

DATATILSYNET
Postboks 458 Sentrum
0105 OSLO

Vår referanse:

11/01281-19

Saksbehandler:

Øyvind Grinde

Deres referanse:

23/01219-2

Dato:

16.05.2023

Redegjørelse for mulig omorganisering av personvernombudene ved helseforetakene i Helse Sør-Øst

Vi viser til Datatilsynets brev den 19. april 2023 med krav om redegjørelse for omorganisering av personvernombudene ved helseforetakene i Helse Sør-Øst RHF. Under følger tilbakemelding på deres spørsmål.

1. Beskrivelse av formålet med å samle personvernombudsordningen gjennom å utnevne et felles ombud i det regionale helseforetaket

Det gjøres mye godt personvernarbeid i Helse Sør-Øst, men for å harmonisere vurderinger og for å møte utviklingen innen teknologi, forskning og nye IKT-løsninger med en økende grad av regionale og nasjonale løsninger, er det nødvendig å styrke arbeidet med personvern ytterligere. I den forbindelse foreslås det en styrket internkontroll innen personvern og endret organisering av personvernombudene i Helse Sør-Øst.

Informasjonsbehandlingen i helseforetakene øker i kompleksitet, mengde og samhandling. Dette gir behov for å styrke personvernarbeidet, og som eksempler kan nevnes:

- Det er en generell trend med mer spesialisering i leverandørmarkedet, for eksempel innen IKT-tjenester, medisinsk-teknisk utstyr og behandlingshjelpemidler. Dette gir bedre og mer effektive produkter og tjenester, men det gir også lengre og mer komplekse verdikjeder. Det er mer krevende og omfattende å forstå og vurdere personvernet i slike verdikjeder. Skytjenester er eksempler på komplekse verdikjeder. Skytjenester tas i bruk i større og større grad i samfunnet rundt oss.

- I helsesektoren fører spesialisering til at behandling av pasienter i større grad involverer flere sykehus, private laboratorier, IKT-leverandører, nasjonale registre og så videre. Trygg og effektiv pasientbehandling fordrer at helseopplysninger deles mellom aktørene i ett og samme behandlingsforløp.
- Bruk av stordata og kunstig intelligens introduseres innen mange områder og vil kunne gi bedre pasientbehandling og mer effektiv ressursbruk. Forskning og pasientbehandling med bruk av stordata og kunstig intelligens har behov for tilgang til store mengder data (helseregistre).
- Sensorer som overvåker pasienter og persontilpasset medisin representerer en utvikling som vil gi nye utfordringer knyttet til vurderinger av personvernet, både innen forskning og pasientbehandling.

Det å kunne gi gode vurderinger innen personvernområdet krever forståelse innen mange ulike områder, som for eksempel kompetanse innen juss, teknologi og helse. Et personvernombud i det regionale helseforetaket vil ha egne ansatte under sin ledelse. Disse vil til sammen ha høy kompetanse gjennom tverrfaglig sammensetning. Personvernombudet og dets ansatte vil ikke ha andre oppgaver, og man unngår dermed eventuelle interessekonflikter.

Helse- og omsorgsdepartementet utarbeidet i 2019 et rundskriv for å avhjelpe utfordringer med ulike oppfatninger om hvordan reglene om taushetsplikt, personvern og informasjonssikkerhet skal forstås. Departementet pekte der på at ved juridisk tvil bør spørsmål løftes i linja, til regionalt helseforetak, eventuelt Helsedirektoratet eller Direktoratet for e-helse. I slike prosesser vil som regel også personvernombudet rådspørres. Samme type problemstillinger er tatt opp i strategi for persontilpasset medisin¹.

Ved å sentralisere personvernombudsfunksjonen legges det til rette for å etablere et fagmiljø som kan gå dypere inn i fagfeltet enn det hvert enkelt helseforetak kan gjøre. Det legges også til rette for likebehandling på tvers av helseforetakene, ved at ombudet vil gi samme rettslige vurdering av like rettslige spørsmål, på tvers av helseforetak. Videre vil ombudet forenkle dialogen med de registrerte, ved at de kan kontakte ett personvernombud for å ivareta sine personvernrettigheter også når det har vært pasientforløp som har krysset helseforetaksgrenser.

Internkontroll for personvernområdet, med blant annet utarbeidelse av styrende dokumenter, er en oppgave som bør være tydelig plassert i en ledelseslinje. Det er i dag svakheter i den overordnede tilnærmingen for å oppnå regional harmonisering av styrende dokumenter innen personvern. Ved å etablere ett personvernombud i Helse Sør-Øst legges det til rette for å kunne styrke ombudsfunksjonen og gi mer harmoniserte råd. I tillegg kan det forenkle arbeid med internkontroll for personvernområdet.

¹ [Strategi for persontilpasset medisin - regjeringen.no](https://www.regjeringen.no)

2. Beskrivelse av hvordan ordningen er tenkt organisert for de lokale helseforetakene og det regionale helseforetaket i fremtiden, inkludert beskrivelse av hvilke oppgaver som vil høre til de forskjellige enhetene

Helse Sør-Øst RHF har et overordnet ansvar for å styre og samordne virksomhetene i helseforetakene i regionen. I dette ligger også et ansvar for et godt og effektivt arbeid med personvern, og for å unngå ubegrunnede forskjeller i arbeidet med personvern i foretaksgruppen. Dette skal være en integrert del av et helhetlig styringssystem, for eksempel ved regionale føringer og styrende dokumenter.

Helse Sør-Øst RHF vurderer å etablere ett personvernombud for helseforetakene i foretaksgruppen. Helse Sør-Øst RHF vil sørge for at ombudet får tilgang til de ressurser som er nødvendig for å utføre oppgavene, inkludert ansatte som rapporterer til ombudet. Ombudet vil ivareta de oppgaver som hører til et personvernombud i henhold til personvernforordningen, jf. forordningens artikkel 39 om personvernombudets oppgaver:

- informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til forordningen, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger,
- kontrollere overholdelsen av forordningen, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdnings- skapende tiltak og opplæring av personellet som er involvert i behandlings- aktivitetene, og tilhørende revisjoner,
- på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35,
- samarbeide med tilsynsmyndigheten,
- fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.

Helseforetakene er, som dataansvarlige, ansvarlige for å etterleve personvernregel- verket, og de må selv ha tilstrekkelig kapasitet og kompetanse innen personvern. Ved utpeking av et konsernombud forutsettes det at helseforetakene beholder minst like god personvernkompetanse og -kapasitet som i dag.

Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene. Helseforetakene kan ikke bestemme hvordan ombudet skal prioritere henvendelsene fra helseforetaket. Helseforetakene skal opplyse ombudet om områder med høy risiko innen personvernområdet, og stille med tilstrekkelige ressurser til at ombudet kan få innsikt i lokale forhold og prioritere sine oppgaver deretter.

Utgangspunktet er at arbeidsoppgaver knyttet til personvern som kan utføres lokalt, forblir i helseforetakene. Kun oppgaver som hører til personvernombudet overføres til det regionale helseforetaket. Blant annet vil personvernrådgivning i forskning i all hovedsak videreføres lokalt i helseforetakene.

I norsk lovgivning er det innen forskning en særskilt rådføringsplikt med ombud *eller en annen* som oppfyller kvalifikasjons- og uavhengighetskravene som stilles til ombud, jf. personopplysningsloven §§ 9-10. Denne funksjonen foreslås videreført lokalt, i tråd med anbefaling fra de administrerende direktørene ved helseforetakene. Det betyr at helseforetakene må peke ut *en annen* (enn personvernombudet) som oppfyller kravene.

At personvernombudsfunksjonen sentraliseres innebærer altså ikke at behovet for personvernkompetanse lokalt forsvinner. Det vil være et betydelig behov for rådgivning og vurderinger lokalt. Typiske oppgaver, som enten kan utføres i eget helseforetak eller som tjenestekjøp fra Sykehuspartner HF, kan være:

- Føre protokoll over behandlingsaktiviteter, som blant annet må inneholde formålet med behandlingen og kategorier av personopplysninger
- Gjennomføre risikovurdering
- Utarbeide personvernkonsekvensvurderinger
- Utarbeidelse av databehandleravtaler, interne retningslinjer og prosedyrer
- Opplæring av ansatte
- Rådgivning til ledere og medarbeidere i konkrete saker, for eksempel i forskning eller ved etablering av nye systemer
- Oppfølging av avvik og håndtering av brudd på personopplysningssikkerheten, inkludert varsling til Datatilsynet

Det er derfor viktig at helseforetakene beholder god kompetanse og kapasitet til personvernarbeid. Om det utnevnes sentralt personvernombud, legges det til grunn at ansettelsesforholdene til dagens personvernombud videreføres i helseforetakene, men da i en endret rolle.

3. Status på arbeidet med omorganisering av personvernombudsordningen i HSØ

Det planlegges med å behandle sak om "styrking av arbeidet med personvern" i styremøte i Helse Sør-Øst RHF den 21. juni 2023.

4. Hvilke av alternativene i personvernforordningen artikkel 37 som hjemler muligheten for å utnevne ett felles personvernombud;

- a. Ved løsning hjemlet i artikkel 37, nr. 2 ber vi om deres begrunnelse for at HSØ regnes som et konsern i personvernforordningens forstand**

b. Ved løsning hjemlet i artikkel 37, nr. 3 ber vi om deres vurdering knyttet til kriteriene organisasjonsstruktur og størrelse

Den foreslåtte organiseringen av personvernombud er forankret i artikkel 37 nr 2.

Helse Sør-Øst RHF mener det er klart at foretaksgruppen er et konsern i henhold til personvernforordningens regler, og at det derved kan utpekes ett ombud for foretaksgruppen, jf. forordningens artikkel 37 nr. 2. Helse Sør-Øst RHF har opprettet helseforetakene og utøver eierstyring gjennom foretaksmøter, jf. helseforetaksloven §§ 9 og 16, jf. § 2. Dette er en ordning som tilfredsstiller forordningens krav til konsern, jf. forordningens artikkel 4 nr. 19.

Vi viser her til fortalens punkt 37:

«37. Et konsern bør omfatte et foretak som utøver kontroll, og dets kontrollerte foretak, der foretaket som utøver kontroll, bør være det foretak **som kan utøve en dominerende innflytelse på de andre foretakene, f.eks. i kraft av eiendomsrett, økonomisk deltaking eller reglene det er underlagt**, eller myndigheten til å få gjennomført regler om vern av personopplysninger. Et foretak som kontrollerer behandlingen av personopplysninger i tilknyttede foretak, bør sammen med disse foretak anses som et konsern.» (vår utheving)

Etter vår mening taler både helseforetaksloven § 2a («Regionale helseforetak skal planlegge, organisere, styre og samordne virksomhetene i helseforetakene som de eier») og § 9 (bestemmelser om stiftelse og eierskap) for at disse vilkår er oppfylt.

Videre er det i forarbeidene til helseforetaksloven Ot.prp. nr. 66 (2000-2001) i ulike sammenhenger lagt til grunn at det regionale helseforetaket med underliggende helseforetak vil regnes som konsern. Eksempelvis legges det på side 85 til grunn at foretaksgruppen må anses som «konsern» etter konkurranseloven. Videre legges det på side 137 til grunn at informasjonsflyten mellom regionalt helseforetak og helseforetak skal skje som i et konsernforhold og i merknadene til § 43 at henvisningen til regnskapsloven innebærer at foretakene må følge regnskapslovens bestemmelser for konsern og konsernregnskap slik at det må avlegges konsoliderte regnskap.

5. Beskrivelse av hvordan ordningen skal sikre personvernombudets frie og uavhengige stilling, jf. personvernforordningen artikkel 38

Personvernombudet vil rapportere direkte til høyeste ledelsesnivå hos hvert helseforetak det er personvernombud for, inkludert Helse Sør-Øst RHF. Ombudet skal ikke motta instruksjoner om utførelsen av sitt arbeid, og ombudet vil ikke bli tillagt andre oppgaver.

6. Beskrivelse av hvordan det skal legges til rette for at personvernombudet kan utføre oppgavene beskrevet i artikkel 39

Det legges til rette for at personvernombudet kan utføre sine oppgaver ved at ombudet har tilstrekkelig kapasitet og kompetanse.

Helseforetakene har plikt til å støtte personvernombudet i forbindelse med utførelsen av oppgavene omtalt i artikkel 39. Helse Sør-Øst RHF følger opp at helseforetakene har et systematisk personvernarbeid som etterlever kravet. I samråd med personvernombudet kan for eksempel personvernforumet videreutvikles.

Kontroll av overholdelse av personvernregelverket kan gjøres i samarbeid med konsernrevisjonen, i samarbeid med revisjonsmiljøene i de underliggende helseforetakene, og i personvernombudets egen regi.

Vi kan ikke se at det vil være noen hindre for et godt samarbeid med tilsynsmyndigheter. For like løsninger, herunder nasjonale og regionale løsninger, kan det være enklere for Datatilsynet å forholde seg til et sentralt personvernombud enn hvert ombud ved helseforetakene som benytter den aktuelle løsningen.

7. Beskrivelse av hvordan oppgaver knyttet til personvern vurderinger i forbindelse med kvalitetssikring og forskning skal organiseres etter den nye modellen for personvernombud, herunder;

a. Vurdering av hvordan kravene i personopplysningsloven § 9, jf. artikkel 37 nr. 5 og 6 og artikkel 38 nr. 3 oppfylles gjennom organiseringen og oppgaveløsningen

Hvert enkelt helseforetak vil være ansvarlig for å sikre etterlevelse av krav til personvern vurderinger i forbindelse med kvalitetssikring og forskning, herunder etterlevelse av personopplysningsloven § 9. Det sentrale personvernombudet vil utføre oppgavene som er tillagt ombudsrollen i forordningen, og det vil selv prioritere oppgavene i henhold til artikkel 39 nr 2. Helseforetakene kan altså ikke basere seg på at det sentrale ombudet vil utføre oppgaver som etter gjeldende regelverk og føringer kan utføres av andre. I dette ligger at helseforetakene må sørge for å beholde kapasitet til selv å utføre personvern vurderinger knyttet til kvalitetssikring og forskning. For personopplysningsloven § 9 innebærer dette også at helseforetakene må etterleve bestemmelsens krav til uavhengighet (m.v.) for personell som skal gi råd i henhold til bestemmelsen, dvs. alternativet «en annen».

Vi håper redegjørelsen dekker tilsynets behov. Ta gjerne kontakt om noe skulle være uklart, om dere ønsker et møte eller om dere har innspill til det videre arbeidet.

Med vennlig hilsen
Helse Sør-Øst RHF

A handwritten signature in blue ink that reads "Terje Rootwelt". The signature is written in a cursive style with a horizontal line above the first name.

Terje Rootwelt
administrerende direktør

Mona Stensby
konserndirektør