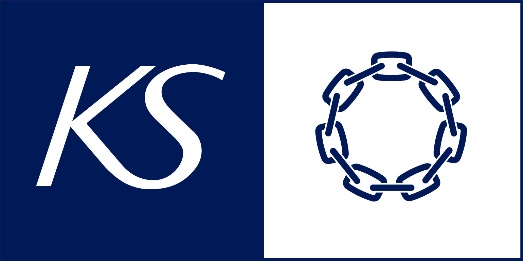
28.08.2024



Standardprosedyre ved overføring av personopplysninger ut av EU/EØS

Innhold

[FAQ 1](#_Toc170222744)

[Standard Operasjonsprosedyre (SOP) – Transfer Impact Assessment 4](#_Toc170222745)

[Hva er en SOP? 4](#_Toc170222746)

[Hvordan går man frem når virksomheten overfører personopplysninger til tredjeland? 4](#_Toc170222747)

[Steg 1: Kjenn dine overføringer 5](#_Toc170222748)

[Steg 2: Identifiser hvilke overføringsgrunnlag som benyttes i virksomheten 5](#_Toc170222749)

[Steg 3: Vurder om overføringsgrunnlaget du benytter er effektivt i lys av omstendighetene rundt overføringen 5](#_Toc170222750)

[Steg 4: Vurder behovet for å iverksette ytterligere tiltak 7](#_Toc170222751)

[Steg 5: Re-evaluer vurderingene som er gjort med jevne mellomrom 8](#_Toc170222752)

# FAQ

* **Hva er målet for denne operasjonsprosedyren?**
* Målet for denne operasjonsprosedyren er å gjøre leseren i stand til å gjennomføre en «Transfer Impact Assessment (TIA)» i tråd med kravene i Kap. V i GDPR og EDPBs veiledning på området.
* **Hva er en Transfer Impact Assessment (TIA)?**
* I en Transfer Impact Assessment vurderer man lovligheten av en bestemt overføring av personopplysninger ut av EU/EØS. Formålet med vurderingen er å sikre at personopplysningene som overføres vil oppnå en beskyttelse som tilsvarer den de ellers er sikret i henhold til GDPR innenfor EU/EØS.
* **Når skal man gjøre en TIA?**
* En TIA skal gjøres når en behandling av personopplysninger innebærer at personopplysningene overføres til et land utenfor EU/EØS.   
    
  Kapittel V i GDPR fastsetter hva som skal til for at en overføring av personopplysninger skal være lovlig. Men kravene i kapittel V i GDPR kommer ikke til anvendelse før det foreligger en overføring av personopplysninger.   
    
  Et sentralt spørsmål er dermed: Når foreligger en overføring av personopplysninger ut av EU/EØS?  
    
  En overføring av personopplysninger foreligger dersom tre vilkår er oppfylt:
  + GDPR gjelder for behandlingen av personopplysninger. Dette vilkåret vil være oppfylt for norske skoleeiere siden de alltid vil være bundet av GDPR.

* + Personopplysningene tilgjengeliggjøres eller sendes fra en behandlingsansvarlig til en databehandler eller en annen behandlingsansvarlig.

* + Virksomheten som personopplysningene overføres til holder til i et land utenfor EU/EØS.
* **Hvordan gjør man en TIA?**
* GDPR stiller ingen formkrav til gjennomføringen av en TIA. En TIA kan derfor gjennomføres på ulike måter. Det sentrale er å dokumentere at man har gjort en vurdering som svarer ut kravene i GDPR Kap. V og [EDPBs veileder](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf).
* **Hvilken metode benyttes?**
* KS anbefaler kommuner å ta i bruk EDPBs sekstrinnsmodell publisert i «*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0, Adopted on 18 June 2021)».*   
    
  Sekstrinnsmodellen gir veiledning om hvordan behandlingsansvarlig kan etterleve prinsippet om ansvarlighet dersom behandlingsansvarlig overfører personopplysninger ut av EU/EØS. Veiledningen inkluderer følgende steg:  
  + - **Steg 1: Kjenn dine overføringer**
    - **Steg 2: Identifiser hvilke overføringsgrunnlag du benytter**
    - **Steg 3: Vurder om overføringsgrunnlaget du benytter er effektivt i lys av omstendighetene rundt overføringen**
    - **Steg 4: Iverksett supplerende tiltak**
    - **Steg 5: Dersom supplerende tiltak er iverksatt; (MER)**
    - **Steg 6: Re-evaluer med jevne mellomrom**

Beskyttelsesnivået i et tredjeland er i stor grad betinget av hvor effektivt overføringsgrunnlaget er. Steg 3 er derfor svært viktig i en TIA. Her må man se på alle de involverte aktører – behandlingsansvarlige, databehandlere og databehandlers underleverandør. Man må også se på hvilke lover og hvilken praksis som påvirker den spesifikke overføringen, i lys av alle overføringens omstendigheter. Dette kalles en landvurdering/tredjelandsvurdering.

* **Hva med «godkjente» tredjeland?**
* Utgangspunktet etter GDPR er at overføringer ut av EU/EØS er forbudt. Det finnes likevel unntak til denne hovedregelen.

Et unntak er at EU-kommisjonen kan «godkjenne» enkeltland gjennom en såkalt adekvansbeslutning. Nærmere bestemt kan EU-kommisjonen beslutte at en stat, et territorium, en sektor innad i en stat eller en internasjonal organisasjon har regler som ivaretar personvernet på en tilsvarende måte som land i EØS-området. Overføringer på grunnlag av adekvansbeslutning (tilstrekkelig beskyttelsesnivå) omtales i artikkel 45 i GDPR. Stater og sektorer som per nå har fått beslutning om tilstrekkelig beskyttelsesnivå er følgende: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Sveits, Storbritannia, Uruguay, Canada, Færøyene, Japan, Sør-Korea, USA.

**Ofte stilt tilleggsspørsmål:** *Trenger man å gjøre en tredjelandsvurdering av USA?*

USA har en adekvansbeslutning som innebærer at hvis en amerikansk virksomhet står på lista over godkjente virksomheter (dataprivacyframework.gov), kan det overføres personopplysninger til den som om det var en europeisk virksomhet.

Når det foreligger en beslutning om tilstrekkelig beskyttelsesnivå, trenger ikke virksomheten gjøre egne vurderinger om beskyttelsesnivået. EU-kommisjonen har gjort dette på forhånd. Da trenger heller ikke virksomheten treffe ytterligere tiltak før de overfører personopplysningene.

* **Hvordan gjennomfører man en tredjelandsvurdering?**
* Nærmere informasjon om hvordan man gjennomfører en tredjelandsvurdering følger i SOP under.

# Standard Operasjonsprosedyre (SOP) – Transfer Impact Assessment

### Hva er en SOP?

En SOP er en prosedyre som beskriver hvordan du skal gå frem for å løse en bestemt oppgave. Formålet med en SOP er å redusere risikoen for feilkommunikasjon og menneskelige feil.

Denne SOPen beskriver hvordan en saksbehandler skal gå frem for å gjøre en Transfer Impact Assessment (TIA) når personopplysninger overføres til land utenfor EU/EØS.

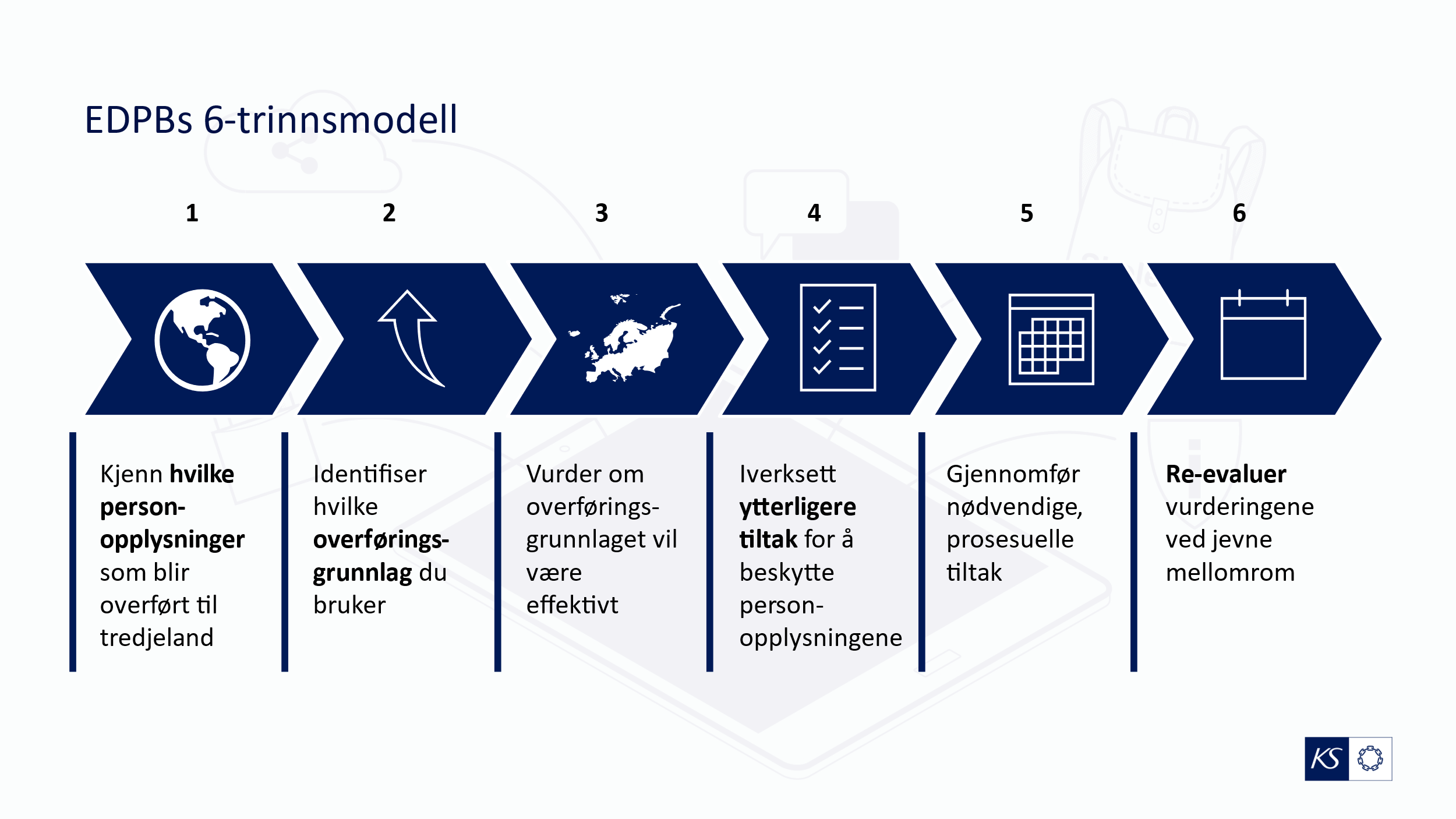
## Hvordan går man frem når virksomheten overfører personopplysninger til tredjeland?

Et eksempel som illustrerer når denne SOP kan hjelpe norske kommuner:

Kommune A ønsker å anskaffe et nytt digitalt oppvekstadministrativt system og inngår derfor en kjøpsavtale med en leverandør. I tilknytning til denne kjøpsavtalen må kommune A inngå en databehandleravtale med leverandør fordi bruk av denne leverandøren innebærer at leverandøren behandler personopplysninger på vegne av kommune A.

I forhandlingene rundt databehandleravtalen viser det seg at denne leverandøren vil overføre kommunens personopplysninger til et land utenfor EU/EØS.

Dersom din virksomhet befinner seg i en tilsvarende situasjon, anbefaler KS at EDPBs sekstrinnsmodell følges slik den er skrevet i «*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0, Adopted on 18 June 2021)»*.

Stegene i EDPBs veileder beskrives her:  


Denne Gjennomgangen begrenses til steg 1-5)

### Steg 1: Kjenn dine overføringer

Første steg er å gjøre seg kjent med overføringene – altså hvilke personopplysninger som overføres ut av EU/EØS og til hvem.

Sentralt i denne øvelsen er å forstå hvilket tredjeland som mottar personopplysninger, hvilke personopplysninger som overføres, eventuelle tidsavgrensninger og hvordan dataene overføres (eks. fjerntilgang, datalagring). Dette er informasjon som også er relevant for senere steg i sekstrinnsmodellen.

Et tips er å ta utgangspunkt i virksomhetens behandlingsprotokoll for de behandlingene som skal vurderes.

Aktivitet: Dokumenter hvilke overføringer som skjer i behandlingsprotokollen.

### Steg 2: Identifiser hvilke overføringsgrunnlag som benyttes i virksomheten

Virksomheten skal sørge for at enhver overføring er forankret i et overføringsgrunnlag. Steg 2 er å gjøre seg kjent med hvilket overføringsgrunnlag som brukes for hver overføring.

Informasjon om behandlinger av personopplysninger som involverer overføring bør fremkomme i virksomhetens behandlingsprotokoll. I behandlingsprotokollen bør virksomheten også føre oversikt over hvilket overføringsgrunnlag som benyttes.

Artikkel 46 i GDPR beskriver de alternative overføringsgrunnlagene. Det sentrale er at den behandlingsansvarlige kan gi og dokumentere «nødvendige garantier» om tilstrekkelig beskyttelsesnivå.

Aktivitet: Dokumenter hvilket overføringsgrunnlag som brukes i behandlingsprotokollen.

Hva du skal gjøre videre i TIAen, avhenger av hvilket overføringsgrunnlag som du har brukt:

* Dersom personopplysningene overføres til et land som EU-kommisjonen har godkjent, er overføringsgrunnlaget en adekvansbeslutning (artikkel 45). Da vil ikke være nødvendig å gjennomføre steg 3, 4 og 5.
* Dersom overføringsgrunnlaget er EUs standard kontraktsbestemmelser (Standard Contractual Clauses (SCC)), skal du gå videre til steg 3.

Aktivitet: Ta stilling til om du må gi videre til trinn 3 og gjøre en landvurdering.

### Steg 3: Landvurdering - Vurder om overføringsgrunnlaget du bruker er effektivt

For at en overføring skal være lovlig må overføringsgrunnlaget være effektivt i lys av omstendighetene rundt overføringen.

Steg 3 i EDPBs sekstrinnsmodell krever at behandlingsansvarlig gjennomfører en landvurdering.

Formålet med en landvurdering er å avgjøre om lovene i det landet det overføres personopplysninger til beskytter personopplysningene på tilsvarende måte som etter GDPR, eller om personvernet utfordres. Formelt skal du se på om disse lovene påvirker effektiviteten av overføringsgrunnlaget ditt. [[1]](#footnote-2)

I landvurderingen skal du se på lokale lover og regler for å analysere om de hjemler inngrep som ikke vil være lovlige etter europeisk standard. Landvurdering skal hjelpe deg å svare på spørsmålet:

Kan mottakeren av overførte personopplysninger garantere et tilstrekkelig beskyttelsesnivå for personopplysningene?

Hvorvidt et tredjeland kan vurderes til å ha tilstrekkelig beskyttelsesnivå avhenger av:

1. Om de lokale lovene som hjemler inngrep i personvernet gjelder for den konkrete overføringen? Sagt på en annen måte – gjør de lokale lovene det mulig for myndighetene i tredjelandet å få innsyn i de personopplysningene som er overført? Og hvis ja;
2. Om lovene oppfyller de «grunnleggende Europeisk garantiene»?[[2]](#footnote-3)

De grunnleggende europeiske garantiene baserer seg på EU-charteret slik det er tolket av EU-domstolen. De representerer den rettssikkerhetsstandarden som alle lover innen EU/EØS må leve opp til for at inngrep i menneskerettigheter[[3]](#footnote-4) skal være lovlige.

I en landvurdering skal du med andre ord vurdere om lovene i det landet du har overført personopplysninger til tilfredsstiller de grunnleggende europeiske garantiene. Dette gjør du ved å se nærmere på lover og praksis i tredjelandet som hjemler inngrep i personvernet.

Ifølge EDPB kan de fire kategorier grunnleggende garantier beskrives slik:

* **Garanti A**: Inngrep må være basert på klare og presise regler som er tilgjengelige for offentligheten.
* **Garanti B**: Inngrep må være nødvendig og proporsjonal for å oppnå et legitimt formål.
* **Garanti C**: Det må være et uavhengig tilsynsorgan som kan gjennomgå bruken av tilgangen.
* **Garanti D**: De registrerte personene må ha tilgang til effektive rettsmidler dersom deres rettigheter har blitt krenket som følge av myndighetenes tilgang.

Landvurderingen skal også inkludere en gjennomgang av hvordan regelverkene gjennomføres og håndheves i praksis. Praksis kan her benyttes til to ulike formål avhengig av om de grunnleggende garantiene vurderes oppfylt eller ikke:

1. Dersom regelverkene man vurderer ikke oppfyller de grunnleggende garantiene, kan beskrivelse av praksis brukes som et faktagrunnlag inn mot identifiseringen av aktuelle kompenserende sikkerhetstiltak.
2. Dersom regelverkene man vurderer oppfyller de grunnleggende garantiene, kan beskrivelse av praksis brukes for å verifisere at regelverkene faktisk håndheves slik loven sier.

Hva du skal gjøre videre i TIAen, avhenger av resultatet i tredjelandsvurderingen:

* Hvis alle de fire grunnleggende garantier er til stede, er personopplysningene godt nok beskyttet ved en overføring.
* Dersom minst én av garantiene ikke er til stede, må det gjennomføres ytterligere tiltak for å gi personopplysningene et tilstrekkelig beskyttelsesnivå.[[4]](#footnote-5) Det betyr at du må gå videre til trinn 4.

**TIPS OG TRIKS TIL STEG 3**Når man skal foreta en landvurdering for å vurdere personvernnivået i et land, er det viktig å fokusere på følgende:

* Unntakene til reglene om vern av personopplysninger: Normalt er det ikke i den generelle personvernlovgivningen man finner de største problemene, men i unntakene som hjemler inngrep i personvernet. Disse unntakene kan være vanskelige å finne og forstå.
* Lover som regulerer overvåkning og etterretning: Både "generell" statlig overvåkning og målrettet etterretningsvirksomhet, og overvåkning som ledd i påtalemyndighetens kriminaletterforskning må vurderes.
* Lover som regulerer kommunikasjonsmidler og telekommunikasjon: Disse lovene kan gi viktig informasjon om hvordan personopplysninger håndteres i det aktuelle landet.

**Slik finner du relevante lover:**

* Dataguidance: En god kilde for å finne troverdig informasjon om personvernlovgivning i forskjellige land er DataGuidance. (<https://www.dataguidance.com/>)
* Søkemotorer: Bruk søkemotorer med søkeord som "personal data in [landet du vurderer]", "surveillance laws", "laws regarding intelligence gathering" eller "telecommunication laws".
* Andre kilder: Bruk statistikk – fra leverandør eller andre, rapporter fra menneskerettighetsorganisasjoner og andre relevante kilder for å få et helhetlig bilde av personvernnivået i landet.

**Viktige tips:**

* Vær tålmodig: Det kan ta tid å finne all relevant informasjon.
* Vær kritisk: Ikke spis alt du leser rått. Vurder om informasjonen er relevant og pålitelig.
* Vær kreativ: Tenk utenfor boksen og bruk forskjellige informasjonskilder.

**Greit å vite:**

* Normal risiko: Det er ikke noe problem å være usikker når du skal konkludere i en landvurdering. Det er alltid en viss grad av usikkerhet når man skal tolke utenlandske lover og rettskilder, og det følger selvsagt en risiko for at konklusjonene tas basert på ufullstendige eller feilaktige slutninger. Dette er helt normalt og vitner bare om at du tar oppgaven på alvor.
* Ikke vær redd for å konkludere: Husk at vurderingen din bare kan bli så god som de tilgjengelige kildene tilsier. Det betyr at du må trekke konklusjoner basert på den informasjonen du har, selv om du kanskje ikke føler du har et fullstendig bilde av det rettslige landskapet. En konklusjon er bedre enn ingen konklusjon.
* Ta forbehold: Det kan være lurt å ta forbehold når du konkluderer basert på ufullstendig informasjon. I slike tilfeller er det fornuftig å legge til forbehold om at konklusjonene kan endre seg dersom nye kilder dukker opp og viser at tolkningen av lovene var feilaktig.

**Her er noen punkter du kan huske på dersom du er usikker:**

* Vær ærlig om din usikkerhet: Det er bedre å innrømme at du er usikker enn å trekke en konklusjon du ikke er trygg på.
* Forklar hvorfor du er usikker: Forklar i din vurdering hvorfor du er usikker og hvilke faktorer som bidrar til usikkerheten.
* Diskuter mulige alternative konklusjoner: Nevn mulige alternative tolkninger av lovene og hvordan disse ville påvirke konklusjonen din.
* Vær åpen for å endre din konklusjon: Vær forberedt på å endre din konklusjon dersom nye kilder dukker opp.

Ved å følge disse tipsene kan du sikre at din landvurdering er ærlig, transparent og pålitelig, selv om du er usikker på noen av konklusjonene.

### Steg 4: Vurder behovet for å iverksette ytterligere tiltak

Dersom beskyttelsesnivået i tredjelandet viser seg å være lavere enn i EØS, må det iverksettes ytterligere tiltak. Dersom det ikke finnes ytterligere tiltak eller det på annen måte viser seg å være umulig å kompensere for det lave beskyttelsesnivået, kan du ikke overføre personopplysningene.

Her må behovet for sikkerhetstiltak avpasses med funnene i steg 3. EDPB kategoriserer aktuelle tiltak inn i 3 grupper; juridiske tiltak, tekniske tiltak og organisatoriske tiltak.

Effektiviteten av tiltakene vil variere på tvers av de ulike gruppene. Juridiske og organisatoriske tiltak er typisk mindre effektive enn tekniske tiltak. Dette er fordi de lokale lovene i tredjelandet – ved kollisjonstilfelle, går foran enhver avtalerettslig forpliktelse eller interne prosedyre som leverandør skulle være underlagt.

Med **teknisk tiltak** menes typisk kryptering, nøkkelhåndtering og pseudonymisering. Kryptering og pseudonymisering gjør dataene utilgjengelig for andre som mangler de nødvendige koblings- eller krypteringsnøkler.

**EKSEMPEL**

Dersom vurderingen i steg 3 avdekker at lovene i tredjeland autoriserer inngrep ut over det nødvendige og proporsjonale, og gjennomgangen av praksis understøtter en slik konklusjon, vil kryptering være mest aktuelt. Tekniske tiltak vil generelt være mest effektive i å gjøre personopplysningene utilgjengelige for tredjelandets overvåkningsinngrep.

EDPB understreker viktigheten av at krypteringen må være «state-of-the-art». Videre vil effektiviteten av nevnte tekniske tiltak være avhengig av at krypterings/koblingsnøkkel ikke forvaltes av dataimportør (leverandør).

Med **organisatoriske tiltak** menes interne rutiner, prosedyrer og fremgangsmåter som etableres for å sikre håndteringen av personopplysningene i virksomheten.

**EKSEMPEL**

Dersom vurderingen i steg 3 avdekker at lovene i tredjeland autoriserer inngrep ut over det nødvendige og proporsjonale, og gjennomgangen av praksis understøtter en slik konklusjon, vil organisatoriske tiltak – i kombinasjon med juridiske og tekniske tiltak, være aktuelt å implementere.

Behandlingsansvarlig bør sørge for at leverandør er organisert slik at virksomheten er godt rustet til å håndtere eventuelle utleveringsbegjæringer. Dette forutsetter gode interne strukturer som sikrer rapportlinjen. Det forutsetter også at leverandørs digitale infrastruktur er preget av fornuftig tilgangsstyring. Behandlingsansvarlig bør i tillegg påse at leverandør dokumenterer eventuelle utleveringsbegjæringer som de mottar.

Med **juridiske tiltak** menes ethvert kontraktsrettslig grep som kan være egnet til å trygge behandlingsansvarliges posisjon i sin avtale med leverandør.

**EKSEMPEL**

Dersom vurderingen i steg 3 avdekker at lovene i tredjelandet forbyr enhver form for varsling om overvåkning eller lignende inngrep, vil dette påvirke de registrertes mulighet til å gjøre gjeldende sine rettigheter i henhold til GDPR. Et juridisk tiltak kan i en slik situasjon være å avtalerettslig binde leverandør til å informere behandlingsansvarlig dersom leverandør mottar utleveringsbegjæring eller på annen måte tvinges til å assistere statlige myndigheters overvåkning.

Merk at leverandør kan være rettslig forhindret å kommunisere utad om utleveringsbegjæringer eller tvungen assistanse dersom tredjelandets lovgivning krever det. Brudd på plikt om «munnkurv» sanksjoneres gjerne med kostbare økonomiske gebyrer for leverandør. Det kan imidlertid tenkes eksempler på andre avtalerettslige ordninger som kan bøte på statlig påvirkning. For eksempel er databehandler – i henhold til de fleste databehandleravtalemaler, forpliktet til å informere behandlingsansvarlig dersom databehandler ikke lenger er i stand til å etterleve sine forpliktelser etter avtalen. Imidlertid er det sjeldent slike klausuler påkrever spesifisering av årsak. På denne måten kan et uspesifisert varsel om manglende etterlevelse fra databehandler være et signal til behandlingsansvarlig om at databehandler har mottatt utleveringsbegjæring, uten at databehandler formelt bryter sine nasjonale forpliktelser. Selv om dette forutsetter en viss koordinering mellom partene, kan tiltaket være et kostnadseffektivt virkemiddel som avhjelper et konkret problem for behandlingsansvarlig, uten at databehandler sanksjoneres.

### Steg 5: Re-evaluer vurderingene som er gjort med jevne mellomrom

Vurderingene som gjennomføres i steg 3 og 4 må fornyes med jevne mellomrom. Dette er fordi forholdene som ligger til grunn og vektlegges i landvurderingen vil endre seg over tid. Effektiviteten av overføringsgrunnlaget kan dermed svekkes dersom endringene ikke oppdages og håndteres. Nye tiltak som tidligere ikke var aktuelle, kan plutselig bli nødvendig å implementere.

Behandlingsansvarlig bør etablere en klar prosedyre for re-evaluering av landvurderingen og behovet for ytterligere sikkerhetstiltak. Frekvensen for re-evaluering må vurderes konkret i hver sak.

## Rapportens struktur – et forslag

GDPR stiller ingen krav til hvordan en TIA eller en landvurdering skal se ut. Det er derfor ikke opplagt hva slags struktur disse vurderingene skal følge.

KS har utarbeidet et forslag til struktur som du kan bruke når du skal gjennomføre en landvurdering. Denne strukturen er implementert i KS sitt malverk for landvurdering.

Malverk for landvurdering er strukturert med følgende innholdsfortegnelse:

Et bilde som inneholder tekst, dokument, Font, skjermbilde

Automatisk generert beskrivelse

### Punkt 1 og 2 – Innledning

En landvurdering bør innledes med en beskrivelse av overføringen som skal vurderes, og formålet med vurderingen. Hensikten med denne beskrivelsen er å gjøre leser i stand til å forstå konteksten som overføringen er en del av. Konteksten av overføringen er i tillegg viktig fordi den etablerer rammene for at landvurderingen. Beskriv eksempelvis om overføringen medfører lagring, tilgjengeliggjøring eller lignende. Dette bidrar til å belyse situasjonsbildet og vil være relevant i spørsmålet om hvilke lover som potensielt griper inn.

Videre bør innledningen inneholde en kort opplisting av regelverkene som skal vurderes, hvilke kilder som er benyttet, samt nødvendige avklaringer og/eller forbehold. Innledningen skal sette leser best mulig i stand til å forstå innholdet i landvurderingen.

### Punkt 3 – Beskrivelse av relevante regelverk i tredjelandet

Landvurderingen bør inneholde en kort og generell gjennomgang av regelverk som berører personvernet i tredjelandet. Størrelsen på denne vurderingen kan variere avhengig av antallet regelverk det er aktuelt å se på.

Hensikten er å etablere en forståelse av det generelle beskyttelsesnivået i tredjelandet. Gjennomgangen kan eksempelvis inkludere en beskrivelse av regelverkets materielle virkeområde, prinsipper for beskyttelse av personopplysninger og om regelverket åpner myndigheters tilgang på data. Andre relevante forhold er hvordan regelverket håndheves, kontrolleres og om rettighetene kan prøves i ordinære domstoler.

### Punkt 4 – Landvurdering

KS anbefaler at landvurderingen følger EDPBs sekstrinnsmodell slik den er beskrevet i SOPen. Punkt 4 bør svare til gjennomgangen av steg 3 over.

Merk at ikke alle regelverk som beskrives i punkt 3 trenger å vurderes i henhold til de europeiske grunnleggende garantiene. Det er kun de regelverk man med sikkerhet mener vil komme til anvendelse på den bestemte overføringen som er relevant å vurdere her. (Se punkt 4.2 i innholdsfortegnelsen over)

Punkt 4 bør fortrinnsvis avklare hvilke relevante regelverk som faktisk kommer til anvendelse. På bakgrunn av disse avklaringene går man deretter videre og vurderer regelverkene opp mot de europeiske grunnleggende garantiene.

1. <https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> [↑](#footnote-ref-2)
2. European Essential Guarantees. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf> [↑](#footnote-ref-3)
3. Personvern er en del av menneskerettighetene som en del av den grunnleggende retten til privatliv i artikkel 8 i Den Europeiske Menneskerettighetskonvensjonen ("EMK") som også er inkorporert i Grunnloven. [↑](#footnote-ref-4)
4. European Essential Guarantees. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf> [↑](#footnote-ref-5)