Schrems II oppsummert

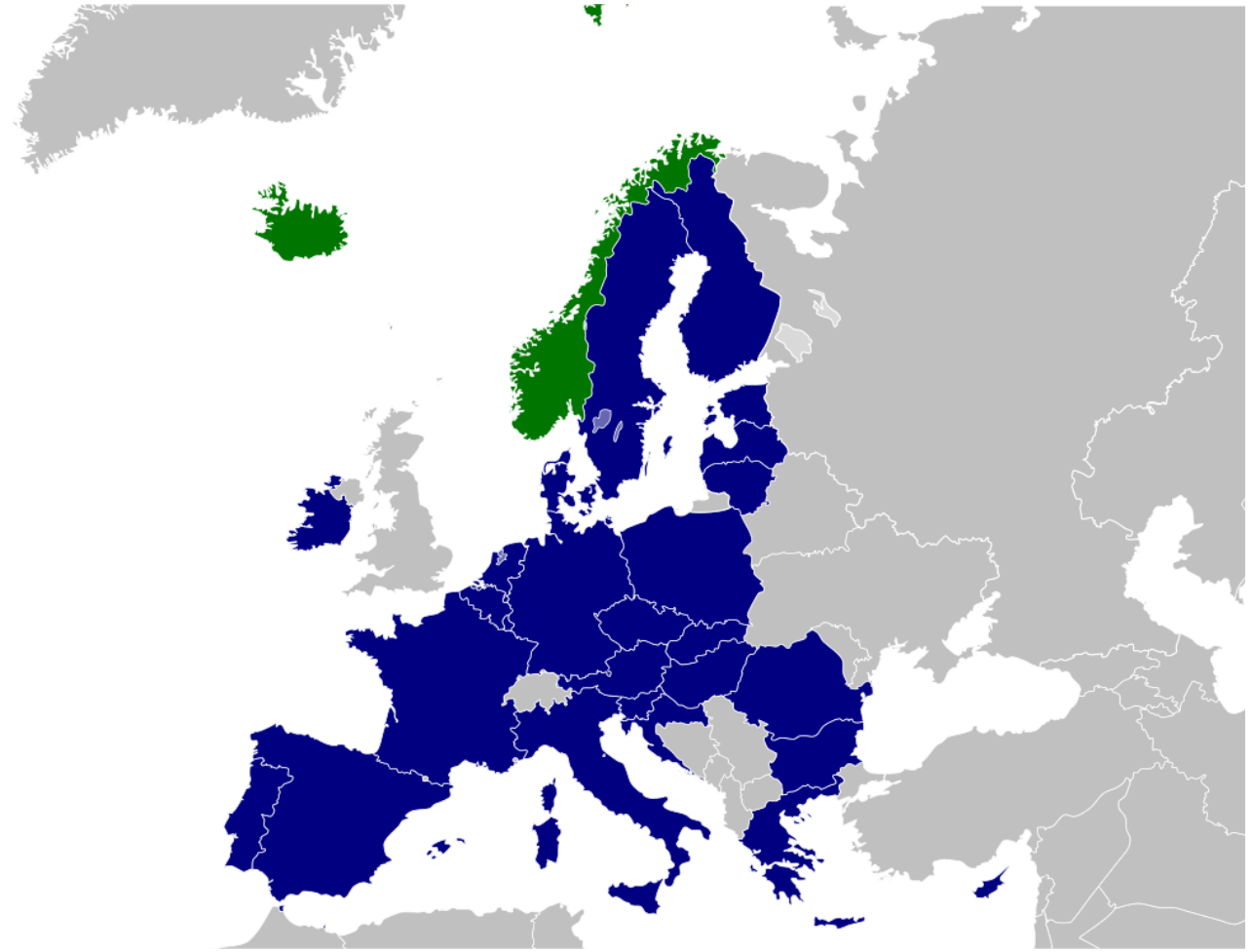
Veronica Jarnskjold Buer | avdelingsdirektør
Tobias Judin | seksjonssjef

NIFS 17. september 2021

Datatilsynet

Hvor i landskapet er vi?

- I EØS er personopplysninger «trygge»
- Vi kan overføre personopplysninger til tredjeland på visse vilkår
- Schrems II-dommen innskrenker denne adgangen
  - Privacy Shield (US) er ugyldig
  - Bruk av standardkontrakter etc. er ikke tilstrekkelig
- Det finnes også unntaksregler



Hvor i landskapet er vi?

- Dilemmaer for norske virksomheter
- Hvor er vi på vei?
  - Amerikansk overvåking
  - Det europeiske markedet
- Datatilsynets forventninger

Datatilsynet

Hva leter du etter?

MENY

Virksomhetenes plikter

Overføring av personopplysninger ut av EØS

All overføring av personopplysninger ut av EØS krever et særskilt grunnlag for å være lovlig. Her er en gjennomgang av hva som skal til for at personopplysninger kan overføres til land utenfor EØS.

Innhold

1. Innledning
2. Områder med tilstrekkelig beskyttelsesnivå
3. Ulike overføringsgrunnlag
4. Standard personvernbestemmelser som overføringsgrunnlag
5. BCR som overføringsgrunnlag
6. Tilleggskrav (Schrems II)
7. Opplysninger utelukkende behandlet i EØS
8. Unntak

Innledning

Virksomheten må ha identifisert om det finnes et overføringsgrunnlag før personopplysningene overføres til et tredjeland eller til en internasjonal organisasjon. Hvis det ikke finnes, er overføringen ulovlig. Det gjelder også hvis overføringsgrunnlaget ikke vil fungere i praksis.

Innad i EØS kan personopplysninger brukes, sendes og deles på tvers av landegrensene hvis man har et behandlingsgrunnlag. Det er fordi disse landene har de samme reglene for *behandling av personopplysninger*, nemlig *personvernforordningen*, også kjent som *GDPR*. Man kan derfor anta at personopplysningene vil være like godt beskyttet i alle land i EØS.

> **Merk!**
>
> Hvis du som privatperson skal sende dine egne personopplysninger ut av EØS, gjelder ikke disse reglene for deg.

To typetilfeller

- Man står selv for overføringen
  - Sende data til en mottaker utenfor EØS
  - Lagre data utenfor EØS
  - Få support fra tredjeland

- Underleverandøren handler på egne vegne
  - Man ber underleverandøren holde data innad i EØS, men underleverandøren sender likevel data til myndigheter i tredjeland

Underleverandøren handler på egne vegne

- Man kan instruere underleverandører (databehandlere) til å ikke overføre

- Dersom en underleverandør velger å overføre i strid med instruksjonene, er det underleverandøren som må forholde seg til Schrems II (de blir selv behandlingsansvarlige for overføringen)
  - I denne situasjonen må man risikovurdere underleverandøren og informasjonssikkerheten – en mer risikobasert tilnærming

- Hva hvis man aksepterer at underleverandør overfører – hva da?

Man står selv for overføringen

1. Know your transfers

2. Finn en overføringsmekanisme (eller unntaksregel)

3. Vurder om beskyttelsesnivået er tilstrekkelig i praksis?
    1. Er det et inngrep?
    2. Er et en krenkelse?

4. Iverksett ytterligere tiltak for å opprettholde beskyttelsesnivået

5. Dokumentasjon og periodisk revisjon

Forutsetning for informasjonssikkerhetsarbeidet

- Grunnlaget for informasjonssikkerhetsarbeidet vårt er lover og regler, retningslinjer, bransjenormer (og herunder sikkerhetsstandarder)
  - Dommen til Schrems II
  - FISA 702 (utlevering)
  - Executive Order 12333 (overvåkning/etterretning)
- Kunnskap om det juridiske er derfor helt avgjørende for å etablere tilstrekkelig personopplysningssikkerhet
- Fordi: Vi oversetter det juridiske til teknologisk

Slurping av data

- En handling der du tilegner deg konfidensiell data i mengder, mer korrekt personopplysninger

Tiltak mot slurping:

- Administrativ sikkerhet – føringene fra ledelsen - styrende dokumenter
  - Fysisk sikkerhet – adgangskontroll etc
  - Personell sikkerhet – kontroll på pc, låst pc, opplæring av brukere
  - Digital sikkerhet – Konfidensialitet, integritet, tilgjengelighet, robusthet
    - Tiltak som kryptering, anonymisering, pseudonymisering
    - Sterkere tiltak at du også håndterer nøklene selv
    - Tilgangskontroll
    - Osv.
  - Databehandleravtalen – DB forholder seg til kontrakt og instruksjoner
    - Rammeverk for koding, konfigurering, anskaffelse og innkjøp, utvikling, oppdatering etc.
    - Rammeverk for godkjenning av 3.partsverktøy, testing av bruk av sikkerhetsverktøy og verktøy
    - Rammeverk for intern kontroll av DB, herunder tredjepartsrevisjon av DB
    - Oppfølging av kontrakt – dynamiske kontrakter

Utleveringsbegjæringer

- FISA – godkjent utlevering av spesifiserte/målrettede personopplysninger
  - Eksempel på sikkerhetstiltak er at data som utlevert er kryptert
- Excecutive Order – overvåkning med egne midler
  - Eksempler:
    - In transit – kryptering, et effektivt tiltak
    - At rest –kryptering, et effektive tiltak både «slurping»/utlevering
    - In use – kryptering vil være et tiltak. Ref lovverket EO og FISA vil kontinuerlig overvåkning og utlevering, *i tillegg pålegg* leverandør /operatør til å gjøre systemendring, tillegge kode el. Usikkert om nevnte lovverk dekker en slik handling.

…kommer det en ny tid?

- Flere bevegelser
  - Nytt avtalegrunnlag før jul? (med selveste Biden i spissen)
  - Lisensiering av teknologi, plattform, drift, funksjoner osv. til europeisk eierskap
    - Google => Orange
    - Vil vi også se de andre 4 store tenke nytt?
  - Innovasjon egenutviklede europeiske skytjenester