

**Juridisk vurdering av fulltekstpublisering av**

**dokumenter med personopplysninger**

**på internett**

(Dato for vurdering 19.11.2021)

Innhold

[1 Innledning 3](#_Toc105766716)

[2 Problemstilling og avgrensning 3](#_Toc105766717)

[3 Rettslig vurdering 3](#_Toc105766718)

[3.1 Overføringsgrunnlag i personvernregelverket 3](#_Toc105766719)

[3.2 Schrems II- dommen 7](#_Toc105766720)

[3.2.1 Kort om hva dommen sier 7](#_Toc105766721)

[3.2.2 Konsekvenser og relevante veiledere 8](#_Toc105766722)

[4 Oppsummering og konklusjon 8](#_Toc105766723)

# Innledning

Denne vurderingen handler om overføring til tredjeland og betydningen av Schrems II-dommen. Vurderingen er utført av Byrådsavdeling for finans ved Seksjon for informasjonssikkerhet og IKT, og er ikke en personvernkonsekvensvurdering eller DPIA, men en vurdering av regelverket og tolkningen knyttet til Oslo kommunes overføring av personopplysninger til tredjeland.

Nye opplysninger vil kunne føre til endringer i vurderingen.

Eventuelle spørsmål knyttet til vurderingen sendes til fagsjef for personvern i Oslo kommune: [maryke.nuth@byr.oslo.kommune.no](mailto:maryke.nuth@byr.oslo.kommune.no).

# Problemstilling og avgrensning

Oslo kommune gjennomfører en rekke behandlinger av personopplysninger som av ulike grunner kan skje utenfor Norge. Personopplysningslovens regler setter begrensninger for når personopplysninger kan behandles i land utenfor EU/EØS (tredjeland). Denne vurderingen tar for seg reglene knyttet til overføring av personopplysninger til tredjeland, samt ser på betydningen av den sentrale dommen Schrems II har for tolkningen av regelverket.

Vurderingen tar kun for seg overføringsgrunnlag som er relevante for Oslo kommune, men det gjøres oppmerksom på at andre overføringsgrunnlag finnes.

# Rettslig vurdering

Nedenfor følger en redegjørelse for relevante bestemmelser i personvernregelverket knyttet til overføring til tredjeland, og betydningen av Schrems II-dommen.

## Overføringsgrunnlag i personvernregelverket

Personopplysningsloven av 2018, som gjør EUs personvernforordning (General Data Protection Regulation – GDPR) til norsk lov, regulerer all behandling av personopplysninger. Formålet med personvernregelverket er å sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger», jf. GDPR art. 1 nr. 2. Personvernregelverket omfatter all behandling av personopplysninger som utføres av blant annet offentlige myndigheter, uavhengig av hvilket formål personopplysningene behandles for.

Når det gjelder overføring av personopplysninger til tredjeland, reguleres dette i GDPR kapittel. V.

*Artikkel 44. Generelt prinsipp for overføring*

Bestemmelsen beskriver det grunnleggende prinsippet om at personopplysninger kun kan overføres til land utenfor EU/EØS dersom bestemmelsene i kapittel V overholdes.

*«Enhver overføring av personopplysninger som behandles eller skal behandles etter overføring til en tredjestat eller til en internasjonal organisasjon, skal finne sted bare dersom den behandlingsansvarlige og databehandleren, med forbehold for de andre bestemmelsene i denne forordning, oppfyller vilkårene i dette kapittel, herunder for videreoverføring av personopplysninger fra tredjestaten eller en internasjonal organisasjon til en annen tredjestat eller en annen internasjonal organisasjon. Alle bestemmelser i dette kapittel skal få anvendelse for å sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves»*

Hva betyr dette for Oslo kommune?

Begrepet overføring er vidt, og ikke definert i personvernforordningen. EDPB har laget retningslinjer som utdyper hva som anses som en overføring, og i Ifølge retningslinjene må tre vilkår være oppfylt for at det skal være snakk om en overføring:

1. Oslo kommune (behandlingsansvarlig) må være underlagt GDPR for behandlingen som skjer
2. Oslo kommune (evt. omtalt som dataeksportør) gjør tilgjengelig eller sender de aktuelle personopplysningene til en databehandler (evt. omtalt som dataimportøren)
3. Databehandleren (dataimportøren) er i et land utenfor EU/EØS eller er en internasjonal organisasjon

I teori og praksis er det å anse som en overføring at personell fra tredjeland har tilgang til opplysningene, selv om opplysningene er lagret innenfor EU/EØS eller et godkjent tredjeland. Dette vil typisk være tilfelle ved såkalt fjernaksess. Virksomhetene må derfor være nøye med å kontrollere hvilke underdatabehandlere hovedleverandøren har, og sikre at de er kjent med hele databehandlerkjeden som kan oppstå.

Det er også relevant å ta stilling til hvilket regelverk selskapet som behandler personopplysningene er underlagt. Dersom dataimportøren er en internasjonal organisasjon, er det relevant å vurdere om organisasjon er underlagt nasjonale regler fra ikke-godkjente tredjeland. Dersom tredjelandets myndigheter faktisk kan kreve å få data utlever, har dette betydning for kommunes overføringsgrunnlag, selv om personopplysningene er lagret i land innenfor EU/EØS.

En ren transmisjon av personopplysninger via tredjeland vil ikke anses som en overføring, f.eks. der personopplysninger sendes i nettverk via servere i tredjeland for å så overføres til en mottaker, en databehandler i et annet land.

Det er opp til virksomheten selv å finne ut hva som er riktig overføringsgrunnlag. GDPR oppstiller flere overføringsgrunnlag, men vi har i denne vurderingen kun trukket frem de mest sentrale for virksomheter i Oslo kommune.

*Artikkel 45. Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå*

Personvernkommisjonen kan beslutte at en tredjestat, et territorium eller en bestemt sektor i en tredjestat eller en internasjonal organisasjon, har et tilstrekkelig nivå for vern av personopplysninger. I slike tilfeller kan personopplysninger overføres til nevnte tredjestat eller internasjonale organisasjon uten at det er nødvendig å innhente ytterligere godkjenning.

*1. Personopplysninger kan overføres til en tredjestat eller en internasjonal organisasjon når Kommisjonen har fastslått at tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat eller den aktuelle internasjonale organisasjonen sikrer et tilstrekkelig beskyttelsesnivå. En slik overføring skal ikke kreve en særlig godkjenning.*

*[…]*

*7. En beslutning i henhold til nr. 5 i denne artikkel berører ikke overføringer av personopplysninger til tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat eller den aktuelle internasjonale organisasjonen som utføres i henhold til artikkel 46-49.*

*8. Kommisjonen skal i Den europeiske unions tidende og på sitt nettsted offentliggjøre en liste over tredjestatene, territoriene og de angitte sektorene i en tredjestat samt internasjonale organisasjoner som den har fastslått ikke eller ikke lenger sikrer et tilstrekkelig beskyttelsesnivå.*

*9. Beslutninger truffet av Kommisjonen på grunnlag av artikkel 25 nr. 6 i direktiv 95/46/EF skal fortsette å gjelde fram til de endres, erstattes eller oppheves ved en kommisjonsbeslutning truffet i samsvar med nr. 3 eller 5 i denne artikkel*

Hva betyr dette for Oslo kommune?

Tredjeland som er godkjent[[1]](#footnote-1) av EU-kommisjonen, er listet opp på deres nettside, og skal til enhver tid holdes oppdatert. Det er viktig å undersøke om tredjelandet er godkjent eller ikke, da kommisjonen kan trekke sin godkjenning tilbake.

Dersom virksomhetene skal overføre personopplysninger kan det være tilstrekkelig å gjennomføre en personvernvurdering for lav/middels risiko, men dette avhenger av andre faktorer også.

*Artikkel 46. Overføringer som omfattes av nødvendige garantier*

Dette er det vanligste overføringsgrunnlaget når personopplysninger overføres til ikke-godkjente tredjeland. Ved signering av standard personvernbestemmelser forplikter leverandøren (dataimportøren) seg til å behandle opplysningene i samsvar med de kravene som gjelder innenfor EU/EØS-området. Samtidig må virksomheten/behandlingsansvarlig (dataeksportøren), sjekke at personopplysningene som blir overført, faktisk får tilstrekkelig beskyttelsesnivå på lik linje som i EU/EØS før overføringen. I tillegg plikter virksomheten/behandlingsansvarlig å sikre at rettssystemet i mottakerlandet gjør det mulig å følge de standard personvernbestemmelsene i praksis. Leverandøren plikter å informere virksomheten/behandlingsansvarlig så raskt som mulig om eventuelle hindringer for å oppfylle kravene.

*1. Dersom det ikke foreligger en beslutning i henhold til artikkel 45 nr. 3, kan en behandlingsansvarlig eller databehandler overføre personopplysninger til en tredjestat eller en internasjonal organisasjon bare dersom den behandlingsansvarlige eller databehandleren har gitt nødvendige garantier, og under forutsetning av at de registrerte har håndhevbare rettigheter og effektive rettsmidler.*

*2. De nødvendige garantiene nevnt i nr. 1 kan uten krav om særlig godkjenning fra en tilsynsmyndighet sikres ved hjelp av*

1. *et rettslig bindende og håndhevbart instrument mellom offentlige myndigheter eller organer,*
2. *bindende virksomhetsregler i samsvar med artikkel 47,*
3. *standard personvernbestemmelser vedtatt av Kommisjonen i samsvar med undersøkelsesprosedyren nevnt i artikkel 93 nr. 2,*
4. *standard personvernbestemmelser vedtatt av en tilsynsmyndighet og godkjent av Kommisjonen i samsvar med undersøkelsesprosedyren nevnt i artikkel 93 nr. 2,*
5. *godkjente atferdsnormer i henhold til artikkel 40 sammen med bindende og håndhevbare forpliktelser for den behandlingsansvarlige eller databehandleren i tredjestaten om å anvende nødvendige garantier, herunder med hensyn til de registrertes rettigheter, eller*
6. *en godkjent sertifiseringsmekanisme i henhold til artikkel 42 sammen med bindende og håndhevbare forpliktelser for den behandlingsansvarlige eller databehandleren i tredjestaten om å anvende nødvendige garantier, herunder med hensyn til de registrertes rettigheter.*

*3. Forutsatt godkjenning fra vedkommende tilsynsmyndighet kan de nødvendige garantiene nevnt i nr. 1 også sikres, særlig ved hjelp av*

1. *avtalevilkår mellom den behandlingsansvarlige eller databehandleren og den behandlingsansvarlige, databehandleren eller mottakeren av personopplysninger i tredjestaten eller den internasjonale organisasjonen, eller*
2. *bestemmelser som skal innføres i administrative ordninger mellom offentlige myndigheter eller organer, og som omfatter håndhevbare og effektive rettigheter for de registrerte.*

*[…]*

Hva betyr dette for Oslo kommune?

Dersom man bruker disse personvernbestemmelsene uendret, trenger man verken søke om forhåndsgodkjenning eller varsle Datatilsynet. Man kan også innta standard personvernbestemmelsene i en større avtale, samt føye til klausuler så fremst disse ikke er i motstrid (direkte eller indirekte) med standard personvernbestemmelser vedtatt av EU-kommisjonen.

Dersom virksomheten benytter overføringsgrunnlag etter GDPR art. 46, men ikke er trygg på at beskyttelsesnivået i tredjelandet i praksis vil være likestilt med EU/EØS sitt beskyttelsesnivå, må også ytterligere tiltak iverksettes. Dette fordi krenkelse av personvernet må motvirkes. Tiltakene kan være tekniske, juridiske eller organisatoriske. Tekniske tiltak bør som utgangspunkt alltid inkluderes, da lokale lover i tredjelandet går foran overføringsgrunnlaget (som ofte er en juridisk bindende avtale) og da vil ytterligere juridiske tiltak kanskje ikke være aktuelt. Men hva som er effektivt i praksis må vurderes konkret i hver enkelt sak.

Tekniske tiltak kan for eksempel være kryptering eller pseudonymisering, men også andre tekniske tiltak kan være aktuelt. Juridiske tiltak kan for eksempel være kontraktsmessig forpliktelse til å iverksette bestemte tekniske tiltak og tiltak når det gjelder nøkkelhåndtering. Organisatoriske tiltak kan gjerne være rutiner, fremgangsmåter og internkontroll for virksomheten. Dette er for eksempel viktig dersom virksomheten får utleveringsbegjæring. Har man gode rutiner for håndtering av slike forespørsler er det viktig med gode rapporteringslinjer og dokumentasjon mv. Dette gjelder også for leverandøren.

For mer informasjon om standard personvernbestemmelser og tilleggskravene i lys av Schrems II, se Datatilsynets veileder om overføring til tredjeland.[[2]](#footnote-2)

*Artikkel 47. Bindende virksomhetsregler (BCR)*

En godkjent BCR tillater multinasjonale selskaper å overføre personopplysninger internasjonalt innenfor samme konserngruppe til land som ikke gir et tilstrekkelig beskyttelsesnivå for personopplysninger. Det er Datatilsynet som kan vedta disse etter søknad og en godkjenningsprosess, samt en uttalelse fra Personvernrådet.

*1. Vedkommende tilsynsmyndighet skal godkjenne bindende virksomhetsregler i samsvar med konsistensmekanismen fastsatt i artikkel 63, forutsatt at de*

1. *er rettslig bindende og får anvendelse på og håndheves av hvert berørte foretak i konsernet eller gruppen av foretak som utøver en felles økonomisk virksomhet, herunder deres ansatte,*
2. *uttrykkelig gir de registrerte håndhevbare rettigheter med hensyn til behandling av deres personopplysninger og*
3. *oppfyller kravene fastsatt i nr. 2.*

*[…]*

Hva betyr dette for Oslo kommune?

Dette er interne regler for overføring av personopplysninger i multinasjonale selskaper, et konsern eller en gruppe av foretak som utøver en felles økonomisk virksomhet.

Dersom dette overføringsgrunnlaget er aktuelt for en virksomhet i Oslo kommune må flere vilkår oppfylles. For nærmere informasjon, se Datatilsynets veileder om overføring av personopplysninger til tredjeland, kapittel 5.[[3]](#footnote-3)

## Schrems II- dommen

EU-domstolen avsa 16. juli 2020 en prinsipiell dom om overføring av personopplysninger til land utenfor EU/EØS. Avgjørelsen kalles "Schrems II-dommen" og er oppkalt etter den østeriske personvernaktivisten Max Schrems. Han klaget til det irske datatilsynet for å stoppe overføringen av personopplysninger mellom Facebook Irland og Facebook Inc. i USA. Begrunnelsen var at personopplysningene hans ikke var godt nok beskyttet i USA.

### Kort om hva dommen sier

Kravet etter personvernforordningen er at behandlingsansvarlig må ha et overføringsgrunnlag ved overføring av personopplysninger til land utenfor EU/EØS. Dette kravet kommer i tillegg til kravet om behandlingsgrunnlag. Begrepet overføring[[4]](#footnote-4) er vidt, og omfatter mer enn lagring av personopplysninger. For eksempel vil fjerntilgang kunne omfattes av begrepet.

I dommen ble overføringsgrunnlaget til USA "Privacy Shield" opphevet, da det var i strid med kravene til et tilstrekkelig beskyttelsesnivå i personvernforordningen, sett i lys av menneskerettighetene. Sentralt i vurderingen var de vide hjemlene til amerikansk etterretning og at europeiske borgere ikke har god nok mulighet til å overprøve beslutningene om overvåking.

Personvernforordningen oppstiller flere andre gyldige overføringsgrunnlag, for eksempel Standard personvernbestemmelser (standard contracual clauses (SCC)). Domstolen konkluderte med at et slikt overføringsgrunnlag i seg selv ikke er nok til å beskytte de registrerte på lik linje med europeisk personvernregelverk. Den enkelte overføring må vurderes for å se om det må iverksettes ytterligere tiltak for å beskytte personopplysningene.

### Konsekvenser og relevante veiledere

De praktiske konsekvensene av Schrems II er per dags dato ikke tydelig. Det er imidlertid utarbeidet flere veiledere for hvordan virksomhetene kan imøtekomme kravene i personvernforordningen kapittel V om overføring til tredjeland. På felles intranett[[5]](#footnote-5) legger det lenke til både det europeiske personvernrådet (EDPB) sine to veiledninger og også det norske og danske datatilsynets veiledere som kan hjelpe virksomheten med vurdering og etterlevelse av regelverket.

EU-kommisjonen og USA arbeider nå med en erstatning for Privacy Shield. Arbeidet pågår i 2022.

# Oppsummering og konklusjon

* Før en behandling skjer, må virksomheten vurdere om det skjer en overføring til tredjeland
* Personopplysninger kan som hovedregel overføres til godkjente tredjeland uten ekstra krav til overføringsgrunnlag
* Dersom overføringen skjer til et ikke godkjente tredjeland, må virksomheten sikre at de har et gyldig overføringsgrunnlag, sammen med ytterligere tiltak, for å sikre beskyttelse på samme nivå som i EU/EØS
* Virksomhetene må selv finne riktig overføringsgrunnlag. GDPR oppstiller flere overføringsgrunnlag i kapittel V

1. Oversikt over godkjente tredjeland finner man her: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/> [↑](#footnote-ref-1)
2. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/sarlig-om-standard-personvernbestemmelser-som-overforingsgrunnlag/> [↑](#footnote-ref-2)
3. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/sarlig-om-bcr-som-overforingsgrunnlag/> [↑](#footnote-ref-3)
4. Se mer om overføringsbegrepet i kap. 3.1, GDPR art. 44 [↑](#footnote-ref-4)
5. <https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/personvern/veiledninger-og-maler/> [↑](#footnote-ref-5)