Helse Sør-Øst RHF
Postboks 404
2303 Hamar

Telefon: 62 58 55 00
Telefaks: 62 58 55 01
postmottak@helse-sorost.no
Org.nr. 991 324 968

DIREKTORATET FOR E-HELSE
Postboks 221 Skøyen
0213 OSLO

Vår referanse:	Deres referanse:	Dato:
21/01474-2		30.11.2021
Saksbehandler:		

Høringssvar - mal for personvernkonsekvensvurdering (DPIA)

Helse Sør-Øst RHF viser til høringsbrevet med høringsfrist 30. november 2021.

Helse Sør-Øst RHF ser positivt på at det utarbeides veiledninger og malverk som er tilpasset sektoren, og at bruk er frivillig, slik at malene kan tilpasses lokale behov. I helseforetakene brukes blant annet egne maler for forskningsprosjekter og egne for ikt-utviklingsprosjekter.

Etter vårt syn er det viktig at metodeverket legger opp til, og veileder om, at omfanget på en personvernkonsekvensvurdering (heretter: pvk[1]) kan variere. Dette for å sikre en risikobasert tilnærming.[2] Størst innsats bør legges i vurdering av de antatt mest alvorlige forhold; dette vil typisk være de egenskaper ved behandlingen som tilsier at en pvk skal utføres.

Det er positivt at man legger opp til gjenbruk av eksisterende dokumentasjon, ikke minst protokollen. Helse Sør-Øst RHF er imidlertid usikre på om malen bør sikte på å også fungere som dokumentasjon av etterlevelse av forordningen utenom pvk-situasjoner (dvs. anbefaling om del A-C alltid fylles ut), men det gås ikke nærmere inn på her.

[1] DPIA brukes mye, men det er ønskelig med en norsk forkortelse. Nav og Skatteetaten synes bruke pvk. Språklig vil formodentlig også pkv og pvkv være relevante alternativer
[2] Artikkel 29-gruppen trekker frem både skalerbarheten og sammenhengen med art 24(1) i oppsummeringen av sin veiledning, se WP248rev1 s 19.

Konkrete tilbakemeldinger til malens ulike deler

Del B

I punkt 2.1 anbefaler Helse Sør-Øst RHF at man er tydeligere på skillet mellom krav og veiledning. Artikkel 29-gruppens *veileder* uttrykker ikke *krav*, men den er til hjelp i vurderingen av om det er høy risiko. I veiledningen om «høy risiko» er det ønskelig at det veiledes i å vurdere risikoen, *ut over* å telle antall treff mot kriteriene fra artikkel 29-gruppens veileder. Aktuelle hjelpespørsmål kan være: Hvordan antar man de registrerte vil oppleve behandlingen? Hvor god kvalitet har opplysningene, hensett til formålet med behandlingen? Hvordan vil feil ramme den registrerte? Det kan gjerne pekes på personvernprinsippene i artikkel 5.

Del C

Helse Sør-Øst RHF foreslår at note 9 justeres slik at det klargjøres at malen viser én av flere måter å oppfylle kravet i artikkel 35 nr 7 bokstav a.[3]

I virksomheter som har internkontroll iht. artikkel 24, bør beskrivelsen i 3.11 og 3.12 kunne innrettes på å primært beskrive de forhold som kan begrunne en høy risiko, dvs. at man fokuserer på utvalgte punkter i 3.11 og 3.12, som grunnlag for risikovurderingen i del D. Videre bør det pekes på muligheten for å henvise til behandlingsprotokoll som utfyllende beskrivelser av behandlingen.

Det er positivt at punkt 3.6 legger opp til at formål og behandlingsgrunnlag beskrives, jf. at dette er gode kriterier for å skille behandlingsaktiviteter fra hverandre. Når det gjelder rettslig grunnlag, vil antagelig små virksomheter finne disse vurderingene vanskelige, og vil ha behov for relevant veiledning.

I punkt 3.9 bør fokus være på databehandlere, og at man inkluderer underdatabehandlere og jurisdiksjonsutfordringer/ behandling utenfor EØS i punktet.

I tillegg til de oppførte punkter anbefales det at man setter av plass til noen friere refleksjoner om risikobildet, herunder om det er noen trusler (inkl. trusselaktører), sårbarheter eller mulige konsekvenser som fremstår som viktige å være oppmerksomme på i del D.[4]

Del D

I veiledningen foreslår Helse Sør-Øst RHF at man understreker at størst innsats bør rettes på å vurdere områder hvor man antar risikoen er høy.

Helse Sør-Øst RHF anbefaler også at man i veiledningen klargjør hvilke deler av kravene i artikkel 35 hvert punkt i malen er ment å dekke. Punkt 4.1, 4.3. og 4.4 synes ha klar

---

[3] Jf. f.eks. britisk veiledning og malverk (What is a DPIA? | ICO),.

[4] Viser her til Digdirs anbefaling for informasjonssikkerhetsvurderinger, jf. foranalyse trinn 2 og 3. De innledende vurderinger av behovet for en pvk vil også være relevante, jf. også momentene som pekes på i vurdering av personvernkonsekvenser (veileder til utredningsinstruksen, FAD 2005), s 11-12.

forankring i forordningen, jf. pvf. 35 nr 7 bokstaver b, c og d. Krav som ev. ikke er knyttet til artikkel 35 bør utgå eller flyttes til andre deler av malen.

Til punkt 4.4 anbefaler Helse Sør-Øst RHF at det utarbeides et forslag til konsekvens- og sannsynlighetsskala; det kan gjøre det enklere å gjenbruke vurderinger mellom virksomheter.

Del E
Punkt 5.1 bør kun omhandle de registrerte og deres representanter, jf. at det er disse som forordningen stiller krav om at involveres, dersom det er relevant, iht. artikkel 35 nr 9.

Ettersom formålet med en pvk er å vurdere risiko for de registrerte, kan det være hensiktsmessig at man både i omtale av del A og D peker på at involvering av de registrerte (typisk vha. deres representanter, f.eks. brukerutvalg) ofte både er hensiktsmessig og påkrevd iht. pvf.

Med vennlig hilsen
Helse Sør-Øst RHF

Øyvind Grinde

Øyvind Grinde
enhetsleder

Jon Berge Holden
spesialrådgiver informasjonssikkerhet