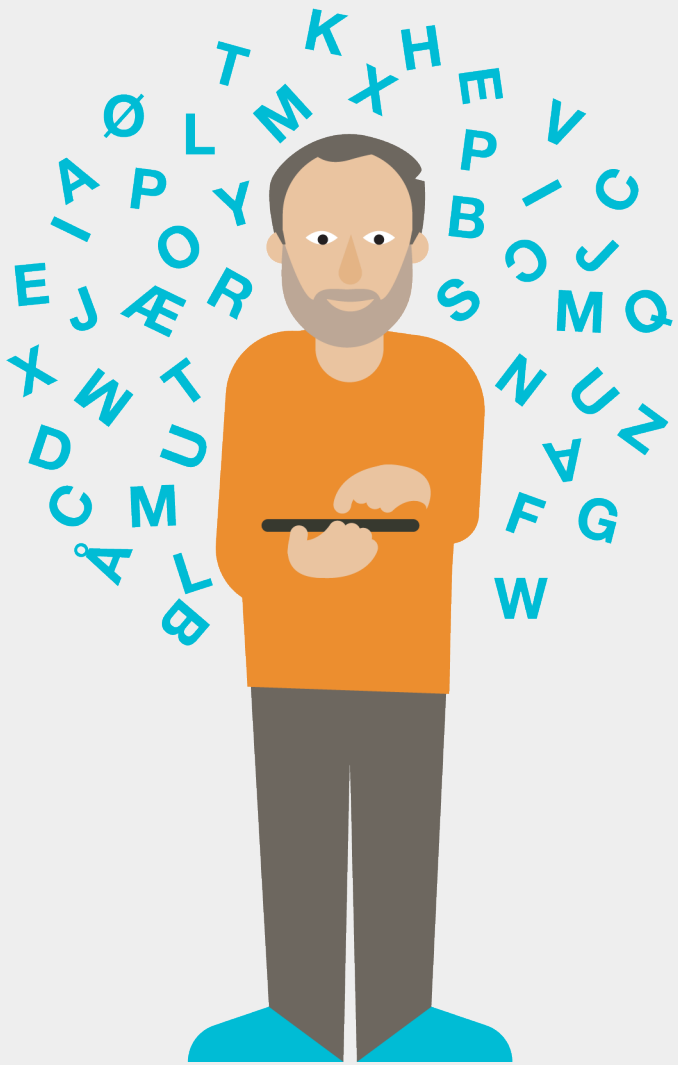
Utvalgte temaer innen personvern

17.02.2022

Kurset «Intro om Normen»

Personvern i Normen

- Personvern i Normen
- Personvernprinsippene
- Behandlingsgrunnlag
- Rettigheter
- Personvernkonsekvensvurdering (DPIA)
- Kort om Schrems II



NORMEN

Normens krav til behandling av helse og personopplysninger

- Dataansvarliges og databehandlers ansvar (Normen kap. 2)
- Behandlingsgrunnlag
- Plikter og krav ved behandling av helse- og personopplysninger
  - Taushetsplikten
  - Informasjon til den registrerte
  - Innsyn
  - Retting og sletting
  - Tilgjengeliggjøring og utlevering av opplysninger i behandlingsrettet helseregister
  - Retten til å motsette seg tilgjengeliggjøring og utlevering
  - Oppbevaring
  - Lagringstid
  - Behandlingsrettet helseregister ved opphør og overdragelse av virksomhet
  - Tilintetgjøring av dokumenter i behandlingsrettet helseregister mv. etter digitalisering
- Innebygd personvern
- Krav om databehandleravtale (Normen kap. 5.7)

Personvernkonsekvensvurdering

Risikovurdering med *personen* i fokus

Personvern
6 viktige områder

Avtaler og leverandører

Databehandleravtale
- Egen
- Databehandlers

Få kontroll på dataene

Personvernrettighetene

Oversikt over og kontroll med personopplysningene

Kartlegging

Lovlig behandling

Protokoll

Personvernprinsippene

Beskyttelse av personopplysningene

Informasjonssikkerhet

«God nok» sikkerhet

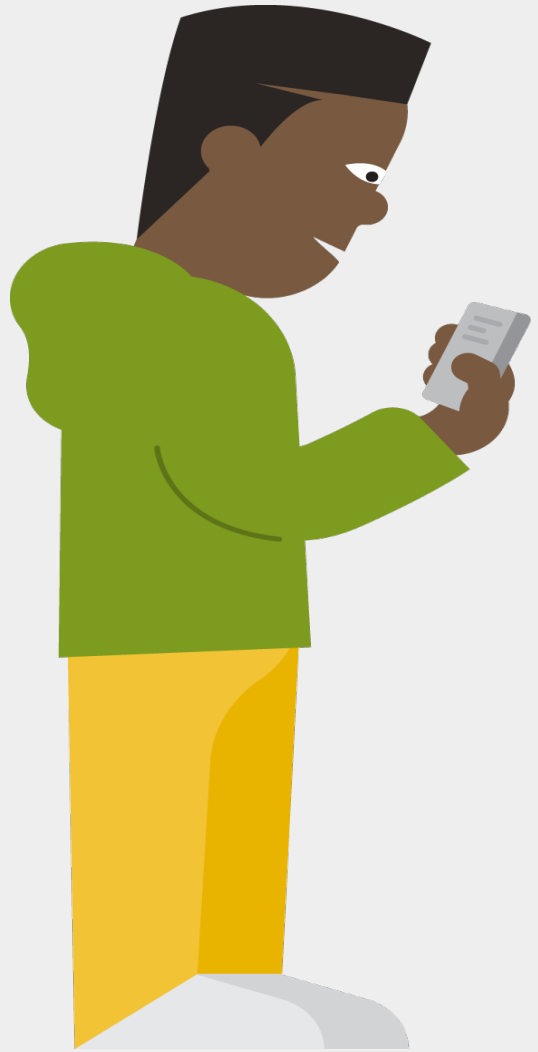
«egnede organisatoriske og tekniske sikkerhetstiltak»

ROS - risikovurderinger

NORMEN

Personvernprinsippene

Lovlig, rettferdig og gjennomsiktig
Formålsbegrensning
Dataminimering
Riktighet
Lagringsbegrensning
Konfidensialitet, integritet, tilgjengelighet
Ansvarlighet



NORMEN

Behandlingsgrunnlag, GDPR art. 6 og 9

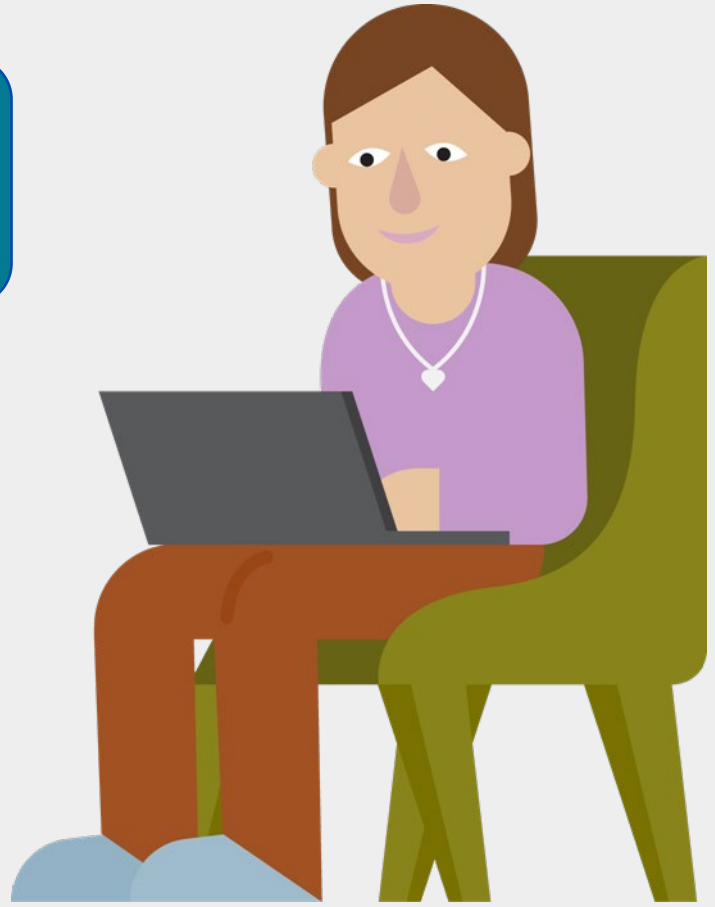
- Pasientbehandling forutsetter behandling av helseopplysninger om pasienten.
- All behandling av personopplysninger krever et lovlig grunnlag, som kalles behandlingsgrunnlag.
- Særlovgivingen inneholder en rekke slike lovlige grunnlag.
- Særlig om samtykke som behandlingsgrunnlag

NORMEN

Rettigheter i personvernlovgivningen

Retten til innsyn

Dataportabilitet



Sletting

Retten til informasjon

Retting

Personvernkonsekvensvurdering

- Risikovurdering for den registrerte
- Når må man gjennomføre en personvernkonsekvensvurdering? Når er det ikke nødvendig?
- Hvordan gjennomfører man en personvernkonsekvensvurdering?


Systematisk beskrivelse av behandlingen
Nødvendighet og proporsjonalitet
Risiko for de registrertes rettig-heter og friheter
Ledelsens validering av DPIA

Eksempel – elektronisk medisineringsstøtte

Normland kommune skal implementere elektronisk medisineringsstøtte. Medisindispenseren plasseres hjemme hos brukerne hvor et fjernpleiesystem gjør det mulig for ansatte å sjekke om pasienten/brukeren har tatt medisinene som de skal. Normland ønsker å forbedre pasientsikkerheten ved at pasienten/brukeren får rett medisin til rett tid og håper at medisinavvikene går ned.

Normland kommune gjør flere vurderinger (bl.a. risikovurdering, helsefaglige vurderinger) for å sikre at løsningen ivaretar krav til informasjonssikkerhet og personvern. De vurderer konsekvensene for personvernet til pasienten/ brukeren, om de har behandlingsgrunnlag og et klart formål og om det er nødvendig og gjennomføre en DPIA etter personvernforordningen artikkel 35. Kommunen gjennomfører den overordnende vurderingen. De vurderer at:

- innføringen av medisindispenserne ikke er en ny prosess da hjemmetjenesten i mange år har jobbet med medisineringsstøtte.
- løsningen ikke samler inn nye personopplysninger om pasientene enn det de allerede gjør
- personopplysningene som behandles ikke er så omfattende.
- teknologien ikke er ny siden dette er blitt brukt i mange andre kommuner
- leverandør får tilgang til opplysningene som registreres i teknologien
- det behandles helseopplysninger i form av type medisiner som kan avsløre et helseforhold.
- det ikke blir inngripende kontakt mellom tjenesten og pasient/bruker. Dersom pasienten/ brukeren ikke tar medisin som planlagt vil dette følges opp av hjemmetjenesten som normalt.

Kort om Schrems II

- Hva kom EU-domstolen frem til?
- Privacy Shield er et ugyldig overføringsgrunnlag
- EUs standardavtaler for overføring av personopplysninger kan brukes, men krever at partene innfører ytterligere sikkerhetstiltak.

- Hva er tilstrekkelige sikkerhetstiltak?

- Hva bør man gjøre nå?
- Kartlegg alle overføringer til tredjeland og hvilket overføringsgrunnlag som ligger til grunn
- Hvis behandlinger er basert på Privacy Shield, må man benytte et annet overføringsgrunnlag
- Risikovurdering. Man må sørge for at beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS, alle forhold tatt i betraktning.
- Dersom beskyttelsesnivået ikke er tilsvarende, må man iverksette ytterligere tiltak.

Spørsmålsrunde!