisering er at koblingen mellom personen som opplysningene gjelder (den registrerte) og personopplysningene som overføres til tredjeland ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger (som da beholdes innenfor EØS og overføres ikke). Det er en forutsetning for pseudonymisering at tilleggsopplysningene som kan brukes til identifisering lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene i tredjelandet ikke kan knyttes til den registrerte, (se GDPR artikkel 4 nr. 5).

Etter eksempel fra EDPB så bør:

- Pseudonymiseringen være tilstrekkelig til at det ikke er mulig å tilbakeføre personopplysningene til en fysisk person, herunder for andre land/tredjelandets myndigheter.
- Koblingen mellom opplysningene i tredjeland og hvem opplysningene knytter seg til (den registrerte) må oppbevares innenfor EØS og ikke tilgjengelig for databehandler eller andre utenfor EØS.
- Koblingen må også sikres av tilstrekkelige informasjonssikkerhetstiltak ved oppbevaringen innenfor EØS.

3.3.3 Spesielt vern

Om databehandlere eller mottakeren i tredjeland er underlagt et spesielt vern mot at opplysningene kan utleveres til myndighetene, så kan dette være et forhold som tilsier bedre sikring av personopplysningene. Dette vil normalt være at databehandleren er underlagt lovgivning som verner opplysningene i tredjelandet også, som domstolene, helsevesen, advokater, visse enheter innenfor finanssektoren mv. Også det at databehandlerens virksomhet ikke er underlagt overvåkingslover, vil kunne være et slikt vern.

3.3.4 Splitte opp behandlingen til flere aktører

Det kan iverksettes tiltak ved at behandlingen splittes opp og det benyttes flere leverandører, f.eks. en databehandler innenfor EØS, og en i tredjeland, hvor da opplysningene blir pga. behandlingen pseudonymisert. Det kan også være et tiltak, men som er mindre effektivt, at hver av databehandlerne behandler kun deler av opplysningene, slik at ikke én databehandler har tilgang til den samlede mengde personopplysninger.

3.3.5 Andre tiltak

Husk at dette er bare eksempler på tiltak, som nevnt ovenfor. Det er andre tiltak som kan være aktuelle, som må vurderes. Det vesentlige er at tiltakene skal medvirke til å sikre at myndighetene i tredjelandet ikke får tilgang til personopplysningene (som Schrems II-dommen gjelder), eventuelt at behandlingsansvarlig blir klar over at tilgang kreves eller har skjedd, slik at denne kan vurdere situasjonen og revurdere overføringen eller andre tiltak.

4 Hva skjer så?

Slik situasjonen er i dag, er det viktigste å begynne på en prosess, som den som er foreslått fra EDPB som beskrives over, for å kunne gjøre en forsvarlig vurdering, eventuelt gjennomføre tiltak, og så avvente om det kommer mer klarhet. Det vil imidlertid skje en del på dette området fremover også, så det kan være at det kommer bedre løsninger eller mer klarhet.

Etter veiledningen fra EDPB så skal datatilsynene (som vårt Datatilsyn) komme med ytterligere veiledninger. Det gjenstår å se om en slik veiledning vil bli like streng som informasjonen som allerede er kommet fra Datatilsynet. Her vil imidlertid de vurderinger som gjøres av datatilsyn i andre land også ha betydning.

Av andre tiltak så er det kommet utkast til nye standardkontraktsbestemmelser (SCC) fra EU-kommisjonen, se punkt 3.2 ovenfor. EU-kommisjonen arbeider også med å få på plass en ny avtale med USA, trolig til erstatning for Privacy Shield, som muligens vil komme før nyttår. Så får vi se hvor lenge denne løsningen varer før vi får Schrems III…

5 Noen tanker til slutt

Etter Schrems II-dommen virket det vanskelig å fortsette å overføre personopplysninger til USA eller til selskaper innenfor EØS med amerikansk hovedkontor. Alle så derfor frem til veilederen fra EDPB. Nå er den kommet, og den gjorde ikke at det ser så veldig mye lysere ut for bl.a. bruk av amerikanske leverandører.

Vurderingene som skal foretas ved overføring til tredjeland som følger av Schrems II-dommen og veilederen fra EDPB er meget vanskelige og omfattende. Vurderingene vil også kreve samarbeid med amerikanske selskap hvor en del hevder fremdeles at Privacy Shield er tilstrekkelig overføringsgrunnlag og ser ikke hensikten med å redegjøre for, og langt mindre innføre, tiltak ut over de som foreligger i dag. At databehandlerne er pålagt å ikke gi noen informasjon om at de kan eller har utlevert opplysninger til amerikanske myndigheter gjør det ikke enklere.

Også det at den enkelte behandlingsansvarlig skal gjøre en tilstrekkelig vurdering av lovgivningen i tredjelandet som overføringen skal skje til, herunder overvåkningslovgivning, samt å vurdere hvilke tiltak som kan iverksettes for å sikre behandlingen av personopplysninger til et nivå som er i det vesentlige på nivå med EU-retten, er en utopi.

I veilederen fra EDPB er det også tatt inn en del kategoriske eksempler som trolig ikke kan tas helt på ordet. Man må legge til grunn at det ikke var EDPBs hensikt å gjøre nær alle virksomheter i Europa til lovbrytere. Det er viktigere å se på selve veilederen fra EDPB, og ikke legge for mye vekt på eksemplene. Men det betyr ikke at tilsynene, som Datatilsynet, vil forstå dette annerledes.

Selv med de gode intensjonene fra Schrems II-dommen og veiledningen fra EDPB, så er det også naivt å tro at enkelte tiltak vil kunne forhindre amerikanske overvåkingsmyndigheter får tilgang til de opplysninger de vil ha. Enkelte tiltak vil imidlertid kunne redusere risikoen, men om myndighetene vil ha opplysningene vil de få dem uansett, også ved hjelp av myndighetene i EØS-land som har blitt avdekket.

Datatilsynet mener at dersom man f.eks. ikke har ressurser eller ekspertise til å gjennomføre de nødvendige vurderingene ovenfor, er usikker på resultatet av vurderingene eller det er påkrevd med ytterligere tiltak, men man vet ikke hvilke ytterligere tiltak som er tilstrekkelige, så er det ulovlig å overføre personopplysningene til tredjeland.

Skal man følge Schrems II-dommen, veiledningen fra EDPB og Datatilsynets oppfatning, så må bruken av amerikanske leverandører stort sett stanses umiddelbart.

På den andre side er det ikke greit at amerikanske myndigheter kan kreve utlevert opplysninger om borgere i andre land. Mange kunder er avhengig av tjenestene fra amerikanske leverandører, men det er ingen god løsning å skyve ansvaret over på de som benytter seg tjenester fra amerikanske leverandører. For de fleste av disse kundene finnes det ikke alternative leverandører innenfor EØS, og EU burde heller ha forsøkt å løse utfordringene med overvåkning med USA enn å kaste kundene av amerikanske leverandører under bussen.

Det gjenstår også å se om Datatilsynet og EDPBs vurderinger kan opprettholdes, eller om forståelsen om dommen er for streng. Det blir spennende å se om datatilsynene skal starte å bøtelegge alle selskaper innenfor EØS for å bruke amerikanske leverandører eller for overføring til tredjeland. Dette vil i tilfelle tilføre staten omfattende inntekter, men på bekostning av virksomheter som ikke har andre valg.

6 Mer informasjon / tilbakemelding

Det er ikke mulig å være helt utfyllende her, og det kan være feil, så si gjerne i fra om det er noe som jeg har glemt eller tatt feil, så oppdaterer jeg artikkelen.

Artikkelen finnes på sandtro.no og på LinkedIn.

Denne artikkelen kan brukes videre og spres, forutsatt at den ikke endres og denne informasjonen om forfatteren beholdes, se mer om rettigheter her.

7 Om forfatteren

Advokat Jan Sandtrø er en uavhengig advokat som bistår klienter innenfor krysningsfeltet mellom juss og teknologi. Han har lang erfaring og omfattende ekspertise innenfor personvern, GDPR, kontrakter for programvare og leveranser, rettigheter for teknologi, digital markedsføring mv. Se mer her.

For oppdateringer, følg på LinkedIn eller Twitter

* * * *

Publisert: 27. november 2020