Personvern i spesialisthelsetjenesten

Tor Åsmund Martinsen

Personvernombud

Oslo universitetssykehus HF

Om sykehuset

- Oslo universitetssykehus er
  - lokalsykehus for deler av Oslos befolkning
  - akuttsykehus for store deler av Oslo-området
  - regionsykehus for innbyggere i Helse Sør-Øst
  - Rikshospital med en rekke nasjonale oppgaver
- 24 000 ansatte
- Budsjett på ca. 27,5 milliarder kroner
- 1,1 mill. pasientbehandlinger pr år
- 3 mill. enkeltpasienter behandlet gjennom årene
- 250 mill. pasientoppslag pr år

Forskning og saksbehandling

- OUS står for ca halvparten av all helseforskning i Norge
- OUS har om lag 75% av prosjektene i HSØ
- 2021: 800 saker, hvorav ca 400 nye REK-studier og resten til kvalitetssikring og registre
- Det er p.t. 2300 aktive REK-studier ved OUS
- Ca 550 kvalitetsregistre

Behandlingsrettede helseregistre

- Pasientjournalsystemer
- Lab-systemer
- Radiologi/multimedia
- Medisinsk-teknisk utstyr
- DIPS Arena
- Felles regional journal
- Kjernejournal
  - Personvernkonsekvensvurderinger DPIA
  - Sky-løsninger

Forenklet oversikt

- Behandlingsrettede helseregistre
- Interne kvalitetsregistre
- Helseforskning
- Kvalitetsstudier/helsetjenesteforskning
- Brede forskningsregistre/medisinsk kvalitetsregister

Melding til PVO –> Protokoll iht GDPR -> tilbakemelding

Helseforskning

- **Hva sjekker vi i helseforskningsprosjekter?**
- Rettslig grunnlag
  - REK + GDPR - DPIA
- Lagring
- Utlevering
  - Dekker samtykket utlevering? Hvordan utleveres opplysningene? Viderebruk?
- Bruk av IKT (F.eks. app o.l.)

3. Land – overføringsgrunnlag?

Overføring til 3. land

Rødt lys: Artikkel 49
Unntak for særlige situasjoner

Gult lys: Artikkel 46
Nødvendige garantier

Grønt lys: Artikkel 45
Beslutning om tilstrekkelig beskyttelsesnivå

Overføringsgrunnlag

- Skal man overføre personopplysninger til 3. land må det foreligge et overføringsgrunnlag. Dette kommer i tillegg til rettslig grunnlag.

- GDPR Artikkel 44.
  - Enhver overføring av personopplysninger som behandles eller skal behandles etter overføring til en tredjestat eller til en internasjonal organisasjon, skal finne sted bare dersom den behandlingsansvarlige og databehandleren…oppfyller vilkårene i dette kapittel…

SCC

- EU-kommisjonens standardavtale (SCC) for overføring av personopplysninger til tredjeland er det mest brukte overføringsgrunnlaget, jf. GDPR artikkel 46 nr. 1 bokstav d).
- Formålet med et slikt overføringsgrunnlag er å sørge for at personopplysningene vil være like godt beskyttet ved overføring til et tredjeland, som de ville vært dersom overføringen fant sted mellom land i EU og EØS som er underlagt GDPR.

USA

- **Overføring til USA**
- **FISA - Foreign Intelligence Surveillance Act (FISA) Section 702**
- **Executive Order (E.O.) 12333**

  - **Det er viktig at virksomheten vurderer om overføringsgrunnlaget faktisk vil fungere slik det skal. Hvis overføringsgrunnlaget ikke sikrer god nok beskyttelse for personopplysningene i seg selv, må man i tillegg iverksette andre tiltak.**

Tilleggskrav

- Noen ganger er det ikke nok å ha et overføringsgrunnlag.
- Standard personvernbestemmelser er ikke bindende for tredjelandets myndigheter, og tredjelandets lover kan gå foran standard personvernbestemmelser.
- I noen tilfeller må standard personvernbestemmelser suppleres av ytterligere garantier og tiltak.
- Dersom det er nødvendig med ytterligere tiltak, men slike tiltak ikke iverksettes, er overføringen ulovlig og må opphøre.

Tiltak

- I utgangspunktet bør de ytterligere tiltakene inkludere tekniske tiltak. Hva som er effektivt i praksis, må imidlertid vurderes konkret i hver enkelt sak.

  - Kryptering og nøkkelhåndtering sentralt
  - Pseudonymisering. Særlig praktisk for forskning (prosjektspesifike løpenumre)
  - Juridiske og organisatoriske tiltak kan også være relevant

European Commission

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

March 2022

The European Commission and the United States reached an agreement in principle for a **Trans-Atlantic Data Privacy Framework.**

Key principles

- Based on the new framework, **data will be able to flow freely and safely** between the EU and participating U.S. companies
- A new set of rules and **binding safeguards to limit access to data** by U.S. intelligence authorities to what is **necessary and proportionate** to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- **A new two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a **Data Protection Review Court**
- **Strong obligations for companies** processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- **Specific monitoring and review mechanisms**