SYKEHUSET I VESTFOLD

Behandling av personopplysninger; Vurdering av personvernkonsekvenser (DPIA)

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	18.01.2023

1. HENSIKT

Hensikten med dokumentet er å avklare:

- **Hvorfor** personvernkonsekvenser skal vurderes
- **Når** det skal gjennomføres en personvernkonsekvensvurdering (DPIA[1]) og hva den skal inneholde
- **Hvem** som skal gjennomføre DPIA
- **Hvem** som skal godkjenne DPIA

2. ANSVAR

Administrerende direktør er dataansvarlig og har ansvaret for at behandling av personopplysninger gjøres med nødvendig sikkerhet og kun i samsvar med gyldig behandlingsgrunnlag.

Systemeier/Prosjektleder skal sørge for en vurdering av **om** det skal gjennomføres en DPIA og sørge for at det gjøres der svaret er JA.

Personvernombudet skal gi råd om hvordan den behandlingsansvarlige best mulig kan ivareta personverninteressene herunder gi råd om DPIA.

Ledere innen ulike enheter og områder har ansvar for å påse at denne prosedyren implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og blir fulgt.

Alle ansatte uansett arbeidsforhold i sykehuset som skal behandle personopplysninger, skal gjøre seg kjent med og følge prosedyren. Dette gjelder uavhengig av organisatorisk plassering og yrkesgruppe.

3. FREMGANGSMÅTE

En vurdering av personvernkonsekvenser skal sikre at personvernet til dem som er registrert i et informasjonssystem ivaretas. Det er flere kategorier registrerte i SiV; pasienter, pårørende, ansatte og besøkende.

En slik vurdering skal utføres i forkant av innføring, endring eller utfasing av alle prosesser og systemer der personopplysninger samles inn, registreres, sammenstilles, lagres og utleveres eller en kombinasjon av slike bruksmåter. Prosedyren skal videre sikre at denne vurderingen utføres på en måte som ivaretar de registrertes rettigheter og sikrer etterlevelse av personvernregelverket som stiller krav til personvern.

Personvernforordningen artikkel 35 definerer når sykehuset plikter å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den.

Vurdering av personvernkonsekvenser er en prosess som **alltid** skal gjennomføres for **alle** behandlinger av personopplysninger. En konkret vurdering av personvernkonsekvenser etter artikkel 35 gjentar denne prosessen, men da først og

[1] DPIA - Data Protection Impact Assessment

fremst for å finne de **ekstra** tiltakene som må til for å redusere en høy risiko som man ikke har klart å redusere tidligere. Dette skal gjøres **før** behandlingen starter.

Når det ikke finnes tilstrekkelige tiltak for å begrense risikoen til et akseptabelt nivå (det vil si at restrisikoen fremdeles er høy), er det krav om forhåndsdrøftelse med Datatilsynet.

I de tilfeller der deler av databehandlingen skjer utenfor SiVs godkjente IKT-løsninger, skal det sikres at tilfredsstillende vurdering av personvernkonsekvenser er gjennomført.

3.1 Momenter som taler for gjennomføring av en DPIA

Kriterier når DPIA kan bli et krav:

- Evaluering eller scoring, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
- Det fattes automatiske avgjørelser basert på informasjon om fysiske personer.
- Systematisk overvåking av registrerte. Eks i stor skala av et offentlig område.
- Særlige kategorier personopplysninger eller andre sensitive personopplysninger av høy personlig karakter (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
- Databehandling i stort omfang, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
- Kombinering eller sammenstilling av datasett.
- Personopplysninger vedrørende spesielt sårbare registrerte (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
- Innovativ eller nyskapende bruk av personopplysninger; bruk av biometriske data for tilgangskontroll, «Internet of Things-løsninger», velferdsteknologi osv.
- Databehandlingen innebærer bruk av ny teknologi som ikke har vært benyttet i pasientbehandling eller til registrering av ansattopplysninger tidligere.
- Når behandlingen i seg selv forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter etter loven eller avtale, eller bruke tjenester.

Datatilsynet har laget liste over behandlingsaktiviteter som **alltid** krever vurdering.

3.2 Hvem vurderer behov for og gjennomføring av DPIA?

Vurderingen av behov for - samt gjennomføring av DPIA, skal foretas av dataansvarlig virksomhet;

Interne prosjekter representert ved:

- Systemeier for applikasjoner og IKT-løsninger (informasjonssystemer)
- Prosjektleder for prosjekter som behandler personopplysninger

NB! Prosjektleder for forsknings-, kvalitets- og innovasjonsprosjekter skal fylle ut Internt skjema for behandling av personopplysninger i forskning, innovasjon og kvalitetssikring ved SiV som sendes til forskning@siv.no. Det interne meldeskjemaet inkluderer en DPIA egenerklæring. Prosjektene vil deretter sendes til NSD for vurdering av personvernet. NSD vurderer om behov for DPIA, lager utkast der det er behov og sender det til sykehuset for godkjenning.

For deltakelse i multisenterstudier skal Internt meldeskjema for deltagelse i multisenterstudier fylles ut. Sendes til forskning@siv.no.

Regionale prosjekter representert ved:

- Systemeier SiV for applikasjoner og IKT-løsninger (informasjonssystemer)
- Prosjektleder SiV for prosjekter som behandler personopplysninger

3.3 Gjennomføring

3.3.1 DPIA-team

Systemeier/prosjektleder oppretter et DPIA-team som avklarer behovet for og evt. gjennomfører DPIA. Systemeier/prosjektleder beslutter om DPIA skal gjennomføres.

DPIA-teamets sammensetning (anbefaling):
- Person med god kunnskap om behandlingen av personopplysninger i aktuelle prosjekt eller IKT-løsning
- Person som har utført eller deltatt i arbeidet med løsningsdesign og teknisk/funksjonell risikovurdering (T-ROS)
- Person med god kjennskap til og fortrinnsvis erfaring fra DPIA-arbeid

3.3.2 Avklare behov
DPIA-teamet fyller inn Del A og B i
MAL Personvernkonsekvensvurdering (DPIA) - Behandling av personopplysninger.
Dersom man i egenerklæringen svarer NEI på alle spørsmål, er det ikke behov for DPIA.
Dersom man ikke kan svare NEI på alle spørsmål, bør det gjennomføres en DPIA.
Beslutning tas av systemeier/prosjektleder.

3.3.3 Gjennomføre
DPIA-teamet fyller ut del C, D og E 1. – E 3.
MAL Personvernkonsekvensvurdering (DPIA) - Behandling av personopplysninger.
Personvernombudet fyller til slutt inn sin vurdering i del E 4 og sender DPIA til godkjenning til systemeier/prosjektleder og administrerende direktør.

3.4 Hvem godkjenner og signerer DPIA?
Administrerende direktør eller den oppgaven er delegert til, godkjenner og signerer DPIA og sørger for at den lagres på sak i sakarkivet (P360). Godkjenning innebærer å slutte seg til vurderingen, beslutte risikoreduserende tiltak eller akseptere restrisikoen.

3.5. Forhåndsdrøftelse med Datatilsynet
Administrerende direktør beslutter å anmode Datatilsynet om forhåndsdrøftelse.
Personvernombudet avtaler møte med Datatilsynet og deltar sammen med systemeier/prosjektleder.

4. GENERELT
En DPIA skal som minimum inneholde:
- Systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med databehandlingen.
- En vurdering av hvorvidt databehandlingene er nødvendige for formålet.
- En vurdering av risikoene databehandlingen medfører for de registrertes rettigheter og friheter, og hvilke planlagte tiltak som er gjort for å håndtere risiko og sikre vern av personopplysninger.
- Informasjon om overholdelse av adferdsnormer.
- Dersom relevant, skal den systemeier / prosjektleder innhente synspunkter om databehandlingen fra de registrerte eller deres representanter.

5. INTERNE REFERANSER
1.1.11.4.5	MAL Personvernkonsekvensvurdering (DPIA) - Behandling av personopplysninger

6. EKSTERNE REFERANSER

Personopplysninger | Datatilsynet
Behandlingsgrunnlag | Datatilsynet
Vurdering av personvernkonsekvenser (DPIA) | Datatilsynet
Veileder for utfylling av mal for personvernkonsekvensvurdering (17).pdf

7. VEDLEGG