Svar på høringsutkast «Ny veileder: Mal for personvernkonsekvensvurdering (DPIA) med veiledning til utfylling»

Helse Midt-Norge henviser til høringsutkast for «Ny veileder: Mal for personvernkonsekvensvurdering (DPIA) med veiledning til utfylling» fra direktoratet for E-helse. En arbeidsgruppe bestående av ressurser fra foretak i Helse Midt-Norge har utarbeidet et felles høringssvar, og vi vil med dette brevet gi vårt svar.

Tilbakemelding på DPIA-veileder og mal

Overordnet er høringsutkastet et godt dokument. Veiledningen er informativ, både for de som skal arbeide med dokumentet, men også for personvernombud og andre som jobber med personvern. Malen har en hensiktsmessig utforming og gir et godt grunnlag for dokumentasjon og revisjon i samme dokument. Ett helseforetak i regionen (Helse Nord-Trøndelag) har tatt i bruk malen i en konkret DPIA og er fornøyd.

Overordnet er Helse Midt-Norge fornøyd med veileder og mal.

Helse Midt-Norge ser likevel at veileder og mal kan forbedres ytterligere. Våre kommentarer, innspill og forslag er oppsummert i punktlisten nedenfor:

1. Skjemaet inneholder mange vage spørsmål og fritekstbokser. Det er i praksis vanskelig for mange å forholde seg til dette. Det vil være ønskelig med flere klikkbare alternativer tilpasset helsevirksomhet i malen, som i praksis gir veiledning og hjelp til rask utfylling. For eksempel kan ulike formål defineres som alternative avkrysningsbokser, avhengig av om det er helsehjelp, forskning, administrasjon etc. Det samme gjelder behandlingsgrunnlag, som også enkelt kan oppstilles som alternativer. (for eksempel «GDPR art. 6 (1) bokstav a (samtykke)»), slik at brukerne lettere og kjappere kan navigere seg gjennom. Da støtter man også lettere analyse av gjennomførte DPIAer i etterkant. Fritekstbokser kan gjerne komme som tillegg til avkrysningsbokser Det vil være nyttig å legge ved flere eksempler på utfylte DPIAer
2. Det vil være nyttig i veiledningen å legge ved enda flere eksempler på utfylte DPIAer, da mange lærer lettere av å se på hvordan andre gjør det, enn å lese teori om hvordan det skal gjøres
3. Gjennomgående ved vurdering av risiko: Overordnet beskrivelse av hva en «risiko» er, og hva «rettigheter og friheter» innebærer, mangler. Det listes opp en rekke eksempler på behandlinger som krever DPIA, f.eks. iht. Datatilsynets liste, eller etter WP29-gruppens punkter, men det gis ingen innføring i andre vurderinger. For at en dataansvarlig skal settes i stand til å vurdere konkrete behandlingsaktiviteter i eget hus, må de ha en forståelse av hva rettigheter og friheter er, hvordan disse verdiene kan krenkes, og hva som i så tilfelle medfører en risiko, på et generelt plan, og ikke kun gjennom eksemplifiseringer.
4. Mal, del A: Tydeliggjøring av ansvarsfordeling mellom felles dataansvarlige.
5. Mal, del A: Databehandlere, underleverandører og andre parter, bør fremgå.
6. Mal, del C, punkt 3.3: Ansatte anses gjerne som en sårbar gruppe, særlig i tilfeller hvor samtykke etterspørres. Det bør derfor tydeliggjøres at samtykke fra ansatte bør være gjenstand for vurdering av fritt avgitt samtykke. Dette begrunnes med skjevhet i maktforhold og –balanse mellom den registrerte og dataansvarlig.
    a. Veiledning til del C, punkt 3.3 og 3.4: Det bør fremgå at ansatte kan anses som sårbare registrerte, da de står i et avhengighetsforhold til dataansvarlig (arbeidsgiver), og at samtykkekompetanse er innskrenket i tilfeller med skjevt maktforhold, f.eks. i forbindelse med søking på jobb.

7. Mal, del D, punkt 4.3: Direktoratet har et uttalt formål om at malen skal være tilgjengelig for flertallet, uavhengig av personvernkompetanse, jf. side 2 i høringsbrevet: «Veilederen og malen skal være anvendelig uavhengig av kompetansenivå innen personvern.» Vurderingen av hvorvidt en behandling kan sies å ha iboende risikoer for den registrertes «rettigheter og friheter» er ikke umiddelbart et tilgjengelig konsept for personer «uavhengig av kompetansenivå innen personvern». Her bør tydeligere veiledning til. Veiledningen til del D bidrar ikke med oppklaringer.
8. Bør være hjelpetekster til hvert punkt (som ikke vises hele tiden, men som man kan trykke på og få opp). På den måten slipper man å rulle og opp ned i malen.
9. Eksemplifisering bør også fremgå i større grad.
10. Veileder anbefales å «webifiseres», f.eks. tilsvarende «Normen». Dette vil øke lesbarhet og anvendelighet
11. Veileder og mal kan fremstå som omfattende for foretak som behandler personopplysninger i mindre skala. At både veileder og mal er i ett dokument er med på å forsterke dette inntrykket
12. Det er ønskelig med flere helserelaterte eksempler, herunder eksempler relatert til forskning
13. Det bør vurderes om veilederen, og eksempler, i større grad kan omfatte DPIA av IKT-systemer
14. For øvrig noen skrivefeil, ulike fonter og andre småfeil.