



**DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT**

Statsråden

Kontroll- og konstitusjonskomiteén
Stortinget
0026 OSLO

Deres ref

Vår ref

Dato

vk/17/2133

13. juni 2017

**Forespørsel fra kontroll- og konstitusjonskomiteen om sak om IKT-
infrastruktur i Helse Sør-Øst**

Jeg viser til brev av 9. mai og 6. juni i år fra Stortingets kontroll- og konstitusjonskomité om ovennevnte, og til mine svar sendt henholdsvis 15. mai og 1. juni i år.

Den foreløpige redegjørelsen fra PwC viser at det har vært en svikt i Sykehuspartner HF's gjennomføring knyttet til planlegging og forberedelse for overføring av drift og modernisering av IKT-infrastruktur til ekstern leverandør. De problemstillingene som reises av kontroll- og konstitusjonskomiteen i brev av 6. juni i år oppfatter jeg at retter seg mot fremtidig bruk av ekstern leverandør for modernisering og drift. Del 2 av redegjørelsen fra PwC vil i større grad fokusere på nettopp de vurderinger og beslutninger som er gjort om fremtidig organisering med bruk av en ekstern leverandør.

**Hvorvidt departementet har gjort uavhengige vurderinger av informasjonssikkerheten
i Helse Sør-Østs fremtidige organisering av modernisering og drift av IKT-infrastruktur**

Kontroll- og konstitusjonskomiteen viser i sitt brev av 6. juni til at det har kommet faglige innsigelser, både fra fagforeningene og fra navngitte fagpersoner. Kontroll- og konstitusjonskomiteen spør på bakgrunn av dette om hva statsråden har gjort for at Helse- og omsorgsdepartementet skulle vurdere sikkerheten i en så viktig sak, uavhengig av de vurderingene som er gjort i Helse Sør-Øst.

De uttalelsene som har kommet har i stor grad vært knyttet til tjenesteutsetting generelt, og en bekymring for om denne konkrete tjenesteutsettingen ville kunne medføre tap av norske arbeidsplasser og nasjonal IKT-kompetanse.

Ett av flere momenter som har vært trukket frem er uro knyttet til fremtidig tilgang til personsensitive opplysninger. Disse momentene har vært av generell karakter, og det har derfor vært naturlig å peke på Helse Sør-Øst RHF i denne sammenheng. De samme forholdene har også vært tema i de spørsmål jeg har mottatt fra Stortinget og i interpellasjonsdebatten 10. november 2016. Mine svar i saken har bygd på den informasjonen jeg har fått fra Helse Sør-Øst RHF.

Det fremgår av mitt brev til kontroll- og konstitusjonskomiteen av 1. juni i år, at det først i møtet med Helse Sør-Øst RHF den 26. april i år ble klargjort for meg at de begrensninger som ligger i at ekstern leverandør "ikke skal ha tilgang til helseopplysninger" ikke innebærer en absolutt sperre. Begrensningen ligger i en kombinasjon av teknologiske, avtalemessige og juridiske sikkerhetsmekanismer som skulle hindre og eventuelt avdekke ureglementær tilgang. Jeg la i dette møtet vekt på at ledelsen måtte sikre seg at styret i Helse Sør-Øst RHF hadde tilsvarende informasjon. Bakgrunnen for møtet 26. april i år var at jeg ønsket å få klarhet i forhold som ble tatt opp i spørsmålet fra stortingsrepresentant Sverre Myrli (spørsmål nr 969 til skriftlig besvarelse). Gjennom arbeidet med dette spørsmålet ble jeg gjort oppmerksom på protokolltilførselen i styremøtet i Sykehuspartner HF den 5. april i år. I protokolltilførselen var det en konkret påpekning av at tilganger kunne benyttes til å hente ut personsensitive opplysninger. Det ble videre satt spørsmålstegn ved om styret i Helse Sør-Øst RHF var innforstått med denne muligheten.

I mitt brev til kontroll- og konstitusjonskomiteen 1. juni i år redegjorde jeg kort for ansvarsforholdene i spesialisthelsetjenesten. Det følger av spesialisthelsetjenesteloven § 2-1 at staten har det overordnede ansvaret for at befolkningen gis nødvendig spesialisthelsetjeneste. Denne plikten oppfylles blant annet ved at staten ved departementet er eier av de regionale helseforetakene. De regionale helseforetakene har etter spesialisthelsetjenesteloven § 2-1 a ansvaret for å sørge for at personer med fast bopel eller oppholdssted innen helseregionen tilbys spesialisthelsetjeneste i og utenfor institusjon.

I Ot. prp. nr. 66 (2000-2001) s. 136 uttales det følgende om rollefordelingen mellom eier og foretak:

"Eierens rolle er å etablere foretaket, tilføre foretaket forsvarlig kapitalgrunnlag, fastsette vedtekter, andre rammer og mål for virksomheten og velge et styre som på vegne av eier skal forvalte foretaket. I tillegg ligger det i eierrollen å følge opp foretakenes drift og resultater i forhold til fastsatte krav og i nødvendig utstrekning iverksette korrektive tiltak. Det er foretaksledelsens ansvar å sørge for at de mål eier setter for virksomheten realiseres best mulig med grunnlag i de ressurser som er stilt til rådighet for foretaket." (Min understrekning)

Og på s. 72:

"Eieren har altså ikke noen direkte kompetanse eller ansvar knyttet til den løpende driften. Det ligger likevel i foretaksmøtets overordnede karakter at det kan gi instruksjer og omgjøre styrets vedtak i alle saker. I tråd med Bedriftsøkonomisk Institutt sin uttalelse, mener departementet at dette bør

være rettigheter av latent karakter. Eiers adgang til å styre i foretaksmøter bør bare brukes i tilfeller hvor det er nødvendig for å ivareta eiers overordnede ansvar og interesser. Dette gjelder både departementets og de regionale helseforetakenes eierstyring. Hvor det ikke er et tillitsforhold mellom eier og ledelsen i foretaket, bør det normale være at eier bytter ut styret, se § 25. Selv om departementet mener at eier skal være varsom med å gå inn i den løpende driften, kan det ikke tilrås at foretaksmøtets kompetanse reduseres. Dette ville bryte med det sentrale utgangspunkt at eier fatter beslutningene i foretakets øverste organ."(Min understrekning)

Uttalelsene viser at den løpende driften ligger til helseforetakene å forvalte. Eier skal tilrettelegge for at foretakene kan oppfylle sitt sørge-for-ansvar, og kan gi overordnende føringer på hvordan driften skal gjennomføres. Det betyr imidlertid ikke at ikke eier kan gripe inn og fatte vedtak i foretaksmøte om enkeltsaker. I noen tilfeller er det krav til at beslutningene løftes til eier i foretaksmøte, jf. helseforetaksloven § 30 om saker av vesentlig betydning. I tilfeller hvor dette gjøres vil beslutningsgrunnlaget normalt være basert på det kunnskapsgrunnlaget som det underliggende helseforetak har utarbeidet. Det kan i den forbindelse vises til følgende uttalelse i Ot. prp. nr. 66 (2000-2001) s. 144 som gjelder helseforetaksloven § 30 og saker av vesentlig betydning:

"Etter bestemmelsens annet ledd er ansvaret for å forelegge saker som angår helseforetak, lagt på det regionale helseforetaket som er eier av helseforetaket. Saken vil dermed bli behandlet i styret i regionalt helseforetak før saken kommer til foretaksmøtet." (Min understrekning)

Uttalelsen viser at det normale er at sakene utredes av underliggende helseforetak, og som dermed har ansvaret for å sikre et forsvarlig beslutningsgrunnlag.

Komiteen ber om en redegjørelse for hva jeg har gjort for at departementet skulle vurdere sikkerheten i en så viktig sak uavhengig av vurderingene i Helse Sør-Øst. Redegjørelsen ovenfor viser at eier ikke foretar vurderinger *uavhengig* av underliggende foretak. Det er foretaket som er ansvarlig for den løpende driften og beslutninger knyttet til denne. Foretakene har dermed også ansvaret for å sikre seg et forsvarlig beslutningsgrunnlag. Som nevnt vil departementet følge med på om den løpende driften av foretaket på et overordnet nivå er forsvarlig.

Det at beslutningsgrunnlaget er utarbeidet av foretaket, betyr ikke at det ikke foretas *selvstendige* vurderinger i departementet. Dersom departementet er av den oppfatning at informasjonen og kunnskapsgrunnlaget er mangelfullt, misvisende eller er utilstrekkelig for å fatte en forsvarlig beslutning eller påse at foretaket driftes forsvarlig, vil departementet be om ytterligere opplysninger eller utredninger fra foretaket.

Med utgangspunkt i de lovregulerte ansvarsforholdene og styringssystem er det ikke naturlig at Helse- og omsorgsdepartementet på eget grunnlag skulle gå inn og utarbeide eget beslutningsgrunnlag, og på det grunnlaget eventuelt overprøve de vurderinger av IKT-sikkerhet som Helse Sør-Øst RHF og helseforetakene har gjort.

I denne konkrete saken har departementet som tidligere informert kun fattet beslutning i foretaksmøte om adgangen til å benytte finansiell leasing for deler av tjenesteavtalen (foretaksmøte 15. september 2016, sak 3). Foretaksmøtet tok ikke stilling til verken bruk av eksterne leverandører eller organiseringen av det videre arbeidet.

Ifølge Helse Sør-Øst RHF skulle det ikke være tilgang til helseopplysninger for eksterne leverandører. Som det fremgår av mitt brev av 1. juni i år så var det først i møtet med Helse Sør-Øst RHF 26. april i år at det ble klargjort for meg at de begrensninger som ligger i at eksterne leverandører "ikke skal ha tilgang til helseopplysninger" ikke innebærer en absolutt sperre, jf omtalen ovenfor. Da dette ble klart for meg la jeg vekt på at styret i Helse Sør-Øst RHF måtte få samme informasjon som meg. Dette fordi jeg ble bekymret for at styret kunne ha oppfattet dette på samme måte som meg under sin tidligere behandling av saken. Med dette tiltaket sikret jeg at styret i Helse Sør-Øst RHF hadde samme informasjon som meg knyttet til det fremtidige regimet for tilgangsstyring, og samtidig forholdt jeg meg til det ansvaret som tilligger styret i denne saken.

Den 2. mai ble jeg klar over at det i planleggingen av overføringen av drift av IKT-infrastrukturen til eksterne leverandører, allerede var gitt tilganger som kunne medføre tilgang til personsensitive opplysninger. Jeg ba derfor om å få en redegjørelse fra Helse Sør-Øst RHF og informerte Stortinget i spontanspørretimen den 3. mai i år.

Helse Sør-Øst RHF har gjennomført flere tiltak i sakens anledning. Den planlagte virksomhetsoverføringen av modernisering og drift av IKT-infrastruktur i regionen er nå stilt i bero. Det har skjedd endringer både i ledelsen i Helse Sør-Øst RHF, i Sykehuspartner HF, og styret i Sykehuspartner HF har blitt skiftet ut. Jeg vil igjen understreke at jeg ser alvorlig på saken, og avventer den videre håndteringen av saken fra Helse Sør-Øst RHF's side.

Hvorvidt departementet har skaffet seg kunnskap om konsekvenser av tjenesteutsetting til utenlandsk leverandør

Innledningsvis vil jeg vise til mitt svar ovenfor om hvorvidt departementet utarbeider selvstendige beslutningsgrunnlag.

Pasientjournalloven gjelder for databehandlingsansvarlige som er etablert i Norge, jf. § 4. Personopplysningsloven gjennomfører EUs personverndirektiv (95/46/EF) i norsk rett og regulerer tilgang til opplysninger fra utlandet. Det er et grunnleggende vilkår at personopplysninger bare kan overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført personverndirektivet oppfyller kravet til forsvarlig behandling. Personopplysninger kan også overføres til andre stater dersom nærmere

bestemte vilkår er oppfylt. Regelverket oppstiller på denne måten et tydelig skille mellom stater i EU/EØS og statene utenfor. Tilgang og annen håndtering av helseopplysninger i styringssystemene reguleres uansett av norsk lov, herunder taushetsplikt, logging og kontroll av logger.

Bruk av eksterne underleverandører (databehandlere), enten disse holder til i Norge eller andre land skal reguleres i avtale. En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt. I pasientjournalloven § 22 er det presisert at en databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene for informasjonssikkerhet.

Departementet fikk ikke indikasjoner som skulle tilsi at Helse Sør-Øst RHF ikke hadde tilstrekkelig kunnskap om eller ikke hadde vurdert konsekvensene av å inngå kontrakt om tjenesteutsetting. På generelt grunnlag er det ikke rettslige hindre for tjenesteutsetting. Dette gjøres i betydelig grad i spesialisthelsetjenesten i dag. Det faktum at Helse Sør-Øst RHF ønsket å benytte en ekstern leverandør for å modernisere og drifte IKT-infrastruktur og premisset for dette ga i seg selv ikke grunnlag for å be om ytterligere informasjon.

Den foreløpige redegjørelsen fra PwC mottatt 24. mai i år har pekt på mulig svikt knyttet til nettopp databehandleravtale med underleverandører. Dette er forhold som Helse Sør-Øst RHF, Sykehuspartner HF og eventuell fremtidig ekstern leverandør må ha orden på dersom det blir iverksatt en virksomhetsoverføring.

Som jeg informerte om i brev av 1. juni i år så vil jeg gi et oppdrag til Direktoratet for e-helse. Det er viktig å sikre at vi har en god og felles forståelse av hva som skal til for en trygg og riktig bruk av både nasjonale og internasjonale leverandører, enten det er bruk av ulike teknologi eller leveranse av drift av IKT-løsninger. Det er viktig å få noen felles avklaringer av de forholdene som kontroll- og konstitusjonskomiteen peker på i sitt brev av 6. juni i år. Oppdraget til Direktoratet for e-helse vil være å se på håndtering av informasjonssikkerhet nettopp ved bruk av private leverandører i helse- og omsorgssektoren. Et element i dette er de utfordringer som knytter seg til bruk av internasjonale leverandører. Arbeidet skal ledes av Direktoratet for e-helse. De må sikre at de sentrale kompetansemiljøene blir trukket inn i arbeidet, og at fagorganisasjoner, tillitsvalgte og brukerorganisasjoner blir invitert til å komme med sine innspill. Forholdet mellom helsetjenesten og sikkerhetsloven må også vurderes. Det er viktig at vi gjennom dette arbeidet settes bedre i stand til å håndtere de utfordringene vi er kjent med, og jeg ønsker derfor at det foreligger et resultat allerede 1. november inneværende år.

Jeg vil avslutningsvis gjøre oppmerksom på at del 2 av redegjørelsen fra PwC vil bli behandlet av styret i Helse Sør-Øst RHF den 28. juni i år. PwC vil blant annet vurdere styringsmodell, fullmakter, ansvar og roller som er etablert i Sykehuspartner HF's prosjekt om fremtidig modernisering og drift av IKT-infrastruktur i Helse Sør-Øst. Videre vil avtalen med HPE vurderes med hensyn på ivaretagelse av informasjonssikkerhet og sikring av personsensitiv informasjon på en forsvarlig måte. Jeg vil avvente styret i Helse Sør-Øst

RHF's videre håndtering av denne redegjørelsen. Dersom det kommer frem informasjon i PwCs redegjørelse som berører de spørsmål som komiteen har vært opptatt av, så vil jeg komme tilbake med en ny orientering.

Med hilsen



Bent Høie

Kopi

Stortingets helse- og omsorgskomiteé