Veileder for gjennomføring av regionale personvernkonsekvensvurderinger (DPIA)

Formål

Formålet med denne veilederen er å tydeliggjøre prosessen for personvernkonsekvensvurderinger (DPIA) ved gjennomføring av regionale prosjekter i Helse Sør-Øst.

Aktuelle brukere av veilederen kan være prosjekteiere og -deltakere, Regionalt personvernråd, personvernledere, Konsernfelles personvernombud, støttefunksjoner, tillitsvalgte og brukerutvalg (ikke uttømmende).

Avgrensning

Veilederen gjelder den regionale prosessen for personvernkonsekvensvurderinger (DPIA), og går ikke nærmere inn på tilstøtende prosesser som regional eller lokal porteføljestyring, lokale mottaksprosjekter på et enkelte helseforetak eller interne rutiner hos Sykehuspartner HF.

Prosessbeskrivelse (fra start til slutt)[1]

1. **Regionalt porteføljestyre beslutter oppstart av utviklingstiltak/prosjekt.**
   1.1. Formål og rettslig grunnlag bør være avklart før beslutning, og komme frem i saksunderlaget til Porteføljestyret.

   1.2. Dersom det på noe tidspunkt er behov for å fastsette foretaksgruppens felles syn på rettslig grunnlag, kan prosjektet ta spørsmålet inn i juridisk koordineringsnettverk til beslutning iht. rutiner for dette nettverket. Rettslig grunnlag kan dermed bli justert i løpet av prosessen.

2. **Prosjektet skal i en tidlig fase informere Regionalt personvernråd (PVR) om prosjektet**
   2.1. Det gjøres ved å oversende saksunderlag til sekretariatet for Personvernrådet (se praktisk informasjon nederst) med vurdering av

[1] Personvernombudet kan spørres om råd underveis i hele arbeidsprosessen med DPIA.

- formål
- rettslig grunnlag
- eventuelle forutgående personvernkonsekvensvurderinger
- prosjektets tidslinje
- hva prosjektet skal løse
- hvem som er dataansvarlig/databehandler

2.2. På grunnlag av denne informasjonen kan Personvernrådet i samarbeid med prosjektet planlegge videre prosess.

3. **Prosjektet utarbeider en personvernkonsekvensvurdering (DPIA) versjon 0.4.**
   3.1. Vurderingen dokumenterer konsekvenser (risiko) for personvernet, og om personvernrisikoen er høy (behov for fullstendig personvernkonsekvensvurdering (DPIA)) eller lav (DPIA versjon 0.4/pre DPIA).

   3.2. Vurderingen sendes til sekretariatet for Personvernrådet. Personvernrådet tar informasjonen til orientering, og kan gi skriftlig tilbakemelding dersom de mener det er nødvendig.

4. **Dersom det vurderes å være <u>lav</u> personvernrisiko er personvernkonsekvensvurdering (DPIA) versjon 0.4 prosjektets dokumentasjon på denne vurderingen** (også kalt "Pre-DPIA").

5. **Dersom det vurderes å være <u>høy</u> personvernrisiko skal det gjennomføres en fullstendig personvernkonsekvensvurdering (DPIA)**.

   5.1. Prosjektet utarbeider personvernkonsekvensvurdering (DPIA) versjon 0.75.

   5.2. Prosjektet avgjør sammen med helseforetakene hvilke helseforetak som skal ta i bruk løsningen først («utvalgte helseforetak»). De to eller tre første foretakene vil normalt være ansvarlige for å vurdere og gi tilbakemelding til prosjektet på utkastet til DPIA.

   5.3. I forbindelse med utarbeidelse av DPIA versjon 0.75 konsulteres brukerutvalget og/eller tillitsvalgte i det regionale helseforetaket og/eller i de utvalgte helseforetakene jf. punkt 5.2 ovenfor. Prosjektet må også sørge for tilstrekkelig involvering i ansvarlig linje og lederforankring med tanke på risikovurderinger som må innarbeides i personvernkonsekvensvurderingen.

   5.4. Prosjektet melder inn sak til Personvernrådet. Saksgrunnlaget gir oversikt og sammenheng i behandlingen av personopplysninger i prosjektet og risikobildet (høyeste risikoer og tilhørende risikoreduserende tiltak).

   5.5. DPIA sendes til gjennomgang i Personvernrådet via sekretariatet.

5.6. Prosjektet presenterer DPIA versjon 0.75 for Personvernrådet.

5.7. De utvalgte helseforetakene samarbeider om felles tilbakemelding til DPIA. Tilbakemeldingen gis på vegne av Personvernrådet.

6. **Prosjektet tar imot tilbakemeldingen** og behandler den før det utarbeides ny versjon av DPIA, som vil være versjon 0.8.

7. **DPIA versjon 0.8 sendes tilbake til Personvernrådet for gjennomgang**. Personvernrådet gir en felles anbefaling (v/de utvalgte helseforetakene) som tas inn i DPIA versjon 0.9.

8. **Personvernombudets vurdering**

8.1. Personvernombudet orienteres i egen oversendelse av DPIA versjon 0.9.

8.2. Dersom det er behov for det, vil personvernombudet gi ytterligere råd til DPIA 0.9. Ombudet vil prioritere å gi råd der ombudet vurderer at det er høyest personvernrisiko.

8.3. Personvernombudet dokumenterer sin vurdering og gir informasjon om den til prosjektet og Personvernrådet.

8.4. Personvernombudet har ikke myndighet til å beslutte eller akseptere personvernrisiko eller risikoreduserende tiltak på vegne av helseforetakene. Personvernombudet er heller ikke en del av helseforetakets saksbehandling av personvernkonsekvensvurderingene.

9. **Personvernombudets vurdering tas inn i endelig versjon**, som benevnes versjon 0.95.

10. **DPIA versjon 0.95 sendes til helseforetakene som forslag til felles DPIA**.

10.1. DPIA-en er ferdig som felles vurdering, men må anses som uferdig fordi den ikke omfatter vurdering av lokale risikoer.

10.2. Prosjektet oversender DPIA 0.95 til helseforetakene via P360. Følgende roller adresseres direkte med lokal personvernleder på kopi:
- lokal systemeier og systemansvarlig
- eventuelt faglig leder som eier prosessen (f.eks. fagdirektør eller forskningsdirektør).

10.3. Det enkelte helseforetaket må vurdere om det er lokale risikoer og ev. tiltak som gjør det nødvendig med lokale tilpasninger. I vurderingen av lokale forhold kan sannsynlighet for at risikoen oppstår variere ut fra lokale forhold i det enkelte foretaket.

10.4. Personvernleder konsulteres og gir en uttalelse som dokumenteres i den lokale versjonen av DPIAen.

11. Helseforetakene utarbeider lokale 1.0 versjoner

11.1. Personvernombudet vil i utgangspunktet ikke uttale seg om endelige lokale versjoner, med mindre det er konkrete ønsker om ny gjennomgang spesielt knyttet til høye lokale risikoer.

12. Etterfølgende endringer må vurderes med tanke på behov for å oppdatere personvernkonsekvensvurderingen.

12.1. Dersom det er avklart at endringen innebærer økt personvernrisiko er det nødvendig å gjennomføre en ny DPIA med tilhørende gjennomgang i Personvernrådet.

Praktisk informasjon:

Kontakten med Personvernrådet i DPIA-prosessen

Sekretariatet for Personvernrådet ligger i Helse Sør-Øst RHF ved fagsjef for personvern, Guro Gidske.

Sak meldes inn via denne lenken *Innmelding til personvernrådet.*

Håndtering av DPIA-dokumenter

DPIA-dokument i versjon 0.9 som skal sendes til personvernombudet legges inn av personvernleder i Teamskanalen - DPIA til PVO | HSØRHF-X-personvern HSØ | Microsoft Teams. Ved manglende tilgang sendes den til personvernombud@helse-sorost.no. Lagring på Teams-området vil da gjøres av personvernombudet.

På det felles området i Teamskanalen føres DPIA inn med dokumentnavn og andre opplysninger i excel-filen DPIA-oversikt.

Formålet med lagring av DPIA i Teamskanalen er felles dokumentasjon av hvilke DPIAer som er til behandling, og hvilken behandling de har fått.

DPIAene som ligger i Teamskanalen kan også ved behov kompletteres med mer informasjon som er relevant å samle på et felles sted i undermapper.

Merk at denne lagringen **ikke** har betydning for behovet for en felles oversikt over all dokumentasjon knyttet til personvernforhold som Sykehuspartner bør ha. Det erstatter heller ikke behovet for lokal dokumentasjon og dokumenthåndtering i lokal saksbehandlingsflyt i P360.

Behandling av DPIA hos personvernombudet
Når DPIA har blitt behandlet i en felles regional prosess vil DPIA i versjon 0.9 gjennomgås av personvernombudet. I de fleste tilfellene vil personvernombudet ha vært tett på i prosessen rundt utarbeidelsen og personvernledernes vurderinger i de ulike fasene. Personvernombudets involvering etter en slik grundig behandling fra personvernlederne vil kunne føre til at det ikke er behov for å gi noen uttalelse fra personvernombudet.

Dersom det er behov for det vil personvernombudet legge inn sin vurdering etter at personvernleder(-ne) har gitt sin vurdering. Der nasjonal mal fra Hdir er brukt vil det være i punkt E3 i dokumentet, og personvernombudet vil kunne bruke punkt E4.

Personvernombudet vil deretter gi beskjed til personvernlederne om innholdet i vurderingen, og avslutte med å oppdatere DPIA-oversikten.