Tredjelandsoverføringer

September 2021 | Eva Jarbekk

SCHJØDT

NY VEILEDER FRA PERSONVERNRÅDET/EDPB

- Prosess november-utkast – endelig versjon juni 2021
  - Mange høringsuttalelser om risikobasert tilnærming
- Konsekvens av Schrems II – ECJ - ikke datatilsynene selv
- Bakgrunn: menneskerettigheter – bl.a. ikke anledning for europeere til rettslige midler om overvåkning i USA
- ECJ og European Charter ikke bindende for oss, men viktig likevel

6 TRINN

Den arbeidskrevende delen av å gå over til nye SCC'er for ALLE overføringer - frist 27. desember 2022

1. Kartlegg overføringer – hvor er PO
2. Hva er overføringsgrunnlaget – (SCC, BCR, annet)
3. Er overføringsgrunnlaget effektivt (OK lovgivning og praksis i 3L?)
4. Hvis ikke – ytterligere tiltak?
5. Eventuelle formelle prosedyrer (ikke praktisk – godkjenning av DT)
6. Gjenta jevnlig

NY VEILEDER FRA PERSONVERNRÅDET/EDPB

En rekke eksempler – «Case 6» mest diskutert

- problematisk lovgivning OG data «in the clear» kan ikke avhjelpes med tekniske tiltak

Rammer mange virksomheter, både leverandører og kunder

NY VEILEDER FRA PERSONVERNRÅDET/EDPB

- Mange formuleringer litt uklare, f eks risikobasert eller ikke – evt hvor stort handlingsrom/aksept for risiko

- Vi hadde webminar med både norsk og dansk datatilsyn for å avklare

SENTRALE AVKLARINGER FRA DATATILSYNENE

STEG 1 – KARTLEGGING

- Enkle og sensitive/særlige PO omfattes
- Brukermetrikk/loggdata omfattes
- Fjernaksess omfattes
  - Viktig å sjekke it-avtaler for dette
- «Intragroup transfers» - som andre overføringer
  - BCR
  - Konserndatabehandleravtaler basert på gammel SCC
  - Filialer/medarbeidere på reise – artikkel 32

STEG 3 – HVA ER «EFFEKTIV»? RISKOBASERT/RISIKOAKSEPT?

Datatilsynene: (bekreftet skriftlig i oppsummering, kan deles)

- Ikke åpnet for risikobasert tilnærming
- EDPB bruker ikke ordet en eneste gang
- Men POs art kan vektlegges ifht om de faktisk rammes av overvåkning - ikke alle PO blir overvåket
- PO som er offentlige overvåkes sjelden, f eks epostadresser
  - Men brukslogg til en epostadresse er ikke offentlig og kan vise profil – viktig for brukermetrikk

..forts..

STEG 3 – HVA ER «EFFEKTIV»? RISKOBASERT/RISIKOAKSEPT?

- Sensitive og vanlige PO har samme beskyttelse
- Ikke stol på leverandørs utsagt alene, må verifiseres
- Antallet eventuelle utleveringer teller – hva om bare 1?
  - Gag-orders kan ofte rapporteres på aggregert nivå

- Dansk datatilsyn mener Kina, Russland og Ukraina har problematisk lovgivning, India og Singapore får ny personvernlovgivning, men har det ikke pt (da vanskelig å vurdere)

RÅD/ANBEFALING

Spør leverandørene

- «Hvem – hva – hvor – hvordan utleveres?»
  - Vær konkret i spørsmålene, ta utgangspunkt i dine PO
- Schrems' spørreskjema er litt omfattende, spisses mot FISA702

RÅD/ANBEFALING

- Dokumenter spørsmål og vurderinger
  - Ikke bruk ordet «risikobasert», EDPB gjør det ikke
  - Beskriv landets innsynspraksis på din type PO – f eks brukes de i fjernaksess-situasjon?
  - Verifiser leverandørens beskrivelser – be dem vise til hvor påstander underbygges – gjerne sektorvis
  - On en eneste utlevering til aktuelle myndigheter har skjedd – gjør nøye vurderinger – Datatilsynene er skeptiske – vær konkret

FORSTÅ CLOUD ACT

- Behandlingsansvarlig bestemmer – PO skal ikke til tredjepart
- En «riktig» databehandleravtale vil gjøre utleveringen ulovlig
- Om databehandleren likevel utleverer – avtalebrudd ihht art. 28
- Behandlingsansvarlig kan instruere databehandleren i å ikke utlevere – også etter inngått avtale

- Pga ikke en Kapittel 5 – problem så kan man bruke en mer risikobasert tilnærming – typen data spiller inn
- Spør leverandør om Cloud Act er brukt på din type PO – undersøk om gag-orders brukes (noe info er offentlig også om hemmelige begjæringer)
- Om man vet databehandleren utleverer, så velg en annen

STEG 4- SUPPLERENDE TILTAK

- Kryptering – transitt, at rest – OG i endring
  - Leverandør skal ikke se «data in the clear»
  - Nøkkelhåndtering er vesentlig
  - Bring-your-own-key er vanskelig
  - Shared-key kan fungere
  - Forskjellig vurderinger mht FISA702 og EO12333/annet
  - Kan få betydning for tjenestenivå

- Pseudonymisering
  - Praktisk i en del tilfeller

OVERORDNET FRA DATATILSYNENE

- Håndhevingen
  - Gjennomfør trinn 1-4 (minst) – ikke bare 1
  - Forskjell på gamle og nye overføringsavtaler? Ja!

- Det politiske perspektivet
  - Smerte for virksomheter – hvor lenge? 1-2 år?
  - CJEUs motiver for Schrems II
    - Forhandlingsposisjon
    - Bedre grunnlag for europeiske tjenestetilbydere – de er på vei, men løser ikke alt