Overføring av personopplysninger ut av EØS etter Schrems II - NOKIOS

Guro Åsbø, juridisk rådgiver

Anna Kristin Ulfarsdottir, juridisk seniorrådgiver

26. oktober 2021

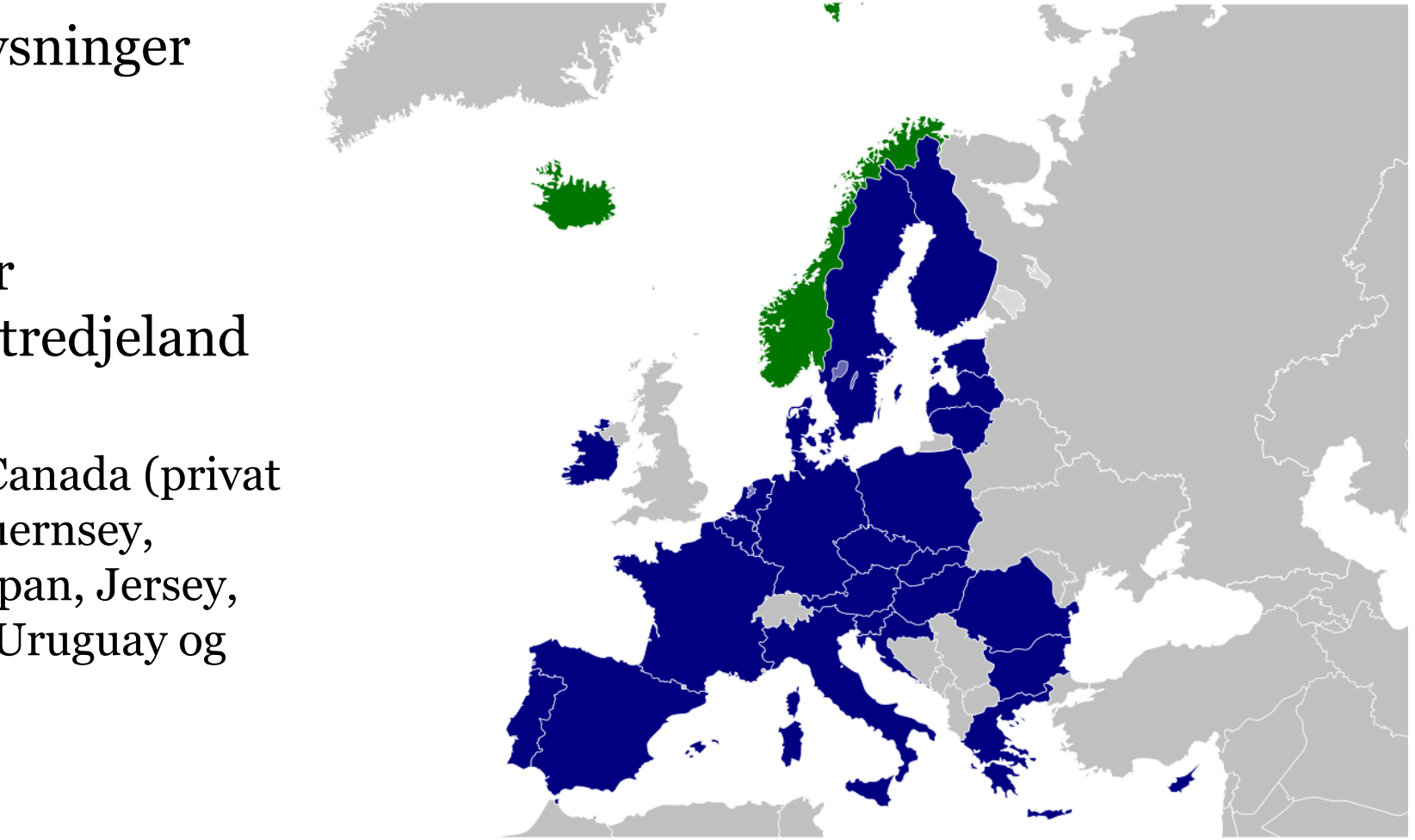
Datatilsynet

GDPR, EØS og tredjeland

- I EØS er personopplysninger «trygge»

- EU-kommisjonen har «godkjent» en rekke tredjeland (artikkel 45)
  - Andorra, Argentina, Canada (privat sektor), Færøyene, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Sveits, Uruguay og Storbritannia

- Andre land: !



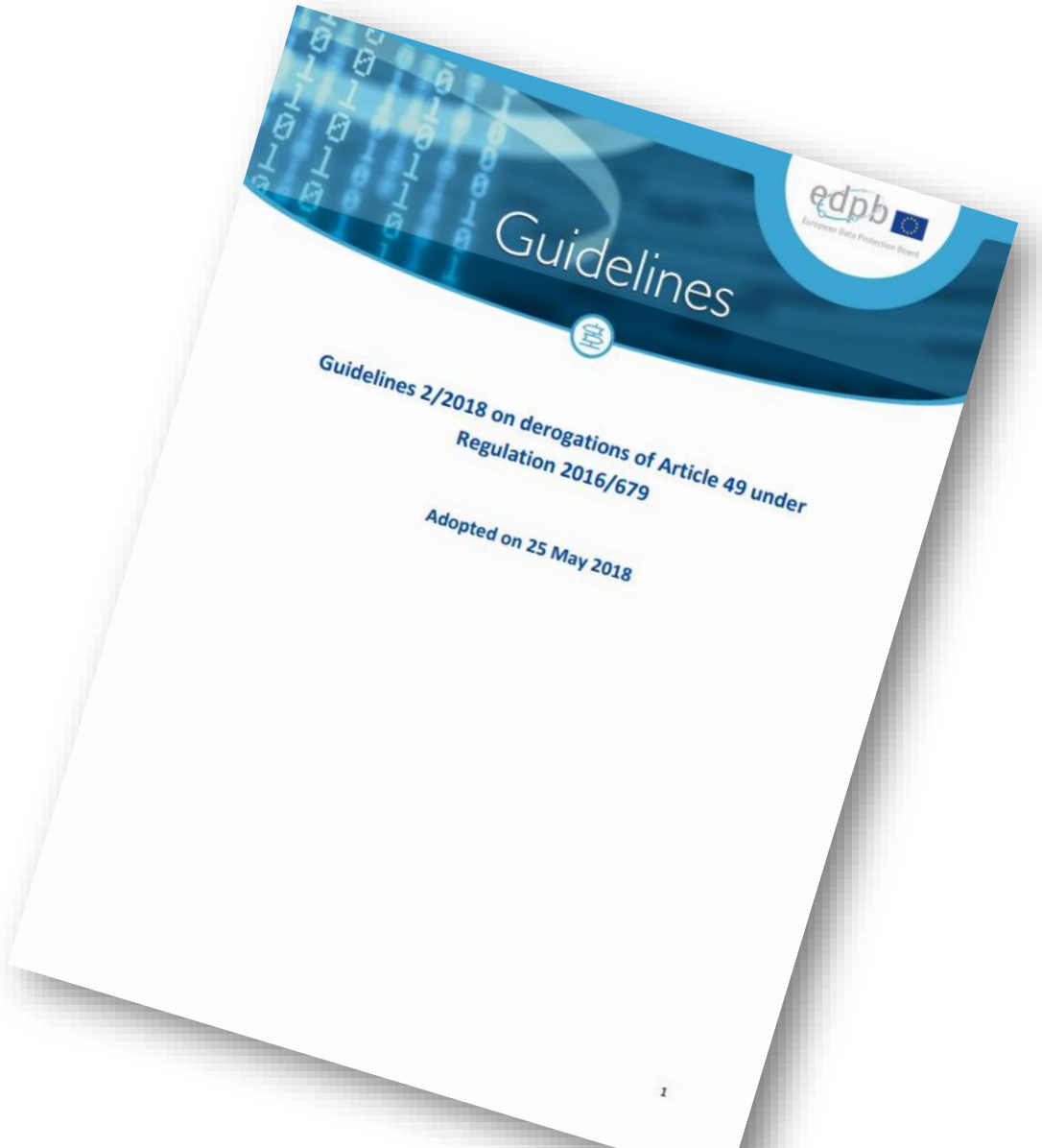
GDPR, EØS og tredjeland

- Overføringsgrunnlag (artikkel 46)
  - Standard personvernbestemmelser vedtatt av EU-kommisjonen (SCCs)
  - Bindende konsernregler (BCR)
  - Bindende avtale mellom offentlige myndigheter eller organer
  - …
- Schrems II
  - Tilleggskrav

Unntak

- Det finnes unntak fra reglene i artikkel 49

- Unntaksreglene er ment å brukes i unntakssituasjoner, ikke som hovedregel



Schrems II - Sakens bakgrunn

- Maximilliam Schrems klager på at Facebooks overføring av pol til USA bør stanses eller forbys pga manglende beskyttelse mot amerikanske myndigheters tilgang (access request) til opplysningene.
- Overføringen var basert på Kommisjonens standard bestemmelser (SCC 2010/87)
- IE SA ber om «preliminary ruling» fra ECJ
- Kommisjonen vedtar ny beslutning om tilstrekkelig beskyttelse «Privacy Shield Decision»

Domstolens vurderinger og konklusjon

- Konklusjonen er at SCC er i utgangspunktet gyldig
- SCC er kun bindende avtale mellom eksportør og importør
- Data eksportør har plikt å undersøke før ev. overføring:
  - Om det er behov for særskilte tiltak («Supplementary Measures») for å sikre at pol er tilstrekkelig beskyttet i tredje land
  - I en dialog med mottaker om det er noe lovgivning i tredjelandet som strider i mot SCC

  Hvis kriteriene ikke er oppfylt, er eksportør pliktig å ikke overføre pol og/eller avslutte avtalen med mottaker
- Det er et vilkår for at nivået av beskyttelse anses tilstrekkelig at det finnes håndhevbare rettigheter («enforcable rights) for de registrerte og effektive juridiske midler («effective legal remedies») i hendhold til EU rett, i praksis.
- I tilfeller av avtalebrudd og landet er uten beslutning om tilstrekkelig beskyttelse (jf GDPR art 45) skal SA stanse/forby overføringen

Domstolens vurderinger og konklusjon

- ECJ mener begrensningene som amerikansk rett har på europeiske borgeres rettigheter mht til myndigheters mulighet til å kreve tilgang/innsyn i europeisk pol er ikke proporsjonell til hva som anses strengt nødvendig iht til EU rett
- ECJ vurderer at ombuds-mekanismen i Privacy Shield ikke gir tilstrekkelige rettigheter i den grad som EU retten krever f.eks om ombudetmannens selvstendighet
- ECJ konkluderer at Privacy Shield beslutningen er ugyldig
- og at uten en gyldig beslutning om tilstrekkelig beskyttelse («adequacy decision») bør SA stanse eller forby overføringen til dette landet

Schrems dommene

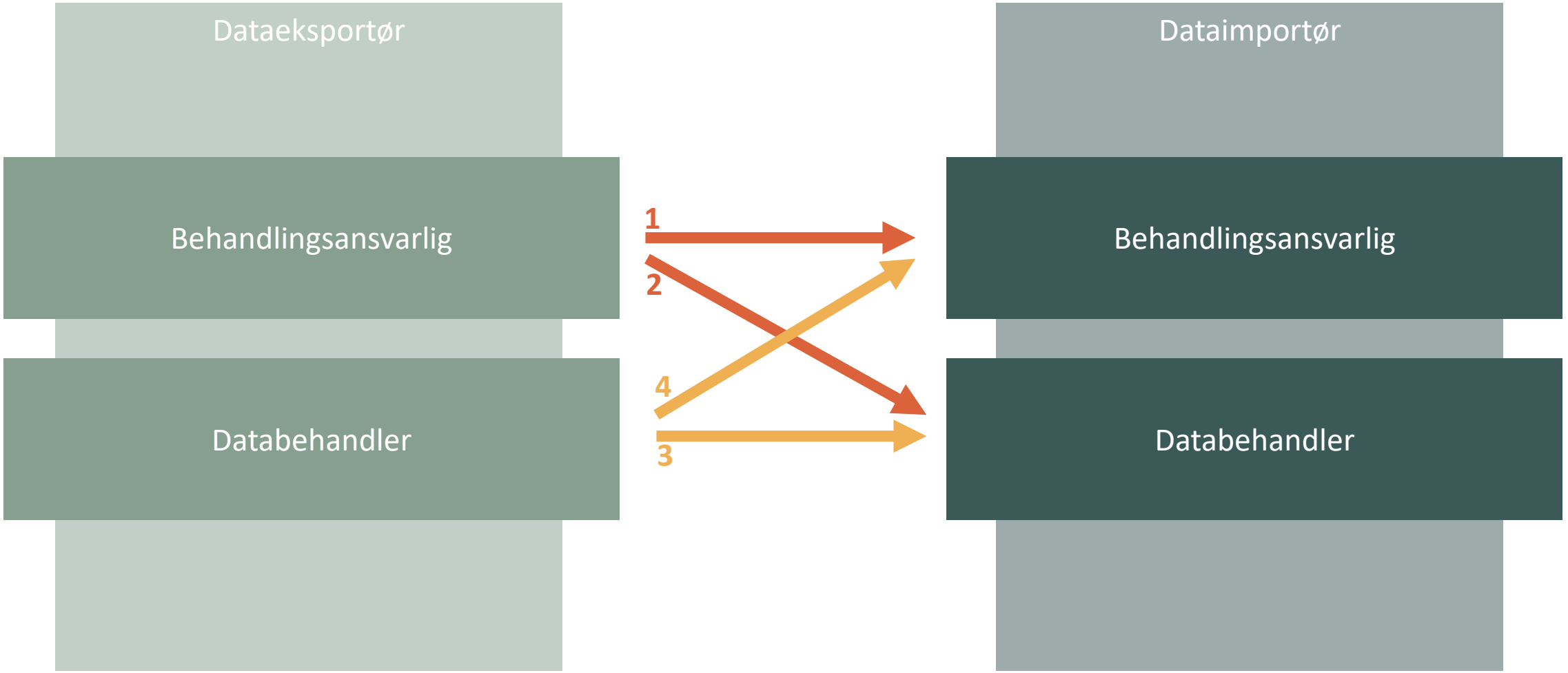
- Schrems I = Safe Harbor
- Schrems II = Privacy Shield
- Schrems II = SCC er gyldig overføringsgrunnlag
- Schrems II = Oppstiller også «tilleggskrav» for overføringer til tredjeland, selv om man bruker et gyldig overføringsgrunnlag

Nye standard personvernbestemmelser (SCCs)

- Tidsperspektivet i Norge

- Hva er nytt?
  - Tilpasset Schrems II
  - Databehandleravtale innbakt
  - De registrerte som third party beneficiaries
  - Docking-klausul
  - Kan tilpasses alle konstellasjoner av dataimportører og dataeksportører

Nye standard personvernbestemmelser (SCCs)



Nye standard personvernbestemmelser (SCCs)

- Tilstrekkelig beskyttelsesnivå og etterlevelse
  - «Ingen grunn til å tro» at lover eller praksis undergraver SCCs
    - Alle omstendigheter ved overføringen
    - Lover og praksis i tredjelandet
    - Kontraktsmessige, tekniske , organisatoriske tiltak
  - Samarbeidsplikt
  - Dokumentasjonsplikt
  - Varslingsplikt
  - Vurderingsplikt

Nye standard personvernbestemmelser (SCCs)

- Plikter ved utleveringsbegjæring
  - Underretningsplikt
  - Er dette alltid mulig?
  - Kan ha plikt til å utfordre begjæringen
  - Dataminimering
  - Dokumentasjon

- Dataimportørens plikt til å si fra hvis man ikke kan følge avtalen

- Dataeksportørens plikt til å suspendere og rett til å terminere

Schrems II – tilleggskrav

- Formålet med reglene er å sikre et tilsvarende beskyttelsesnivå

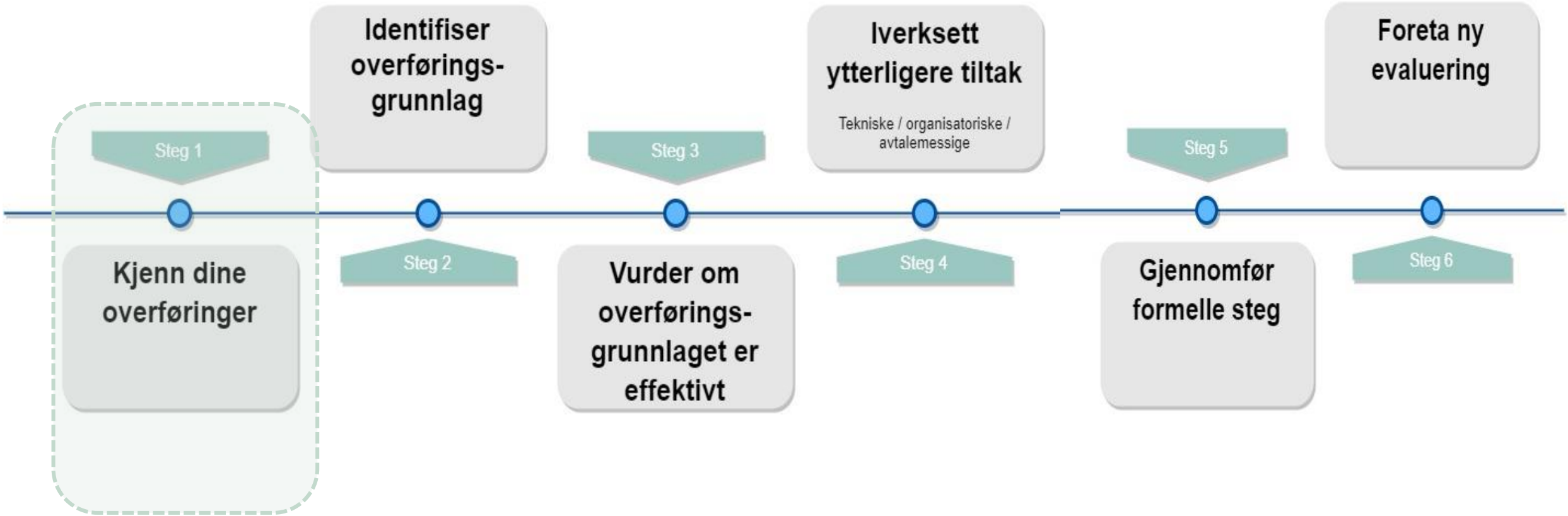
- Overføringsgrunnlagene har svakheter
  - Frivillige mekanismer
  - Lokal lov/praksis kan gå foran slike mekanismer

- Må derfor undersøke om beskyttelsesnivået blir tilsvarende i praksis
  - Alternativt: Iverksette ytterligere tiltak

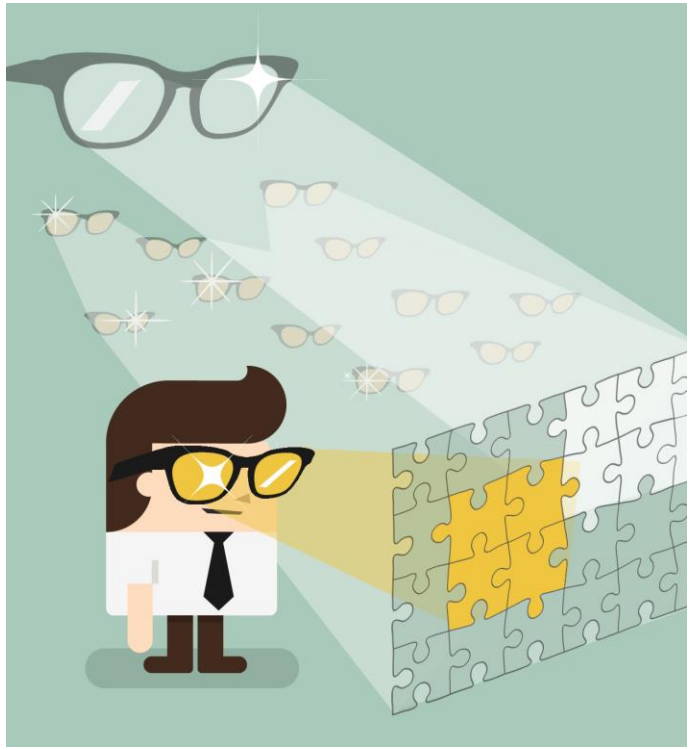
Hva må man gjøre?

- Hvordan tolke forordningens regler i etterkant av avgjørelsen?
- Anbefalinger fra Personvernrådet – 6 steg
  - Recommendations 01/2020 (2.0) om ytterligere tiltak
  - Recommendations 02/2020 om hvordan man skal vurdere overvåkingslover

1. Kjenn dine overføringer



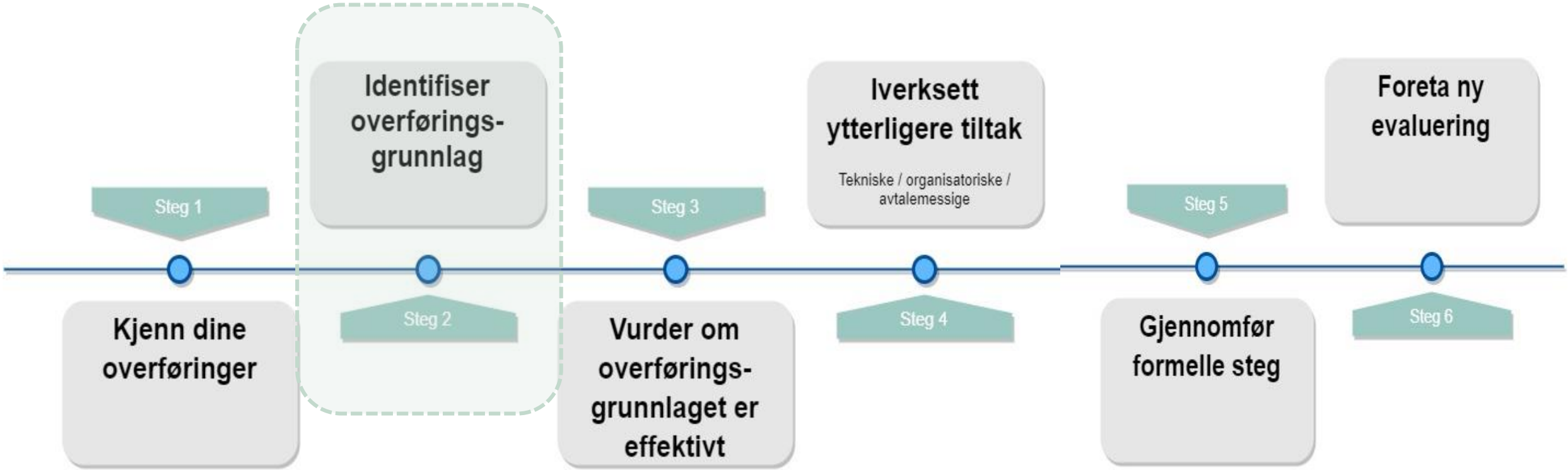
1. Kjenn dine overføringer



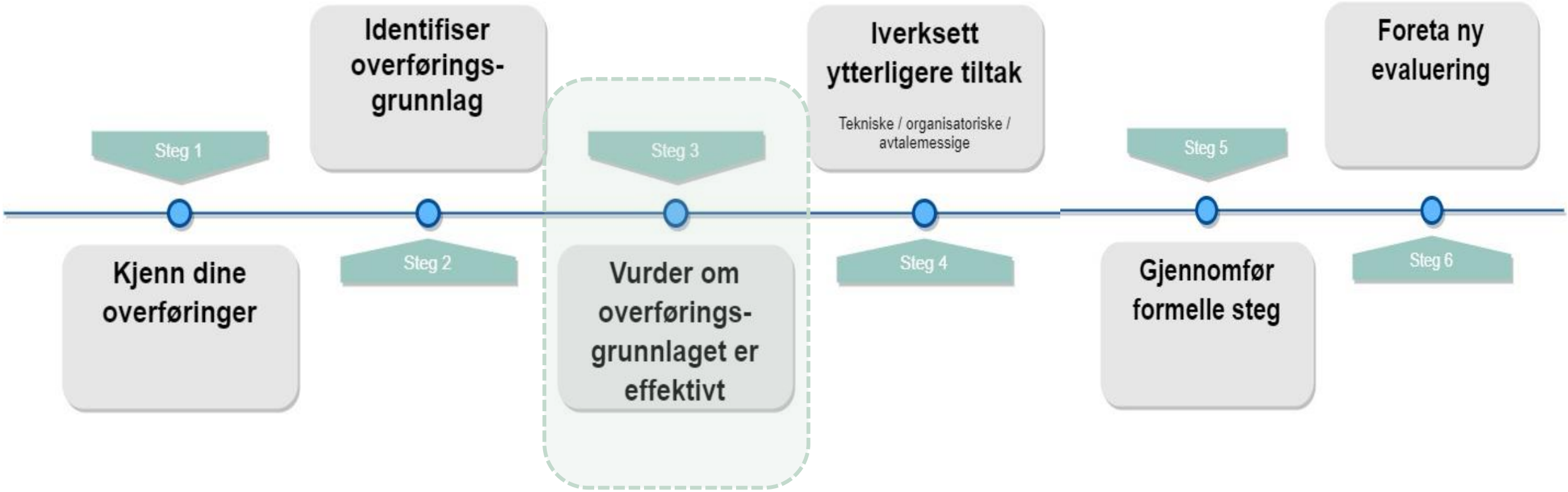
Skaff oversikt – sjekk protokollen

- Forutsetning: Må ha oppdatert oversikt over alle tjenester og ansvarsforholdene
  - Overfører vi personopplysninger til tredjeland?
  - Overfører våre databehandlere personopplysninger til tredjeland?
  - Overfører våre databehandleres underleverandører personopplysninger til tredjeland?
  - Hvilke tredjeland er det snakk om?

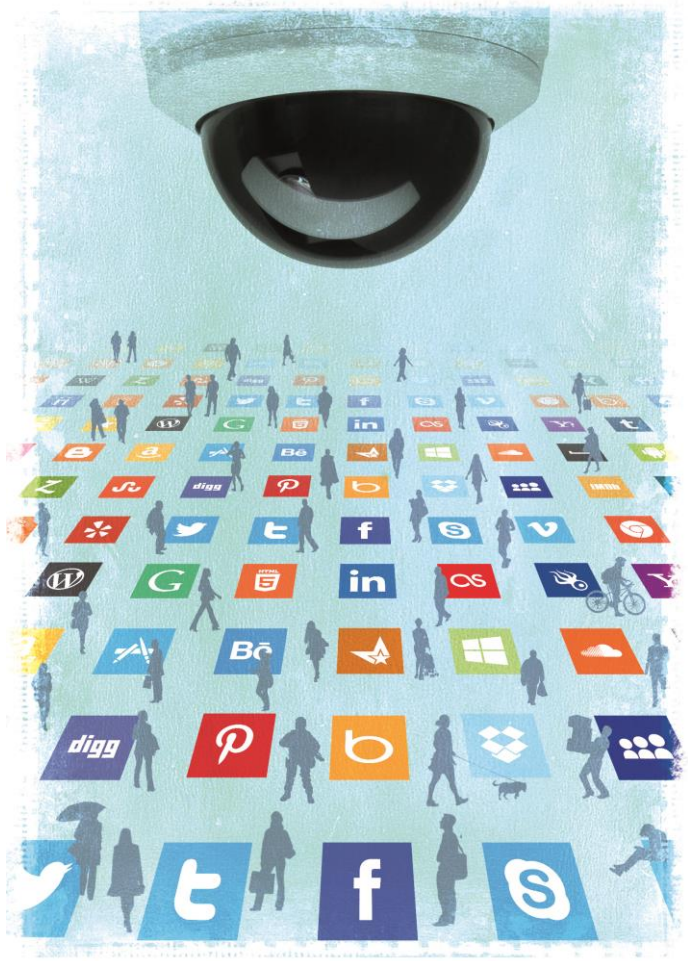
2. Identifiser overføringsgrunnlag



3. Vurder om overføringsgrunnlaget er effektivt



3. Vurder om overføringsgrunnlaget er effektivt



- Hindrer lover/praksis i tredjelandet datamottaker å følge kravene i overføringsgrunnlaget?
  - Fordel å involvere datamottaker i vurderingen

- Se hen til:
  - Hele kjeden av involverte aktører
  - Hvilke overføringer det er snakk om
  - Særlig om overvåkningslover
    - Nødvendig og forholdsmessig i et demokratisk samfunn
    - Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

Reviderte anbefalinger fra EDPB – endringer

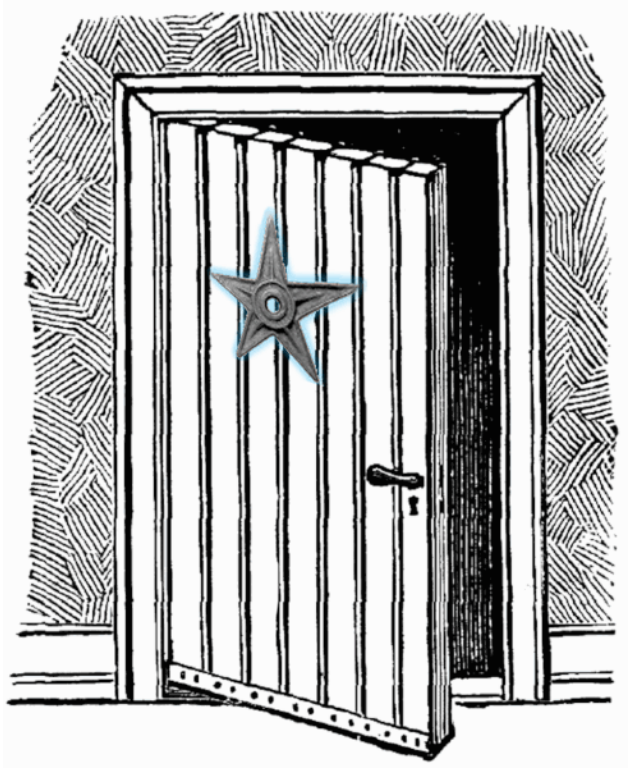
- Informasjonens kvaliteter
  - Relevant
  - Objektiv
  - Pålitelig
  - Etterprøvbarhet
  - Tilgjengelig

- Andre presiseringer
  - Trenger ikke å tenke på «alt» – bare den konkrete overføringen
  - Begrensninger og inngrep i tredjelandet kan være OK
  - Fremtiden bringer nye muligheter for gode tiltak
  - Presiseringer i *use cases* og ytterligere tiltak

Særlig om USA – Schrems II

- USA har flere overvåkingslover, herunder E.O. 12333 og 702 FISA
  - FISA 702 gjelder «electronic communication service providers» og «remote computing services» i og utenfor USA

- EU-domstolen:
  - Ikke tilstrekkelig begrenset
  - Ikke underlagt effektive overprøvingsgarantier



4. Iverksett ytterligere tiltak

4. Iverksett ytterligere tiltak

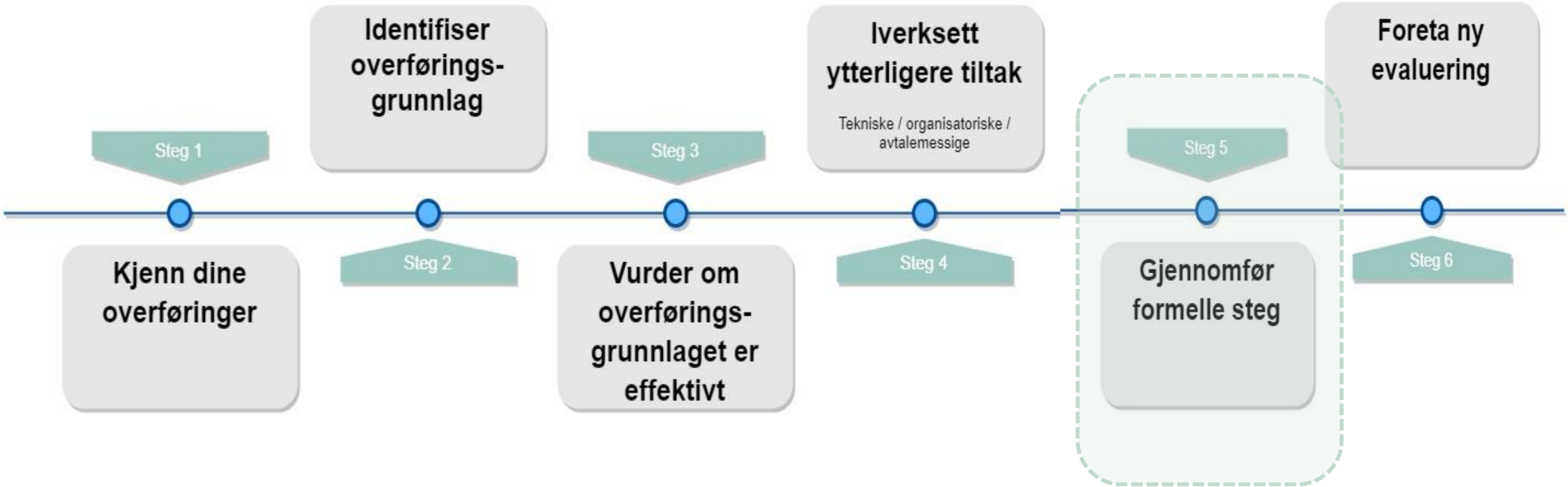
- Hvordan skal man vurdere beskyttelsesnivået i et annet land i praksis?
- Hvilke ytterligere tiltak er tilstrekkelige?
- Konsekvensene av at overføringer må stoppe

Viktige budskap fra EDPBs veiledere

- Tekniske tiltak: *Use cases*
  - Kryptering spiller en viktig rolle – på visse vilkår
  - Kryptering løser ikke alt
  - Pseudonymisering kan være en løsning i visse tilfeller (praktisk for f.eks. helseforskning)
  - Taushetsplikten er relevant
  - Dårlig nytt for fjerntilgang og support

- Kontraktsmessige og organisatoriske tiltak kan også iverksettes i kombinasjon med tekniske tiltak

5. Gjennomfør formelle steg



6. Foreta ny evaluering

Tilsynsmyndighetens rolle

- Tilsynsmyndighetene har plikt til å forby overføringer der vilkårene ikke er oppfylt

- Har foreløpig bare mottatt tre klager – fra noyb
  - Totalt 101 klager til EØS-tilsynsmyndigheter

- EUs datatilsyn (EDPS) har gjennomført tilsyn

Datatilsynets nye veileder

- Schrems II
  - Inngrep vs. krenkelse
  - Charteret vs. EMK
  - Offentlig tilgjengelige personopplysninger
  - Virksomhetene vurderer og dokumenterer

- Opplysninger utelukkende lagret i EØS
  - Hvem er behandlingsansvarlig?
  - Hvilke plikter har man?
  - Tjenestevilkårene tar forbehold

- Unntak
- Er veiledning frivillig å følge?

Myter

- Så lenge vi bruker EU-kommisjonens standard personvernbestemmelser (SCCs), er vi trygge

- Det er ingenting som tyder på at tredjelandets myndigheter faktisk har hentet eller vil hente ut data

- Kryptering løser alt

Diskusjon i grupper

The long and winding road. Gilbert Lane at Causeway Moss

Oppsummering

- Forordningen setter en høy standard, se artikkel 44
- Ansvaret ligger hos aktørene
- Enkelte overføringer må stoppe
- Konkret vurdering
- Politisk løsning ?

Takk for oss!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no