Direktoratet for e-helse
Postboks 221 Skøyen,
0213 OSLO

postmottak@ehelse.no

Deres ref.:	Vår ref.:	Dato:
21/699-1	21/16187-2	29.11.2021

Folkehelseinstituttets høringssvar til ny mal for personvernkonsekvensvurdering (DPIA)

Bakgrunn

Direktoratet for e-helse har sendt på høring utkast til en ny veileder: «Mal for personvernkonsekvensvurdering med veiledning til utfylling». Veilederen skal gi virksomheter i helse- og omsorgssektoren en mal for og veiledning til gjennomføring og dokumentasjon av personvernkonsekvensvurdering i henhold til kravene i personvernforordningen artikkel 35. Den er en videreutvikling av Direktoratet for e-helses «Mal for DPIA»1 som ble publisert i 2019.

Direktoratet for e-helse ønsker tilbakemelding på følgende:

1. Er dette en hensiktsmessig utforming av en mal for personvernkonsekvensvurdering til bruk i helse- og omsorgssektoren?
2. Dekker veiledningen til utfylling det meste av det virksomheten bør være oppmerksom på når den gjør en personvernkonsekvensvurdering?
3. Er formatet hensiktsmessig? (PDF med både mal og veiledning til utfylling, samt mal i word-format)

Folkehelseinstituttets tilbakemelding og vurdering

Det er positivt at direktoratet har revidert eksisterende mal og veileder for personvernkonsekvensvurderinger og vi takker for muligheten til å gi innspill. Vi har hatt en intern prosess på tvers av områder og avdelinger for å kunne gi innspill på vegne av instituttet. Nedenfor følger FHIs innspill på de tre spørsmålene som direktoratet ønsker tilbakemelding på:

1. Er dette en hensiktsmessig utforming av en mal for personvernkonsekvensvurdering til bruk i helse- og omsorgssektoren?

Folkehelseinstituttet
Postboks 222 Skøyen
0213 OSLO

Telefon 21 07 70 00

folkehelseinstituttet@fhi.no
www.fhi.no
NO 983 744 516

Avdeling for rådgivning e-helse
Elisabeth Hagen

Malen er tilpasset helse- og omsorgssektoren generelt og retter seg ikke mot spesifikke deler av sektoren. Siden malen er ment å kunne benyttes for personvernkonsekvensvurdering til bruk i hele helse- og omsorgssektoren, er den nødvendigvis gitt en svært generell utforming. Det kan være hensiktsmessig å ha ulike maler for DPIA for ulike behandlingsaktiviteter. Ved FHI har vi valgt å utarbeide to DPIA-maler; én mal som benyttes for DPIA i forskningsprosjekter og én mal som benyttes for DPIA for systemer, registre og administrative løsninger.

Erfaringen i FHI er at brukerne ønsker seg mer avkrysning (alternativer) og mindre fritekstfelt. Det har også vært gitt innspill om at noe mer veiledningstekst og eksempler på utfylling bør ligge i selve malen og at begreper som brukes i malen må være entydig definert. Strukturen med inndeling i ulike deler virker fornuftig. Direktoratet nevner i veiledningen at virksomheten kan bruke del A, B og C, for alle behandlinger, men i realiteten vil mange stanse ved B dersom de kommer til at DPIA er unødvendig. Her kan vi kommentere at FHI har valgt å legge vurdering av behandlingsgrunnlag i den første delen av vår mal. Dette for å sikre at også de som etter behovsvurderingen konkluderer med at DPIA ikke er nødvendig, vil - som et minimum - likevel ha dokumentasjon for vurdering av behandlingsgrunnlag.

I innledningen til malen er det gitt noen definisjoner, blant annet personopplysning og helseopplysning. Vi ber dere vurdere å ta inn noen flere sentrale begreper, som f. eks særlig kategori personopplysning og datansvarlig.

Vurderingen av om en DPIA vil være nødvendig å gjennomføre i del B 2.1 flg. er sentral. FHI foreslår mindre justering der:

2.1. Når må virksomheten gjennomføre en personvernkonsekvensvurdering?:

- Et av kravene i personvernforordningen artikkel 35 (3) er oppfylt.
- Behandlingen er i Datatilsynets liste over behandlingsaktiviteter som alltid innebærer høy risiko for de registrertes rettigheter og friheter.
- To eller flere vurderingskriterier i artikkel 29-gruppens (EDPBs) veileder er oppfylt.
- Virksomheten har tidligere hatt konsesjon fra Datatilsynet eller godkjenning fra REK som er datert før juli 2018.
- Virksomheten har tidligere utført en personvernkonsekvensvurdering og ser et behov for å oppdatere denne pga. endring i behandlingen av personopplysninger.
- Virksomheten har etter en konkret vurdering kommet til at det sannsynligvis foreligger høy risiko for de registrertes rettigheter og friheter (legg vurderingen til i lista over vedlegg, se punkt 1.7).

2. Dekker veiledningen til utfylling det meste av det virksomheten bør være oppmerksom på når den gjør en personvernkonsekvensvurdering?

Malen og veiledningen dekker kravene til hva en personvernkonsekvensvurdering skal inneholde etter GDPR artikkel 35. Vi har ikke gjort en selvstendig vurdering, men må også forutsette at den bygger på Datatilsynets veileder om personvernkonsekvensvurderinger og andre aktuelle standarder.

Veiledningen for punkt 2.1 samsvarer ikke med nummereringen i selve malen. Veiledningen viser til punkt 2.1.1 osv., men malen har ingen underpunkter under punkt 2.1.

3. Er formatet hensiktsmessig? (PDF med både mal og veiledning til utfylling, samt mal i word-format)

Med den utformingen malen er gitt, hvor det blant annet i stor grad forutsettes utfylling av vurderinger og tekst i egne fritekstfelt synes det hensiktsmessig å ha malen i word-format. Vi har sett eksempler på DPIA-maler i tabeller i excel, men det fremstår lite hensiktsmessig all den tid en DPIA forutsetter mye tekst i beskrivelser, begrunnelser og vurderinger. Brukervennligheten ville imidlertid vært bedre med bla. nedtrekksfelt med alternativer der det er mulig og «pop-ups» med veiledningstekst. Det tar mye tid å bytte frem og tilbake mellom selve malen og veiledningen.

Av hensyn til effektivitet og behov for internkontroll kan prosessen med gjennomføring av DPIA med fordel koordineres elektronisk til andre prosesser internt, f.eks. vil deler av kjerneinformasjonen (del A) og beskrivelsen av behandlingen (del C) være informasjon som må fylles inn i virksomhetens behandlingsprotokoll. Det oppleves som unødvendig tungvint å fylle ut mye av den samme informasjonen flere steder, men vi har altså og enn så lenge ingen bedre løsning for dette ved FHI. Vi vil derfor fremsette som et fremtidig ønske at malen blir elektronisk og kan integreres med andre systemer for forenkling av utfylling. For eksempel på den måten at en utfylling av DPIA-mal kan integreres i eller lenkes til i løsninger for behandlingsprotokoller etter personvernforordningen artikkel 30.

Vennlig hilsen

Susanne Abusdal Hegg
Avdelingsdirektør (fung)

Elisabeth Hagen
Seniorrådgiver

Liste over mottakere:
Direktoratet for e-helse