Personvern i skyen og overføring over landegrensene

Sikkerhetssymposiet 2019

Jan Sandtrø

Oversikt

- Overføring til tredjestater (utenfor EØS-området)
- Personvern og skytjenester
- Bruk av skytjeneste som databehandler
- Informasjonssikkerhet og internkontroll
- Tillit i kjernen av problemstillingen:
  - Kan man stole på at personopplysninger behandles innenfor reglene i tredjestater?
  - Kan man stole på at personopplysninger behandles innenfor reglene hos skyleverandør?

Overføring av personopplysninger

Artikkel 1. Formål og mål

1. Denne forordning fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger.

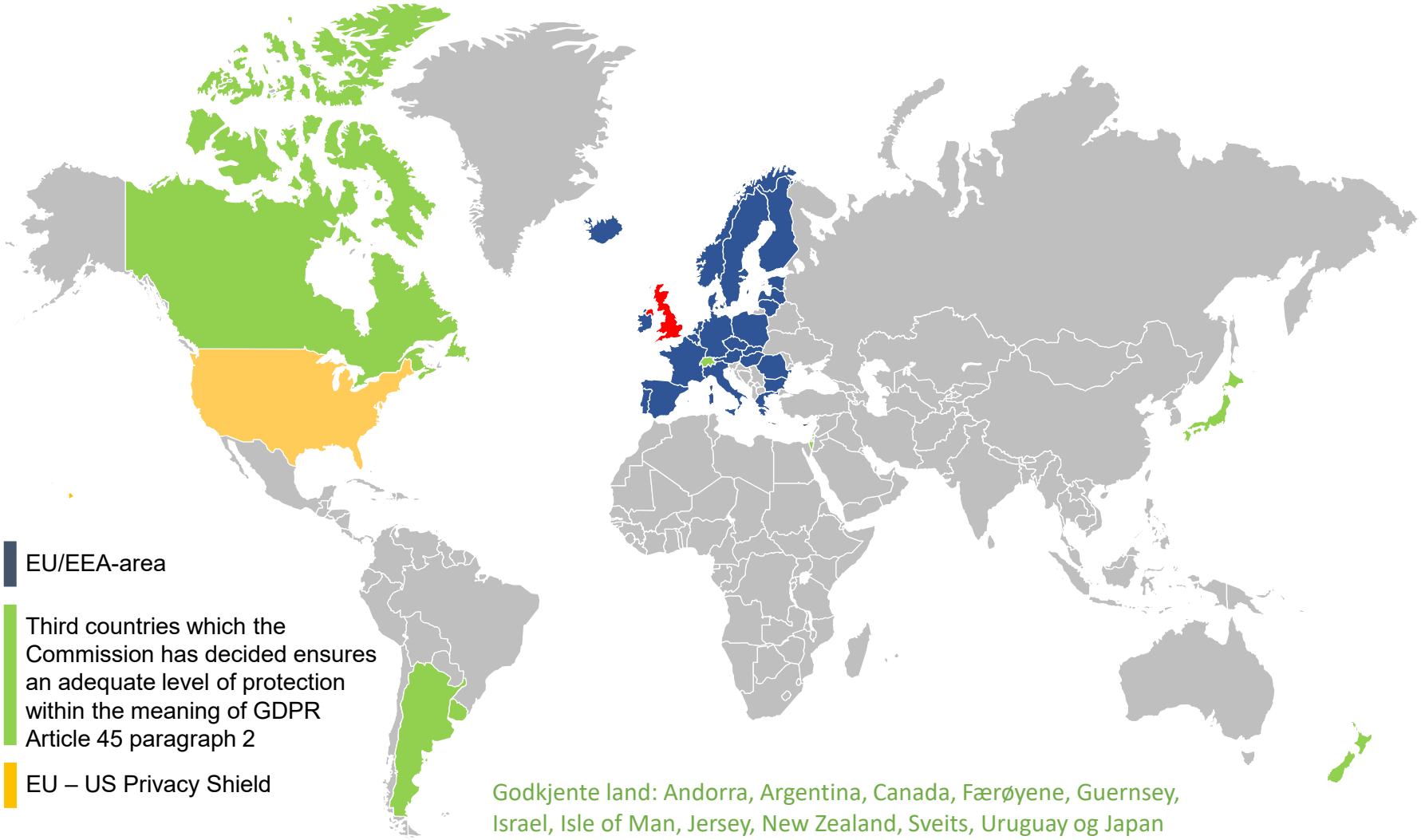
2. Denne forordning sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.

3. Fri utveksling av personopplysninger i Unionen skal verken begrenses eller forbys av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.

Grunnlag for overføring

- Overføring kun tillatt dersom det følger reglene i GDPR kapittel V
  - Dvs. må foreligge et lovlig grunnlag for overføring
  - Gjelder også videreoverføring fra tredjestaten og videre
- Grunnlagene:
  - «**Godkjent land**»: Overføring til land som er godkjent av EU-kommisjonen («sikrer et tilstrekkelig beskyttelsesnivå»)
  - **Nødvendige garantier**:
    - Standardkontrakter (EUs standardkontrakter - SCC)
    - Bindende virksomhetsregler (Binding Corporate Rules) (artikkel 47)
    - Godkjente adferdsnormer (artikkel 40)
    - Godkjent sertifiseringsmekanismer (artikkel 42)
  - **Internasjonale avtaler** mellom EU og tredjestater (som Privacy Shield)
  - **Særlige situasjoner**, herunder samtykke (artikkel 49)

Tredjestater

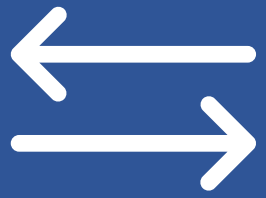


Godkjente land: Andorra, Argentina, Canada, Færøyene, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Sveits, Uruguay og Japan

Spesielt om EUs Standard Contract Clauses

- Tre varianter:
  - Behandlingsansvarlig til behandlingsansvarlig (2 stk)
  - Behandlingsansvarlig til databehandler
- IKKE databehandler til databehandler
  - Kan kun inngås av behandlingsansvarlig
  - Kan løses med fullmakt fra behandlingsansvarlig (kunden)
- Må alltid inngå databehandleravtale i tillegg – SCC er ikke dekkende som databehandleravtale
- Kan være del av andre avtaler
- Trenger ikke få godkjenning fra eller varsle Datatilsynet
  - Forutsatt at det ikke gjøres endringer i avtalene

Overføring?



- Ingen definisjon i lovverket (herunder GDPR)
- Typetilfelle:
  - Aksessering av data lokalisert i Norge fra tredjeland
  - Tilgang til system i Norge fra tredjeland
- Praksis i Norge
- Rammer ikke det at det gjøres tilgjengelig opplysninger på internett (offentlig) fra Norge

Bruk av databehandler i skyen

- GDPR artikkel 28: Behandlingsansvarlig skal kun bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.
- Databehandleren må kunne vise at man har gode nok tekniske og organisatoriske tiltak som sikrer at loven følges i praksis.
- Vurdering av om databehandleren kan vise frem tilstrekkelige garantier
  - Særlig se på databehandlerens dybdekunnskap, pålitelighet og ressurser.
  - Databehandleren er underlagt godkjente bransje-/adferdsnormer eller en godkjent sertifiseringsmekanisme er et moment i vurderingen
- Den behandlingsansvarlige må vurdere om databehandleren gir tilfredsstillende garantier sett i sammenheng med personopplysningene som skal behandles
- Datatilsynet mener at garantiene skal «dokumenteres»
  - ISAE3402, SOC2, ISO27001, ISO27002, ISO27018
- Databehandleravtale som dekker kravene i artikkel 28

Informasjonssikkerhet og skytjenester – noen problemstillinger

- Hvor data lagres
  - Norske krav
  - Personvernmessige krav (overføring til tredjestater)
  - Lokale regulatoriske krav (dvs. hvor dataene er lagret)
  - F.eks. CLOUD Act og utlevering til myndigheter
- Utlevering av data til behandlingsansvarlig (tilgjengelighet)
  - Etter personvernlovgivningen
  - Etter kontrakten
  - Dersom leverandøren opphører sin virksomhet
  - Mulighet til rettslige virkemidler for å få utlevert personopplysninger?

Oppsummering

- Overføring ut av / tilgang fra utenfor EØS-området
  - Skjer det overføring / tilgang?
  - Foreligger det grunnlag for overføring/tilgang?
  - Er det allikevel tillatt å overføre personopplysninger ut av EØS-området?
  - Hva om grunnlaget ikke fortsatt består?
- Gir skyleverandør «tilstrekkelige garantier»?
  - Er disse garantiene kontrollert?
  - Er garantiene dokumentert?
  - Databehandleravtale?
  - Får man dataene hvis noe skjer?

Takk for meg

Jan Sandtrø

Advokat MNA

+47 99731934

Jan@Sandtro.no

www.sandtro.no

linkedin.com/in/sandtro

twitter.com/JanSandtro