Deloitte Advokatfirma AS
Dronning Eufemias gate 14
Postboks 221 Sentrum
NO-0103 Oslo
Norway

Tel: +47 23 27 96 00
Fax: +47 23 27 96 01
www.deloitteadvokatfirma.no

Direktoratet for e-helse

Deres ref 21/699

30. november 2021

Høringssvar - Ny veileder: Mal for personvernkonsekvensvurdering (DPIA) med veiledning til utfylling

Deloitte Advokatfirma viser til Direktoratet for e-helse sin høring av ny mal og veileder for gjennomføring av personvernkonsekvensvurdering og vil med dette benytte sjansen til å komme med enkelte innspill til direktoratets publiserte forslag.

Vi vil innledningsvis understreke at utkastet til både mal og veileder er svært godt og fremstår som gjennomarbeidet. Både mal og veileder er pedagogisk oppbygd med mange gode eksempler som gjennomgående gjør det enklere å bruke malen operativt. Grepet med løpende henvisninger til kilder for mer informasjon og ytterligere veiledning er etter vår oppfatning også veldig nyttig. Gjennom vår omfattende praktiske erfaring fra gjennomføring av personvernkonsekvensvurderinger i ulike virksomheter, ikke minst fra arbeid med å bistå kunder som ikke har tilsvarende erfaring, har vil likevel noen innspill som vi håper kan bidra til ytterligere forbedring. Vi har i hovedsak strukturert høringssvaret vårt etter punktene Direktoratet for e-helse særlig har bedt om innspill på.

Om Deloitte

Deloitte er en av Norges største leverandører av rådgivningstjenester til helsesektoren. Flere av våre konsulenter og advokater har spisskompetanse og bred erfaring fra oppdrag på og bistand til både regionalt nivå og hos helseforetakene, men også for mindre aktører som ikke har den samme kompetansebase som et helseforetak.

Personvern har i flere år vært et satsningsområde for Deloitte globalt og vi er i dag verdensledende når det gjelder rådgivning knyttet til personvern, GDPR og informasjonssikkerhet. I Norge har Deloitte Advokatfirma 17 advokater og advokatfullmektiger som daglig arbeider med juridiske problemstillinger på disse områdene og som til sammen har svært bred og variert erfaring fra juridisk rådgivning og operativ juridisk bistand. Vi har lang erfaring med å bistå både offentlige og private virksomheter med alle typer problemstillinger knyttet til deres bruk/behandling av personopplysninger som ledd i store digitaliserings- og utviklingsprosjekter.

I Deloitte jobber vi aktivt for å være en tydelig stemme og ledende aktør innen digital transformasjon av helsesektoren. Deloittes helsegruppe har dedikerte konsulenter med helse- og medisinfaglig bakgrunn, teknologispesialister, innovasjonsspirer, portefølje-, program- og prosjektledereksperter samt advokater/jurister med personvernrettslig ekspertise, som er begeistret for teknologiens muligheter.

Vår erfaring fra personvernarbeid og fra helsesektoren generelt, sammen med vår spesielle erfaring fra digitaliseringsarbeid, har gitt oss særlig god innsikt i de utfordringer små og store virksomheter i helse- og omsorgssektoren står overfor når de skal gjennomføre personvernkonsekvensvurderinger.

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

Deloitte er av den oppfatningen at malen er hensiktsmessig utformet. Som nevnt over, mener vi både mal og veileder er pedagogisk oppbygd med mange gode eksempler som gjennomgående gjør det enklere å bruke malen operativt. At det løpende henvises til kilder for mer informasjon og ytterligere veiledning er etter vår oppfatning også veldig nyttig

Vi vil imidlertid likevel foreslå å bytte plass på del B – behovsvurdering og del C - beskrivelse av behandlingen av personopplysninger. Årsaken til at vi foreslår dette, er at det alltid er nødvendig å ha oversikt over behandlingen for å kunne vurdere om det er sannsynlig at behandlingen kan innebære en høy risiko for den registrerte, og således vil innholdet i del C være nødvendig for å vurdere behovet for å måtte gjennomføre en personvernkonsekvensvurdering.

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

Deloitte er av den oppfatning at veiledningen dekker det meste av det virksomheten bør være oppmerksom på når det gjør en personvernkonsekvensvurdering. Vi har imidlertid noen innspill som vi tror kan forbedre veiledningen ytterligere, spesielt med tanke på den delen av målgruppen som er små virksomheter med begrenset tilgang til personell med fagkompetanse innen personvernregelverket. Tilbakemeldingen gis ved å kommentere enkelte punkter i mal/veiledning under.

Felles dataansvar, punkt 1.2

Det kan være vanskelig å avgjøre om det foreligger felles dataansvar og det er derfor bra at det er en god og forklarende tekst i veileder. Vår erfaring tilsier at flere virksomheter gjennomfører denne vurderingen alene, uten at den andre dataansvarlige involveres. Manglende involvering av den andre dataansvarlige kan føre til at det gjøres feil vurderinger og at man heller ikke får inngått den avtale (arrangement) som personvernforordningen krever, særlig for å sikre tilstrekkelig ansvarsfordeling. Det er også vår oppfatning at dersom slike vurderinger først er gjennomført bør de dokumenteres for å synliggjøre for ettertiden hvilke forhold som gjorde at det ble konkludert med felles dataansvar.

*Indikasjoner på at personvernkonsekvensvurdering må gjennomføres, punkt 2.*1

Det bør komme frem at det i denne pre-vurderingen er viktig å forsikre seg om at man har lov til å gjennomføre selve behandlingen. Dersom del C – beskrivelse av behandlingen av personopplysninger gjennomføres og dokumenteres før del B – vil dette være ivaretatt.

Har personvernombudet uttalt seg i vurderingen av behovet for å gjennomføre en personvernkonsekvensvurdering, punkt 2.2

Dersom man svarer nei på dette punktet, bør det fremgå en kort begrunnelse for hvorfor personvernombudet ikke har uttalt seg. Dette for å øke bevisstheten om at ombudet bør rådføres i vanskelige avgjørelser. Personvernombudet vil, i motsetning til de fleste andre i en virksomhet, ha mengdetrening hva gjelder gjennomføring av personvernkonsekvensvurderinger og vurdering av vanskelige personvernspørsmål. Personvernombudets erfaringer vil derfor gjøre ombudet til en nyttig sparringspartner.

Sett inn begrunnelsen for hvorfor virksomheten har kommet til at det skal/ikke skal gjennomføres en personvernkonsekvensvurdering, 2.4

Se våre kommentarer til punkt 2.2. Dersom personvernombudet ikke har vært involvert, bør det kort begrunnes.

Beskriv de forskjellige behandlingsaktivitetene som inngår i vurderingen, punkt 3.6

Teksten i veilederen er god og det er en stor fordel at lagringstid etterspørres samtidig som behandlingsaktiviteten skal beskrives. Vår erfaring tilsier imidlertid at det kan være fordelaktig at det i veilederen beskrives noe rundt *hvordan* lagringstid skal vurderes.

Videre tilsier vår erfaring, at enkelte virksomheter, ved utarbeidelse av behandlingsprotokoller, deler opp behandlingen i veldig mange behandlingsaktiviteter, i stedet for å beskrive en helhetlig prosess med ett behandlingsgrunnlag. Dette kan medføre at gjennomføringen av personvernkonsekvensvurderingen blir mer

omfattende, og fremstår mer byrdefull enn nødvendig. Vi ser at veiledningen på side 7 definerer både *behandling* og *behandlingsaktivitet* og at der fremkommer at behandlingsaktiviteter kan grupperes. Vi mener at dette kan tydeliggjøres ved gjennom at det også av fotnote 10 i malen kan fremkomme at ved en prosess som omfatter flere behandlingsaktiviteter med samme behandlingsgrunnlag, er det tilstrekkelig at prosessen beskrives en gang. Det bør med andre ord ikke være nødvendig å legge til en tabell per behandlingsaktivitet.

Når det gjelder beskrivelsen av behandlingsgrunnlag, tror vi det kan være fordelaktig at veilederen lister opp de ulike alternativene i personvernforordningens artikkel 6 sammen med noen eksempler som også inkluderer eksempler på supplerende rettsgrunnlag som kan være typisk for sektoren. At det av høringsutkastet vises til at flere virksomheter i helse- og omsorgssektoren synes det er vanskelig å finne behandlingsgrunnlag for å behandle personopplysninger, underbygger viktigheten av å ha god veiledning og utførlige eksempler på dette området.

Utdyp forhold som ikke fremgår tydelig av beskrivelsen av dataflyt, punkt 3.8
I punkt 3.7 skal dataflyten beskrives og i punkt 3.8 skal det utdypes forhold som ikke fremgår tydelig av dataflyten. For å gi ytterligere hjelp til personvernkonsekvensvurderingen, tenker vi at veilederen her kan beskrive at det her er et mål å få frem eventuelle forhold ved behandlingen som kan medføre at personvernrisikoen øker. Foreligger det for eksempel kompleks samhandling mellom mange aktører, stiller det økte krav til informasjonssikkerhet. Dersom behandlingen innebærer at det hentes inn informasjon/personopplysninger fra andre kilder, er det viktig at eventuell automatisert innhenting er satt opp slik at informasjon innhentes fra autorative kilder slik at datakvaliteten sikres. Utstrakt bruk av mellomlagring kan utfordre prinsippet om retten til å bli glemt, dette bør derfor også omtales slik at man kan ta det med i selve personvernkonsekvensvurderingen.

Beskriv bruk av leverandører (inkludert databehandlere) og relasjonen til disse, punkt 3.9
Ved bruk av databehandlere vil man i dag ofte møte problemstillinger knytter til overføring av tredjeland og Schrems II-dommen. Dette kan også være aktuelt for gjennomføring av helseforskningsprosjekter. Vi savner en omtale av regelverket i personvernforordningen kapittel V i veilederen.

Dersom behandlingen av personopplysninger gjelder et system/løsning, hvordan er personvern bygget inn, punkt 3.13
I punkt 3.11. og 3.12 skal man besvare hvordan henholdsvis personvernprinsippene og de registrertes rettigheter ivaretas, mens man i 3.13 skal beskrive hvordan personvern er bygget inn i løsningen. Beskrivelsene i disse tre punktene vil etter vår erfaring ofte gli over i hverandre, og det bør derfor åpnes opp for at disse kan besvares under ett. Vi synes som tidligere nevnt at det er veldig positivt at veilederen henviser til hvor leseren kan finne ytterligere veiledning. Når det gjelder punkt 3.13 kan det, etter vår mening være hensiktsmessig å henvise til Datatilsynets veiledning om innebygget personvern[1].

Det følger av personvernforordningen artikkel 32 at det skal gjennomføres en risikovurdering knyttet til personopplysningssikkerheten før oppstart av behandlingen. Der det allerede er gjort en risikovurdering knyttet til informasjonssikkerheten, bør dette henvises til i kapittel 3. Der en slik vurdering ikke er gjennomført, vil være hensiktsmessig å innta et punkt hvor tiltak for å sikre konfidensialitet, integritet og tilgjengelighet i behandlingen beskrives. Der det identifiseres behov for tiltak for å redusere risiko, må dette også beskrives.

Beskriv vurderingen av om behandlingen av personopplysningene er nødvendige for å ivareta formålet punkt 4.1
Beskriv vurderingen av om det er mulig å ivareta formålene på en mindre inngripende måte punkt 4.2
Det å vurdere behandlingens nødvendighet og proporsjonalitet er noe av det som erfaringsmessig oppleves som mest utfordrende i en DPIA. Det vil her være verdifullt for leseren å få noen flere knagger og eksempler beskrevet i veilederen som vil hjelpe dem i vurderingen av om det er et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordeler som oppnås med behandlingen. Er det sammenheng mellom formålet og de planlagte aktivitetene og står disse i forhold til formålet?

[1] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Beskriv hvilke risikoer for de registrerte for de registrertes rettigheter og friheter virksomheten har identifisert punkt 4.3 Beskriv/konkretiser hvilke risikomomenter som er vektlagt i vurderingen punkt 4.4.
Vår erfaring tilsier at det er hensiktsmessig at det beskrives hvilken risiko som vil ligge i behandlingen etter at tiltak er iverksatt. Dersom de ulike risiki videre plasseres i en matrise vil dette tydeliggjøre for både ledelsen og personvernombudet hvordan det totale risikobildet ser ut etter tiltak. En samlet oversikt over alle tiltak i en tabell sammen med tydelig ansvarlig og frist for gjennomføring kan videre gjøre oppfølgning enklere, spesielt dersom det er identifisert mange risiki.

Ettersom direktoratet ved malen ønsker å legge til rette for gjenbruk og deling, mener vi det vil være hensiktsmessig at veilederen inneholder en tabell som beskriver de ulike nivåene for sannsynlighet og konsekvens for å sikre at det etableres en felles forståelse av risikobegrepene og hva de ulike nivåene av sannsynlighet og konsekvens innebærer.

Er formatet på produktet hensiktsmessig?
Det er svært viktig at malen også finnes i word-format slik at den kan fylle ut direkte. Deloitte støtter derfor dette formatvalget. Som beskrevet over under punktene 4.3 og 4.4 mener vi det kan være hensiktsmessig å ha en matrise som viser det totale risikobildet etter tiltak samt en tabell som gir oversikt over planlagte tiltak, ansvarlige og frister.

Dersom det er ønskelig at vi utdyper våre tilbakemeldinger i et møte eller på annen måte, er det bare å ta kontakt.

Med vennlig hilsen
Deloitte Advokatfirma AS

Hanne Pernille Gulbrandsen (e.f)
Partner
hgulbrandsen@deloitte.no

Marianne Lie Howard (sign)
Senior Manager / Advokatfullmektig
marhoward@deloitte.no