AKERSHUS UNIVERSITETSSYKEHUS

DIREKTORATET FOR E-HELSE
Postboks 221 Skøyen
0213 OSLO

Deres ref	Vår ref	Saksbehandler	Dato
21/699	21/12448-8	Knut Thomas Sjølie	23.11.2021

Svar på høring - Mal for personvernkonsekvensvurdering (DPIA) med veiledning til utfylling

Viser til deres brev av 19.10.2021 vedrørende høring om mal for personkonsekvensvurderinger (DPIA) med veiledning og utfylling. Ahus' høringssvar følger under i tre kapitler, i tråd med direktoratets ønsker om spesifisert tilbakemelding.

Overordnet mener Ahus det kan være hensiktsmessig med felles mal for DPIA. Dette kan forenkle og stimulere til større grad av deling og gjenbruk av DPIA. En god mal og veiledning for DPIA er en forutsetning for å øke bruken av felles mal-dokument.

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

Ahus mener det er hensiktsmessig at personvernkonsekvensvurderingen er fristilt fra veiledningsmateriellet. På den måten blir DPIA-dokumentet mer oversiktlig, brukervennlig og lettlest.

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

Om malen og veilederen

- Bakgrunn

Det er uttalt at malen og veilederen skal være anvendelig, uavhengig av brukerens kompetansenivå innen personvern. Det er derfor viktig å løfte frem at vurderingene skal ta utgangspunkt i den registrertes perspektiv. Vurderingene skal ta for seg konsekvensene for den registrertes rettigheter og friheter. Det er ikke forklart hva som menes med disse rettighetene og frihetene, dette kan med fordel fremkomme.

Ahus mener det er positivt at det fremheves at man bør ha identifisert et lovlig grunnlag for databehandlingen før det er aktuelt å gjøre en personvernkonsekvensvurdering. Ahus mener det er utfordringer knyttet til formål som er for overordnet og vagt formulert, se punkt 3.3.3. Ahus foreslår at formål og lovlig grunnlag for databehandlingen, bør løftes lenger frem i mal-dokumentet, gjerne som en ny del B.

Ahus støtter at arbeidet med å vurdere personvernkonsekvenser bør startes i konseptfasen. Dette bør fremheves, gjerne med en egen underoverskrift tidlig i dokumentet.

Postadresse:
Akershus universitetssykehus HF
Postboks 1000
1478 LØRENSKOG

Besøksadresse:
Sykehusveien 25
Nordbyhagen

Telefon: +47 67 96 00 00
E-post: postmottak@ahus.no

Bank: 8601.71.65447
Org.nr: 983 971 636
Web: www.ahus.no

- Definisjoner

Til definisjon av «dataansvarlig»: Formuleringen i annet punktum er upresis. Begrepet «dataansvarlig» brukes i norsk helselovgivning istedenfor «behandlingsansvarlig» for ikke å blande dette sammen med den som er behandlingsansvarlig for helsehjelp.

Definisjonen av begrepet «personopplysning» bør komme før definisjonen av «helseopplysning». Ahus mener at det er fornuftig å skille begrepene, selv om samlebetegnelse «helse- og personopplysning» henger igjen i litteratur og veiledere innen helse- og omsorgssektoren. En helseopplysning er en personopplysning, og det er derfor unyansert og kunstig når disse fremstilles som to ulike kategorier. Man bør heller definere begrepet «særlige kategorier av personopplysninger» etter artikkel 9, der helseopplysninger inngår som én kategori. Det er ikke utelukkende helseopplysninger som behandles etter artikkel 9, ei heller i helsesektoren.

Merknader til malen

- Til Mal del C

Det er lagt opp til en mal i ulike deler, der delene kan benyttes om hverandre etter virksomhetens behov. En slik tilnærming er hensiktsmessig. Med en slik tilnærming mener vi imidlertid det kan være en fordel at lovlig grunnlag for databehandlingen og formålsangivelsen løftes ut av del C og inntas i en ny del B. Dette vil kunne være en naturlig plassering dersom alle deler av malverket skal fylles ut. Man må ha formål og lovligheten klart for seg før man gjennomfører en behovsvurdering (nåværende del B).

- Mal del D

Tilnærmingen som er foreslått, vil gi en god oversikt over risikoer og hvordan redusere disse. Direktoratet kan imidlertid vurdere om det skal inntas diagram tilsvarende de som benyttes i ROS, som viser sannsynlighets- og konsekvens før og etter tiltak.

- Til Mal del E

Det er positivt at man i malen inntar innspill fra de registrerte, brukerrepresentanter og andre interessenter. I innledningen fremgår det at dette ikke er obligatorisk, jf. ordet «kan», mens man i punkt 5.1 spør om hvilke innspill man har fått, som gir inntrykk av at dette er obligatorisk. Her bør man omformulere spørsmålsstillingen i punkt 5.1.

Merknader til veilederen

- Veiledning til del A: Kjerneinformasjon

I punkt 1.1 og 1.2 skal det oppgis navn på dataansvarlig og hvilken rolle denne har. Her bør det inntas en veiledning for å vurdere hvem som er dataansvarlig, gjerne med henvisning til EDPBs Guidelines 07/2020 on the concept of controller and processor in the GDPR. For de fleste databehandlinger er det klart hvem som er dataansvarlig. I enkelte tilfeller hvor flere er involvert i prosessen, må dataansvaret baseres på en konkret vurdering. Dataansvaret identifiseres ut fra hvem som "bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes", jf. personvernforordningen artikkel 4 nr. 7. Artikkel 29-gruppen og EDPB har pekt på at kriteriet "bestemmer" oppsummert kan deles inn i kontroll basert på eksplisitt juridisk kompetanse, kontroll basert på implisitt kompetanse, og kontroll basert på faktisk innflytelse. EDPBs veiledning gir tolkningsbidrag til hva som ligger i kriteriet "bestemmer". Det legges til grunn at dataansvar identifiseres ut fra hvem som har "decision-making power" over formål og midler. Det sentrale er altså hvem som har bestemmelsesrett, og ikke om den er utøvd. Manglende utøvelse av dataansvar kan derfor ikke tas til inntekt for at virksomheten ikke er dataansvarlig.

Ahus mener det er viktig med god deltakelse i personvernkonsekvensvurderinger. Det er flere eksempler hvor slike prosesser er overlatt til én person alene. Det er positivt at man omtaler dette i punkt 1.5. Ahus anbefaler at man benytter informasjonssikkerhetsrådgiver eller lignende, fremfor eller i tillegg til «CISO» som eksempel på ressurser man kan rådføre seg med.

- Veiledning til del B: Behovsvurdering

Som tidligere nevnt under punkt 3.1.1 er det hensiktsmessig å innta en forklaring av hva de registrertes rettigheter og friheter er. Uten å vite dette, vil det være vanskelig å vurdere hvilken risiko behandlingen vil utgjøre for disse.

- Veiledning til del C: Beskrivelse av behandling av personopplysninger

I veilederen er det utstrakt bruk av henvisninger til eksterne lenker som beskriver og utdyper temaer som omtales, som er bra. Det mangler imidlertid grunnleggende informasjon i veilederens punkt 3.1 om hvordan man skal beskrive formålet. Dette bør inntas i veiledningsteksten. Det bør fremgå i teksten at formålet må være konkret angitt og formidles klart, slik at det er mulig å vurdere om de registrerte opplysningene er nødvendige, og om behandlingen skjer i overensstemmelse med forordningens bestemmelser. Formålet har helt sentral betydning for vurderingen av hvilke rettslige rammer som oppstilles for den aktuelle behandlingen, og gjelder blant annet lovvalg, hvilke opplysninger som kan samles inn og varigheten av databehandlingen.

Den samme mangelen på veiledning viser seg også i punkt 3.11 om prinsippene og i punkt 3.12 om rettigheter. Det bør som et minimum inntas en kort forklaring i veiledningen av hva som ligger i de ulike prinsippene og til rettighetene. Henvisningene til eksterne linker bør heller gi utdypende informasjon.

Som tidligere nevnt anbefaler Ahus at formålsangivelse og lovlig behandling av personopplysningene inntas som en egen del. Direktoratet kan også vurdere å innta eksempler på hjemmelsgrunnlag etter personvernforordningen og nasjonal lovhjemmel på vanlige behandlinger innen helse- og omsorgssektoren.

Er formatet hensiktsmessig?

Formatene er kjente, og vil kunne tas i bruk i virksomheten umiddelbart. Det er også lett å innta dette i dagens system.

Med hilsen
Akershus universitetssykehus HF

Øystein Mæland
Administrerende direktør

Knut Thomas Sjølie
Spesialrådgiver

Dokumentet er elektronisk godkjent

Vår dato
23.11.2021

Vår referanse
21/12448-8

Mottaker	Kontaktperson	Adresse	Post
DIREKTORATET FOR E-HELSE		Postboks 221 Skøyen	0213 OSLO