

# HVORDAN KOMME I GANG MED SCHREMS II- VURDERINGER?

Seminar for IIA Norge

ASTRID EIKENES SKORPEN OG ELINE MARIE FJELDBERG  
02.06.2022

Alt innhold i denne presentasjonen tilhører BDO AS eller BDO Advokater AS og skal ikke kopieres eller distribueres uten vårt skriftlige samtykke.





# AGENDA

- Kort om bakgrunnen
- Steg 1-4 i EDPB sin veileder

# Hva er en overføring av personopplysninger til tredjeland?

- Ikke definert i GDPR, men EDPB har definert begrepet i nye retningslinjer (retningslinjene er på høring)
- Følgende vilkår må være oppfylt:
  1. En behandlingsansvarlig eller databehandler er underlagt GDPR for en bestemt behandling av personopplysninger, og
  2. Denne virksomheten (dataeksportøren) tilgjengeliggjør eller sender de aktuelle personopplysningene til en annen behandlingsansvarlig, felles behandlingsansvarlig eller databehandler (dataimportøren), og
  3. Dataimportøren er i et land utenfor EØS eller er en internasjonal organisasjon

- Eksempler på overføring:
  - Oppbevaring av personopplysninger på en server i tredjeland
  - Utlevering av personopplysninger til en behandlingsansvarlig i et tredjeland
  - Databehandlere i tredjeland får tilgang til personopplysninger som er lagret i EU/EØS i forbindelse med support, programvareoppdatering, feilretting eller oppfølging av sikkerhetshendelser
    - Obs! Dette gjelder også databehandlers underdatabehandlere

# Overføringsgrunnlag

- Vanlige overføringsgrunnlag:
  - Beslutning fra Europakommisjonen om at tredjelandet har et tilstrekkelig nivå av vern av personopplysninger
  - Bindende virksomhetsregler (ofte kalt BCR)
  - EUs standard personvernbestemmelser (ofte kalt Standard Contractual Clauses eller SCCs)
    - OBS! Det har kommet nye SCCer som må være inngått innen 27. Desember 2022.
- Unntak i GDPR artikkel 49
- Tidligere overføringsgrunnlag for overføringer til USA:
  - Safe Harbour (kjent ugyldig i Schrems I-avgjørelsen i 2015)
  - Privacy Shield (kjent ugyldig Schrems II-avgjørelsen i 2020)

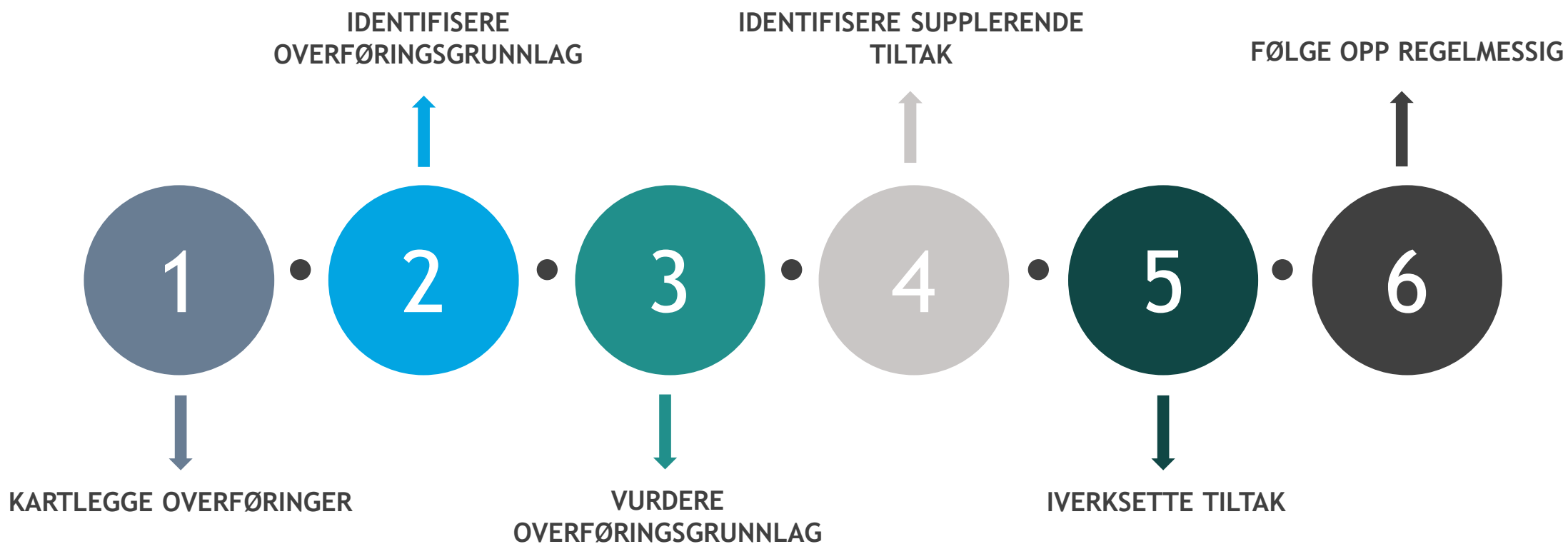


# Kravene i Schrems II

- Utfordringer med overføringer til USA:
  - US Foreign Intelligence Surveillance Act (FISA) section 702 gikk foran mekanismene i Privacy Shield
  - Proporsjonalitet i inngrepet i de registrertes personvern, både når det kom til omfanget av personopplysninger som samles inn og tilgangen til personopplysningene
  - Adgang for registrerte til å effektivt håndheve sine rettigheter
- De registrerte må oppnå et beskyttelsesnivå i tredjestaten som er «essentially equivalent» til vernet som EU-retten oppstiller.
  - BCR eller SCC er ikke nødvendigvis tilstrekkelig

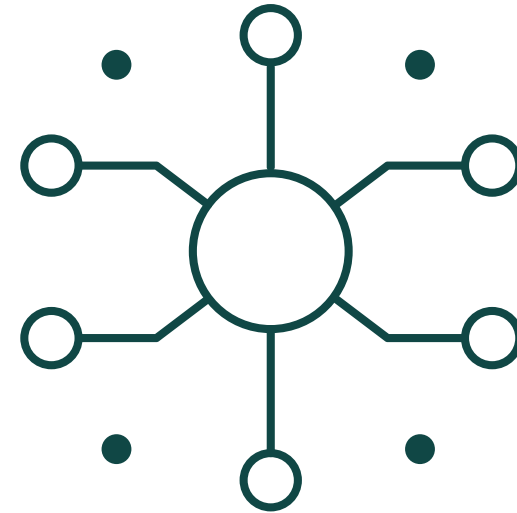


# Proessen for å vurdere overføringer



# Steg 1: Kartlegge overføringer

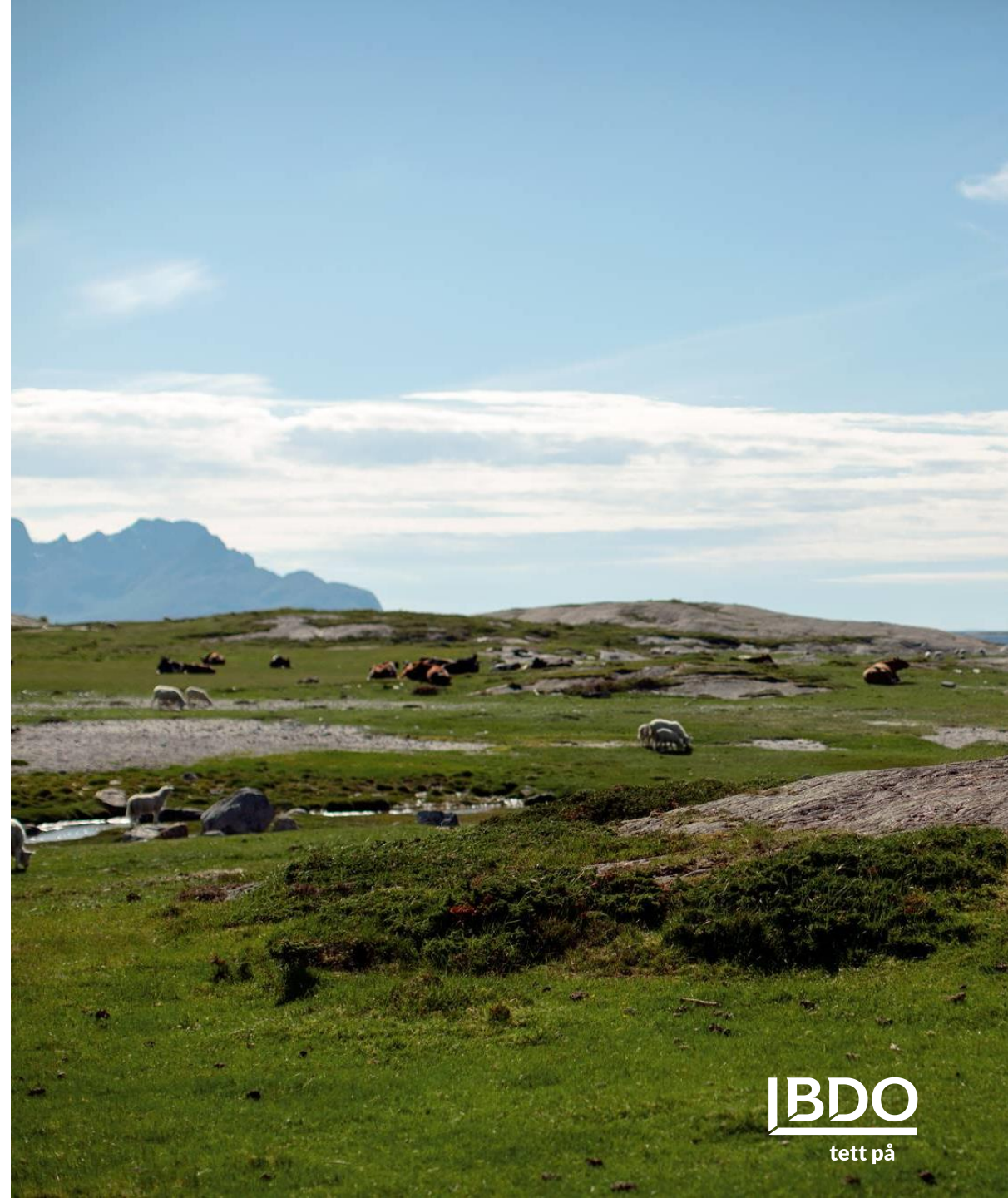
- Følgende momenter bør kartlegges:
  - Underleverandører i tredjeland (inkluderer fjerntilgang)
  - Hvilke personopplysninger som overføres
    - Hvordan og når dette skjer
  - Overføringsgrunnlag
  - Supplerende tiltak
  - Leverandørens egne vurdering





# Steg 1: Kartlegge overføringer

- Praktiske tips:
  - Ta utgangspunkt i eksisterende oversikter (f.eks. protokoll, leverandørregister, applikasjonsoversikt mv.)
  - Utarbeid et spørreskjema
  - Involver og ansvarliggjør linjen
- Utfordringer:
  - Ufullstendige svar
  - Tidkrevende





# Steg 2: Identifisere overføringsgrunnlag

- Vanlige overføringsgrunnlag:
  - Beslutning fra Europakommisjonen om at tredjelandet har et tilstrekkelig nivå av vern av personopplysninger
  - Bindende virksomhetsregler (ofte kalt BCR)
  - EUs standard personvernbestemmelser (ofte kalt Standard Contractual Clauses eller SCCs)
    - OBS! Det har kommet nye SCCer som må være inngått innen 27. Desember 2022.
- Unntak i GDPR artikkel 49
- Praktisk tips:
  - Identifiser overføringsgrunnlag i kartleggingsfasen



# Steg 3: Vurdere om overføringsgrunnlaget har en reell effekt

- Vurder om lov og praksis i tredjeland undergraver beskyttelsesnivået ved den spesifikke overføringen
  - Behandlings formål
  - Kategorier av personopplysninger og opplysningenes format
  - Involverte aktører
  - Aktuell sektor
  - Overføringens art (fjerntilgang eller lagring i tredjelandet)
  - Dataformat
  - Muligheten for videre overføring til andre tredjeland
- Beskyttede mottakere (ofte medier, advokater og helsepersonell)



# Steg 3: Vurdere om overføringsgrunnlaget har en reell effekt

- «Det er først når lokale lover og praksis går lenger enn det som er nødvendig og proporsjonalt at beskyttelsesnivået undergraves»\*
- Virksomheten trenger ikke å implementere tiltak «der det ikke er noen grunn til å tro at den problematiske lovgivningen vil bli anvendt på overføringen i praksis»\*\*
  - Vurderingen må være detaljert og vise at loven ikke blir tolket eller anvendt i praksis slik at den dekker overføringen
  - Det er uklart hvor langt dette unntaket strekker seg og hvor mye som skal til før det kan benyttes
- Datatilsynet er tydelige på at dette ikke skal være en risikovurdering





# Steg 3: Vurdere om overføringsgrunnlaget har en reell effekt

- Se oversikten i [EDPBs veileder](#) for alle relevante kilder
- Praksis og vurderinger fra anerkjente internasjonale institusjoner og organisasjoner
  - Det Europeiske Personvernrådet
  - Amnesty International
  - FN
  - Den Europeiske Menneskerettighetsdomstolen
  - Global Privacy Assembly
- Private initiativ (Husk kildekritikk)\*
  - [IAPP](#)
  - [Privacy international](#)
  - [DLA Piper](#)
  - [Enforcement tracker](#)
- Åpenhetsrapporter og erklæringer fra dataimportør



# Steg 4: Identifisere supplerende tiltak

## TEKNISKE TILTAK

- Kryptering med nøkkelhåndtering
- Pseudonymisering med nøkkelhåndtering

## KONTRAKTUELLE TILTAK

- Forpliktelse til å iverksette tekniske tiltak og tiltak for nøkkelhåndtering
- Forpliktelse til å utfordre utleveringsbegjæringer fra myndighetene

## ORGANISATORISKE TILTAK

- Internkontroll
- Rutiner for håndtering av utleveringsbegjæringer
- Streng tilgangsstyring

# Steg 3 og 4: Praktiske tips

- Kom i gang med arbeidet!
- Lag en mal for vurderingen (det finnes flere maler tilgjengelig\*)
- Dokumenter alle vurderinger og identifiserte tiltak
- Vurder alternativer
- Undersøk unntak i artikkel 49
- Lag en rutine for fremtidige overføringer
  - Sikre at kravene hensyntas tidlig i anskaffelsesfasen
- Følg med på rettsutviklingen





Astrid Eikenes Skorpen  
Advokatfullmektig / Senior Associate  
+47 993 56 743  
[astrid.skorpen@bdo.no](mailto:astrid.skorpen@bdo.no)

Eline Marie Fjeldberg  
Advokatfullmektig / Associate  
+47 958 48 414  
[eline.marie.fjeldberg@bdo.no](mailto:eline.marie.fjeldberg@bdo.no)





**BDO**

**tett på**