Datatilsynet

Sykehuset i Østfold HF
Postboks 300
1714 GRÅLUM

Deres refranse	Vår referanse	Dato
17/02156	16/01531-47/GRA	24.10.2017

Varsel om vedtak – overtredelsesgebyr - Sykehuset Østfold HF

Innhold

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

1 Innledning

Datatilsynet sendte den 26. mai 2017 brev til alle helseforetakene i Helse Sør-Øst RHF. I brevet ba vi om en redegjørelse blant annet for hvilke risikovurderinger og aksept av restrisiko som lå til grunn for beslutningen om å tjenesteutsette ansvaret for IKT-drift i regionen. Vi viser til likelydende brev fra alle helseforetakene datert 14. juni 2017 der det er gjort rede for hvilke vurderinger som er gjort i forbindelse med at det er inngått avtale med ekstern leverandør om strategisk samarbeid og IKT-drift.

I det følgende vil vi vurdere saken og besvare redegjørelsene samlet.

Innledningsvis ønsker vi å understreke at Datatilsynet er positiv til at det gjøres tiltak for å etablere en robust og sikker IKT-infrastruktur og drift av denne. Modernisering av de

eksisterende løsningene kan gi økt robusthet, bedre funksjonalitet, økt pasientsikkerhet og informasjonssikkerhet.

Det er grunn til å understreke at saken er spesiell fordi det er første gang norske helseforetak har besluttet å legge drift av hele helseregionens IKT-infrastruktur til ekstern leverandør i utlandet. Driften omfatter behandling av helseopplysninger om mer enn halve Norges befolkning og saken er av den grunn også prinsipiell med tanke på liknende prosjekter som er under planlegging i helsesektoren.

2 Datatilsynets vurdering –oppsummert

Vi har gjennomgått svarene fra helseforetakene. Svarene som er gitt i redegjørelsen samt informasjon vi har mottatt i forbindelse med våre undersøkelser ligger til grunn for følgende hovedkonklusjoner:

- De behandlingsansvarlige helseforetakene ikke har hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet.
- Helseforetakene har overlatt ansvaret for beslutninger som har betydning for pasientenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandleren og til ansatte lenger ned i organisasjonen.
- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsvurderinger før det ble besluttet å konkurranseutsette avtale om strategisk partnerskap, herunder drift og vedlikehold av IKT-infrastruktur.
- Det ble heller ikke gjennomført nødvendige risiko og sårbarhetsanalyser i forkant av at det ble besluttet å velge underleverandør i Bulgaria.
- Valgt underleverandør har i et begrenset tidsrom hatt tilgang til pasientopplysninger i strid med ledelsens forutsetning om tilgangskontroll.

Manglende sikkerhetsledelse og manglende rutiner for å sikre kontroll anses å være i strid med kravene i pasientjournalloven § 22 jf. § 5, personopplysningsloven §§ 13- 15 og personopplysningsforskriften §§ 2-3, 2-7 og 2-15.

Manglende etterlevelse av plikten til å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten er i strid med kravet i personopplysningsforskriften §§ 2-4 jf. 2-1 og pasientjournalloven § 22.

Tilgang til pasientopplysninger er gitt i strid med ledelsens forutsetninger og dermed uten forankring i ledelsen. Dette innebærer overtredelse av personopplysningsforskriften §§ 2-11 og 2-13 til 2-15. Tilgang gitt i strid med ledelsens beslutning viser også manglende ledelsesforankring som omtalt i forrige punkt.

Datatilsynet mener det er svært alvorlig at denne avtalen ble inngått uten at det forelå tilstrekkelige risikovurderinger og uten at restrisiko ble vurdert og akseptert av de behandlingsansvarlige i forkant av avtaleinngåelsen.

Alle tiltak som er satt i verk i etterkant av avtaleinngåelsen, og som følge av at saken har vært løftet i media vurderes som nødvendige for å avhjelpe situasjonen som har oppstått. Datatilsynet er tilfreds med at det tas ansvar for å rette opp de feilene som er avdekket og at Helse Sør-Øst har stanset prosjektet inntil videre.

På grunnlag av disse konklusjonene varsler vi følgende pålegg:

3 Varsel om pålegg -Vedtak om overtredelsesgebyr

Dette er et varsel om at Datatilsynet, i medhold av pasientjournalloven §§ 29 jf. 22 og 5 vil fatte følgende vedtak:

Sykehuset Østfold HF pålegges å betale et overtredelsesgebyr til statskassen, pålydende Kr. 800 000,- -kroner åttehundretusen- , for

1. *overtredelse av bestemmelsene i personopplysningsforskriften om sikkerhetsledelse og organisering av sikkerhetsarbeidet i virksomheten jf. §§ 2-3, 2-7 og 2-15,*
2. *brudd på krav om å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten i samsvar med kravene i § 2-4 jf.2-1 pasientjournalloven § 22 samt*
3. *overtredelse av bestemmelsene om tilgangskontroll i personopplysningsforskriften §§ 2-11 og 2-13 til 2-15.*

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

4 Generelt om bruk av databehandlere i helsesektoren

Lovpålagte krav om klare ansvarslinjer, sikkerhetsledelse, ledelsesforankring og kontroll er nødvendige for å sikre at den behandlingsansvarlige behandler personopplysninger i samsvar med prinsippet om ansvarlighet. Ansvarlighetsprinsippet er grunnleggende i personvernretten, på lik linje med prinsippene om bl.a. rettferdig og gjennomsiktig behandling av personopplysninger og prinsippet om forholdsmessighet.

Helseforetakenes handlingsrom når det gjelder tjenesteutsetting og bruk av databehandlere i utlandet er ikke særregulert, og følger derfor av de alminnelige bestemmelsene i personopplysningsloven jf. pasientjournalloven § 5 og personopplysningsloven § 15. Dette betyr at helseopplysninger kan overføres til en databehandler og behandles av denne på den måten som er skriftlig avtalt med den databehandlingsansvarlige. Skriftlig avtale er også et krav dersom opplysningene skal overføres til noen andre (en tredjepart) for lagring eller bearbeidelse. Dette betyr at det må foreligge skriftlig avtale mellom den databehandlingsansvarlige og databehandleren dersom databehandleren ønsker å benytte underleverandører for deler av virksomheten.

Dersom en databehandler befinner seg i utlandet kommer også bestemmelsene i personopplysningsloven § 29 og 30 til anvendelse. Lovens utgangspunkt er at overføring av opplysninger til utlandet er forbudt, med mindre staten sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført EUs personverndirektiv om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller i prinsippet kravet til forsvarlig behandling.

Regelverket åpner derfor for bruk av databehandlere i helsesektoren forutsatt at den behandlingsansvarlige forsikrer seg om at lovens øvrige krav er oppfylt. Dette gjelder uavhengig av om formålet er å tjenesteutsette lagring, infrastruktur, applikasjon, drift eller administrasjon av hele eller deler av virksomheten.

Overføring av personopplysninger til en ekstern leverandør eller databehandler, er bare tillatt dersom leverandøren tilfredsstiller kravene i personopplysningsforskriftens kapittel 2 jf. § 2-15. Formålet med bestemmelsene i kapittel 2 er å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene, i den grad det er nødvendig for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet. Det følger av § 2-1 siste ledd at informasjonssikkerhetstiltak som treffes i medhold av forskriften skal stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd.

Tiltakene som treffes skal være planlagte og systematiske. Dette følger av pasientjournalloven § 22 og forskriften § 2-1. Ansvaret for at kravene i forskriften er oppfylt er plassert hos den som har det daglige ansvaret for virksomheten.

Den behandlingsansvarlige skal etablere klare ansvars og myndighetsforhold overfor eksterne leverandører og beskrive disse i en egen avtale. Den databehandlingsansvarlige plikter også å ha kunnskap om sikkerhetsstrategien hos leverandøren og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet. Den behandlingsansvarlige er derfor pålagt å gjennomføre jevnlige revisjoner med databehandler jf. § 2-5.

Dersom databehandleren vurderer å gjøre endringer som har betydning for informasjonssikkerheten i sitt informasjonssystem, ut over det som er avtalt med den behandlingsansvarlige, er det følgelig også et krav etter § 2-7, jf. § §§ 2-4 og 2-15 jf. personopplysningsloven § 15, at slike endringer krever autorisasjon fra den behandlingsansvarliges daglige leder.

Plikten til å gjennomføre risikovurdering er regulert i forskriften § 2-4. Formålet med en slik vurdering er å skaffe slik oversikt over og informasjon om hvilke konsekvenser endringen kan få som er nødvendig for å sette den behandlingsansvarlige i stand til å ta riktige beslutninger. Når virksomheten vurderer å gjøre endringer som kan påvirke de kriteriene virksomheten har satt for akseptabel risiko, må ledelsen ta stilling til spørsmålet før de beslutter at endringen er gjennomførbar. Dersom tjenesteutsetting påvirker den behandlingsansvarliges plikt til å sikre etterlevelse av krav om konfidensialitet, må det vurderes om dette kan avhjelpes, eller om risikoen blir så stor at den ikke kan anses forenelig med kriteriene for akseptabel risiko. Ledelsen kan ikke beslutte tjenesteutsetting dersom den hindrer virksomheten å etterleve

lovpålagte krav, eller dersom den får konsekvenser for de registrerte som er i strid med deres rettigheter etter regelverket.

5 Sakens bakgrunn

Datatilsynet mottok høsten 2016 flere henvendelser fra ansatte i Helse Sør-Øst konsernet og pasienter som var bekymret fordi de mente de vedtatte planene om tjenesteutsetting ville få konsekvenser for personvern og informasjonssikkerhet i helseforetakene. Vi henvendte oss til Helse Sør-Øst RHF for å undersøke saken nærmere. I etterkant av første møte høsten 2016 har vi vært i dialog med Helse Sør-Øst RHF og Sykehuspartner. Innledningsvis var ikke helseforetakene representert i den dialogen som fant sted mellom Datatilsynet og Helse Sør-Øst. Derfor henvendte vi oss direkte til foretakene når vi ba om redegjørelse for saken.

5.1 Om foretaksmodellen

Helse Sør-Øst RHF og Sykehuspartner har frontet denne saken gjennom å svare for beslutninger og valg som er tatt. Helse Sør-Øst RHF er et regionalt helseforetak. Regionale helseforetaks ansvar og oppgaver er regulert i helseforetaksloven §§ 2 og 2a. Regionalt helseforetak er virksomhet som eies av staten alene og som er opprettet i medhold av lovens § 8.

Regionale helseforetak skal legge til rette for spesialisthelsetjenester, forskning, undervisning og andre tjenester som står i naturlig sammenheng med dette eller er pålagt i lov. De regionale helseforetakene skal ha et overordnet ansvar for å iverksette den nasjonale helsepolitikken i helseregionen. Regionale helseforetak skal planlegge, organisere, styre og samordne virksomheten i helseforetakene som de eier. I forbindelse med langsiktig planlegging skal regionale helseforetak vurdere om deler av tjenestene skal ytes gjennom inngåelse av avtale med private eller offentlige virksomheter som de ikke eier selv.

Helseforetak er virksomheter som eies av ett eller flere regionale helseforetak eller helseforetak og som er opprettet i medhold av helseforetaksloven § 9. Helseforetak yter spesialisthelsetjenester, forskning og undervisning, samt andre tjenester som står i naturlig sammenheng, eller som er pålagt i lov eller avtalt med den kommunale helse- og omsorgstjenesten.

Det er presisert i helseforetaksloven § 6 at helseforetakene selv har rettigheter og plikter, er part i avtaler med private og offentlige myndigheter og har partsstilling overfor domstoler og andre myndigheter. Det er videre presisert at det er foretakets eier som hefter ubegrenset for foretakets forpliktelser. Når flere foretak eier virksomhet sammen, blir samtlige eiere ansvarlige for virksomhetens forpliktelser.

Virksomhetens eier er staten ved Helse- og omsorgsdepartementet i regionale helseforetak, og staten ved regionale helseforetak i helseforetak.

Helseforetaksloven inneholder ingen bestemmelser som sier noe særskilt om roller og ansvar etter personopplysningsloven. Generelt er det slik at plikten til å etterleve bestemmelsene i

personopplysningsloven og pasientjournalloven påhviler den virksomheten som er behandlingsansvarlig, dette samsvarer med helseforetaksloven § 6.

I § 2a heter det at det regionale helseforetaket skal vurdere om deler av tjenesten skal ytes gjennom avtale med eksterne virksomheter. Dette er særlig relevant ved vurdering av om private helsetjenester skal benyttes for å supplere helsetilbudet, men ordlyden kan også tilsi at RHFet skal vurdere om IKT-tjenester skal ytes gjennom avtale. I dette ligger at Helse Sør-Øst kan gi føringer dersom de vurderer det slik at IKT-tjenester skal tjenesteutsettes.

Helseforetakene har i midlertid selv ansvaret for å sikre at slike føringer ikke går på bekostning av de pliktene de har etter det regelverket som gjelder for helsetjenesten, herunder personopplysningsloven og pasientjournalloven.

Helse Sør-Øst RHF har organisert arbeidet med å utkontraktere IKT-drift som et prosjekt som er ledet av Sykehuspartner. Sykehuspartner ble etablert som et helseforetak 1. januar 2015 og er etter dette et selvstendig rettssubjekt med eget organisasjonsnummer. Sykehuspartner er databehandler for alle helseforetakene i helseregionen, men er også ansvarlig for konsernovergripende IT-anskaffelser. I møte med Datatilsynet er det presisert at det er Sykehuspartner som er eier av avtalen med ekstern leverandør.

Vi har derfor lagt til grunn at helseforetakene ved administrerende direktør er databehandlingsansvarlig for personopplysninger helseforetaket behandler som en nødvendig del av det å yte, administrere og kvalitetssikre helsehjelp. Vi har også lagt til grunn at det regional helseforetaket kun har et «sørge for»-ansvar når det gjelder pasientbehandling og dermed ikke er behandlingsansvarlig for pasientopplysninger.

5.2 Nærmere om avtalen som er inngått med ekstern leverandør

I kunngjøringsteksten i Doffin er Helse Sør-Øst RHF oppgitt som oppdragsgiver for avtale om strategisk partnerskap innenfor IT-infrastruktur tjenester. Følgende er oppgitt i kunngjøringen: *« Helse Sør-Øst søker en strategisk partner som kan utvikle og endre IT-infrastruktur i tjenestene for å realisere prosjektet «Digital fornying», og drifte /forvalte infrastrukturen i fremtiden. Med utvikle menes å utvikle nye tjenester for å muliggjøre «Digital fornying». Med endre menes: standardisere, konsolidere og modernisere dagens infrastrukturlandskap. Med drifte/forvalte menes å besørge tjenesten som en «managed service», inkludert livssyklus støtte og kontinuerlig fornyelse, og koordinering av relevante integrasjonsaktiviteter.»*

Avtalens verdi er oppgitt å være 6,9 mrd. NOK over en periode på 7 år, med mulighet for 3 års forlengelse. Anskaffelsesprosedyren som er benyttet er konkurransepreget dialog. Avtalen er signert 15. september 2016. Konkurransen ble kunngjort 20. oktober 2014.

5.3 Datatilsynets saksbehandling

Datatilsynet etterspurte allerede i første møte med Helse Sør-Øst i oktober 2016 risikovurdering og personvernkonsekvensvurdering som lå til grunn for avtalen om tjenesteutsetting av IKT-drift.

I dette møtet ba vi om et nytt møte slik at disse vurderingene kunne fremlegges for Datatilsynet. I tilsynets innkalling til neste møte ba vi helt konkret om «at dere spesifikt går igjennom vurdering av personvernkonsekvenser for outsourcing av Helse Sør-Østs infrastruktur, som vi legger til grunn at de databehandlingsansvarlige har gjennomført før avtalen ble inngått. Som diskutert i forrige møte ønsker vi også å høre hvordan dere arbeider for å etablere tiltak for å hindre informasjons-/dataflyt ut av deres kontrollsfære. Videre etterspurte vi hvordan Helse Sør-Øst hadde vurdert behovet for forhåndsdrøftelser med Datatilsynet, jf. den nye forordningen som trer i kraft mai 2018.

Det ble ikke gjennomført nytt møte med Helse Sør-Øst før 4. april 2017. Datatilsynet mottok ingen av de etterspurte vurderingene i mellomtiden og møtet ble utsatt gjentatte ganger. I dette møtet ble det vist til at landvurdering for Bulgaria nylig var utført, og at man ønsket et nytt møte med tilsynet for å snakke om de erfaringene man hadde gjort bl.a. i møte med det bulgarske datatilsynet. For øvrig kom det klart frem i møtet at fremdriften i prosjektet ville gå som planlagt og at drift fra Bulgaria skulle iverksettes 1. mai i samsvar med prosjektplanen.

Et nytt møte ble avholdt 16. mai med representanter fra Helse Sør-Øst og Sykehuspartner til stede. I etterkant av dette møtet ble landvurderingen oversendt til oss. I dette møtet ble det informert om at prosjektet var midlertidig stanset i den forstand at driftsoperatører i Bulgaria ikke ble gitt de tilganger som de skulle ha etter opprinnelig prosjektplan.

I dette møtet ble vi også orientert om at det var satt i gang en ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod) i regi av PwC. Prosjektet var stanset i påvente av resultatet fra denne revisjonen.

Vårt krav om redegjørelse

Vår oppgave som tilsynsmyndighet i denne saken er å undersøke i hvilken grad de behandlingsansvarlige har handlet i samsvar med sine plikter etter pasientjournalloven § 22 jf. § 5, personopplysningsloven §§ 13-15 og personopplysningsforskriften kapittel 2 og 3. Vårt hovedfokus har vært å undersøke hvilke tiltak som ble gjort for å sikre etterlevelse av lovens krav i forbindelse med at det ble besluttet å benytte ekstern leverandør til drift av IKT-infrastruktur.

Helseforetakene ble bedt om å redegjøre for følgende:

1. Hvilke risikovurderinger lå til grunn da helseforetakene besluttet at drift og leveranse av IKT-infrastruktur i helseregionen kunne tjenesteutsettes og hvilke vurderinger lå til grunn for helseforetakets aksept av restrisiko? Plikten til å gjennomføre slike vurderinger følger av personopplysningsforskriften § 2-4 jf. pasientjournalloven § 22.

2. Hvilke risikovurderinger lå til grunn da helseforetakene besluttet at drift og leveranse av IKT-infrastruktur i helseregionen kunne leveres av valgt leverandør i Bulgaria, og hvilke vurderinger lå til grunn for helseforetakets aksept av restrisiko ved valg av denne leverandøren? Plikten til å gjennomføre slike vurderinger følger av personopplysningsforskriften § 2-4 jf. pasientjournalloven § 22 jf. § 5.

3. Gi en oversikt over hvilke eksterne leverandører som har tilgang til sykehusenes informasjonssystem, hvilke land leverandørene har tilgang fra, hvilke typer tilganger de har, til hvilke systemer, til hvilke personopplysninger (omfang, sensitivitet), samt formålet med tilgangene.

5.4 Helseforetakenes redegjørelse

Helseforetakene har valgt å besvare vårt krav om redegjørelse ved å utforme et felles brev. I besvarelsen vises det til at Sykehuspartner (SP) er felles IKT-leverandør og databehandler for alle helseforetakene og at det er SP som er ansvarlig for inngåelse av avtale med ekstern IKT-partner. Ekstern leverandør vil være en underleverandør til Sykehuspartner som fortsatt vil være ansvarlig leverandør overfor helseforetakene. Som følge av dette er risikovurderinger gjennomført i fellesskap for hele foretaksgruppen.

Helseforetakene har i sin redegjørelse lagt til grunn at verken beslutningen om å tjenesteutsette driften til en ekstern leverandør eller kontraktsinngåelsen med leverandøren innebærer en endring som har betydning for informasjonssikkerheten som krever risikovurdering i henhold til personopplysningsforskriften § 2-4.

Helseforetakene legger også til grunn at det ikke er et krav at risikovurdering skal gjennomføres før behandling av personopplysninger *iverksettes* eller før man *iverksetter* endring som kan ha betydning for informasjonssikkerheten. De viser til at det ikke fremgår av bestemmelsen i § 2-4 at slik vurdering må være foretatt før det tas beslutning om at arbeid med konkurranseutsetting skal påbegynnes. De anfører også at det vil være umulig å fullføre en risikovurdering før omfanget av tjenesteutsettingen, status på informasjonssystemene og kravene som vil bli stilt til informasjonssikkerhet og –tiltak hos leverandøren er nærmere avklart.

Videre er det gjort rede for at prosjektet, inkludert virksomhetsoverdragelse og overdragelse av driftsansvar fra SP til ekstern leverandør er stilt i bero, jf. styremøtet i Helse Sør-Øst RHF og deres vedtak av 24.05.17. Sykehuspartner ble i samme møte pålagt å utarbeide en plan for å styrke tilgangsstyring og forbedrede metoder for risiko- og sårbarhetsanalyser. De er også bedt om å gjennomføres nye risiko- og sårbarhetsanalyser og å sikre nødvendig forankring i helseforetakene. SP er også pålagt å utrede mulige alternativer for etablering av modernisert IKT-infrastruktur.

6 Datatilsynets vurdering og begrunnelse

I dette kapittelet vil vi redegjøres for rettslig grunnlag og de vurderinger vi har gjort som har ledet frem til vedtaket som er varslet i kapittel 2.

6.1 Ledelsesforankring/ansvarlighet

6.1.1 Rettslig grunnlag

Det følger av personopplysningsloven § 15 at en databehandler ikke kan behandle eller overføre opplysninger til en tredjepart uten at dette er skriftlig avtalt med den

behandlingsansvarlige. Ansvaret for avtaleinngåelsen kan gjerne delegeres, men databehandlingsansvaret og pliktene som følger av dette kan ikke delegeres.

Dette betyr at ansvaret for å beslutte om tjenesteutsetting i stort omfang er forsvarlig, om personvern blir ivaretatt, at det foreligger tilstrekkelig informasjonssikkerhet og aksept av restrisiko, ikke kan delegeres til andre, som for eksempel databehandleren eller det regionale helseforetaket.

Det er derfor helseforetakene som må svare for de risikovurderingene som ligger til grunn når det fattes beslutninger som har betydning for personvern og informasjonssikkerhet ved endringer som kan ha betydning for det som på forhånd er fastsatt som kriterier for akseptabel risiko.

Styring og kontroll er nødvendig for å sikre at de databehandlingsansvarlige etterlever sine lovpålagte plikter til bl.a. å vurdere risiko og personvernkonsekvenser ved tjenesteutsetting av IKT-drift og infrastruktur jf. pasientjournalloven § 22, personopplysningsloven § 15 og personopplysningsforskriften kapittel 2. Ledelsens plikt til å ha kontroll med virksomhetens informasjonssikkerhet kommer også klart til uttrykk i personopplysningsforskriften § 2-7. Bestemmelsen fastsetter krav om klare ansvars og myndighetsforhold for bruk av informasjonssystemet. Det stilles også krav om at endringer av konfigurasjon skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglig leder.

6.1.2 Opplysninger fremkommet i saken

Svarene vi har mottatt fra helseforetakene inneholder ingen dokumentasjon som viser at ledelsen i helseforetakene har vurdert og tatt stilling til i hvilken grad restrisiko er akseptabel for sin virksomhet.

Redegjørelsen viser derimot at Sykehuspartner har gjort vurderinger og tatt beslutninger på vegne av helseforetakene.

Eksempler på manglende kontroll og forankring omtales også fortløpende i våre øvrige vurderinger, da dette er en grunnleggende feil som materialiserer seg på flere områder.

6.1.3 Datatilsynets vurdering

Vår vurdering er at de behandlingsansvarlige ikke har hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet. Vi viser til redegjørelsen der det står at det er Sykehuspartner som har vært ansvarlige for kontraktsinngåelsen og at eventuelle risikovurderinger derfor er utført samlet for hele foretaksgruppen.

Helseforetakene har overlatt ansvaret for beslutninger som har betydning for pasientenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandleren og til ansatte lenger ned i organisasjonen. Organiseringen av prosjektet har derfor bidratt til å pulverisere ansvaret for å sikre at den databehandlingsansvarliges plikter etterleves. Konsekvensen av dette er manglende forankring og kontroll med beslutninger som er tatt.

6.1.4 Konklusjon

Manglende kontroll og manglende rutiner for å sikre kontroll anses å være i strid med kravene i pasientjournalloven § 22 jf. § 5, personopplysningsloven §§ 13- 15 og personopplysningsforskriften §§ 2-3 og 2-7.

6.2 Tilgangskontroll

6.2.1 Rettslig grunnlag

Tilgangskontroll skal sikre personopplysningers konfidensialitet, integritet og tilgjengelighet, jf. personopplysningsforskriftens §§ 2-11, 2-12 og 2-13 og pasientjournalloven § 22 jf. §§ 15 og 16. Tilgangsstyring er et sårbarhetsreduserende tiltak som implementeres på grunnlag av en risikoanalyse.

6.2.2 Opplysninger fremkommet i saken

Ut fra de listene vi har mottatt fra det enkelte sykehus (Vedlegg 8) ser vi at alle helseforetakene per i dag har europeiske driftsoperatører som har tilgang til pasientopplysninger i større eller mindre omfang. I tillegg ser vi at flere av sykehusene også har driftsoperatører fra 3. land utenfor EU. Dette er land som blant annet USA og India.

Når det gjelder tilgangen som er gitt til underleverandøren i Bulgaria i denne konkrete saken har Sykehuspartner informert Datatilsynet om at tilgangen var planlagt og ble gitt i samsvar med prosjektplanen. De har forklart for Datatilsynet at leverandøren har fått tilgang på like vilkår som andre leverandører. De har presisert overfor tilsynet at det ikke dreier seg om et avvik. Helse Sør-Øst RHF ved øverste leder har på sin side uttalt offentlig at det var en forutsetning for deres beslutning om å tjenesteutsette driften av IKT-infrastrukturen at utenlandske databehandlere ikke skulle ha tilgang til pasientopplysninger.

Dette viser at det har vært et sprik mellom ledelsen i Helse Sør-Øst og de ansvarlige for gjennomføring av kontrakten når det gjelder oppfattelsen av hva avtalen faktisk innebar med hensyn til hvilke tilganger som er nødvendige for oppfylle oppgavene som de bulgarske medarbeiderne skulle gjennomføre.

I PwC's revisjonsrapport pkt. 7 bekreftes tilsvarende funn.

6.2.3 Datatilsynets vurdering

Oversikt over eksisterende avtaler

Vår vurdering er at redegjørelsen viser at helseforetakene kan dokumentere oversikt over eksterne leverandører som har tilgang til sykehusenes informasjonssystemer. Ut over dette er vår vurdering at denne konkrete saken skiller seg fra de øvrige vi har fått oversikt over, blant annet fordi avtalene som er gitt tidligere gjelder tilganger av mindre omfang, knyttet til avgrensede systemer innenfor IKT-infrastrukturen. Vi mener derfor at det er store forskjeller på den tilgangen driftsleverandører av medisinteknisk utsyr o.l. har og den som er nødvendig for de som skal drifte og vedlikeholde hele IKT-infrastrukturen. Disse forskjellene innebærer at denne avtalen frembringer et helt annet risikobilde enn hva som har vært aktuelt ved mindre

omfattende avtaler. Derfor skulle man etter vår vurdering, åpenbart gjennomført en ny risikovurdering der man tok høyde for avtalens omfang og egenart.

Vi vurderer det som svært bekymringsverdig at det i forbindelse med denne konkrete saken ikke er iverksatt ekstra tiltak for å klarlegge om den tilgangen som er nødvendig for gjennomføring av avtalen er forenelig med foretakenes sikkerhetsstrategi og innenfor fastsatt risikotoleranse.

Databehandleravtaler

Vi legger til grunn at tilgangene som er beskrevet i Vedlegg 8 følger av databehandleravtaler som er inngått i samsvar med interne retningslinjer for informasjonssikkerhet og er avtaleregulert på en måte som sikrer vern av personopplysninger i samsvar med personopplysningsloven § 15 og forskriften § 2-15 jf. § 2-11. Vi har ikke kontrollert i hvilken grad disse avtalene tilfredsstiller lovens krav

I forbindelse med denne saken har vi fått opplyst at helseforetakene ikke har uført sikkerhetsrevisjoner av Sykehuspartener i forkant eller i etterkant av at det ble besluttet at virksomheten skulle være databehandler for alle foretakene. Vi har ikke hatt anledning til å undersøke forholdet mellom helseforetakene og Sykehuspartner som databehandler nærmere, men dersom det aldri er gjennomført sikkerhetsrevisjon –eller risikoanalyse for bruk av sykehuspartner som databehandler, kan dette også utgjøre avvik fra kravene i personopplysningsforskriften §§ 2-5 og 2-15 og pasientjournalloven § 22.

Vi presiserer at helseforetakene må gjennomgå sine rutiner for risikovurdering ved tildeling av leverandørtilgang og behandlingsansvarliges plikter ved bruk av databehandleravtaler for å sikre etterlevelse av kravene i dagens regelverk og det nye regelverket som trer i kraft 25. mai 2018.

Tilgangen som ble gitt til tjenesteleverandør i Bulgaria

Vi vurderer det som tilstrekkelig dokumentert at ekstern leverandør har hatt tilgang til pasientopplysninger, og at det ikke finnes system som gjør det mulig å finne ut om og i hvilken grad tilgangen til opplysningene har vært berettiget. Det er også uomtvistet at det ikke finnes et system som sikrer den behandlingsansvarlige oversikt over hvilke handlinger som er utført i systemet. Det er derfor uklart om opplysninger har kommet på avveie eller ikke.

Sykehuspartner har bekreftet overfor tilsynet at tilgangen er gitt i samsvar med avtale, mens ledelsen i Helse Sør-Øst har definert tilgangen til pasientopplysninger som et avvik. Ledelsen har lagt til grunn at tjenesteleverandøren ikke skulle ha tilgang til pasientopplysninger. Legger vi ledelsens forutsetning til grunn, innebærer det at opplysninger kom på avveie da tjenesteleverandøren fikk tilgang til pasientopplysninger.

Situasjonen er uheldig og kunne etter vår vurdering vært unngått dersom styrets beslutning hadde vært fattet på grunnlag av en risikovurdering der det i tilstrekkelig grad hadde kommet frem hvilke tilganger som er nødvendige for å nå målet med avtalen og hvilken risiko tilgangen innebærer med hensyn til konfidensialitet, tilgjengelighet og integritet.

Når de behandlingsansvarlige ikke er klar over at avtalen innebærer at det vil bli nødvendig for leverandøren å ha tilgang til pasientopplysninger, er det åpenbart at beslutningsgrunnlaget ikke i tilstrekkelig grad har gjort det mulig for de ansvarlige å fatte beslutning på riktig grunnlag.

Dersom tilgangene regnes som avvik innebærer dette overtredelse av personopplysningsforskriften §§ 2-9, 2-11, 2-13 til 2-16. Saken er ikke meldt til Datatilsynet som avvik og manglende avviksmelding er i så fall også i strid med kravet i forskriften § 2-6.

6.2.4 Konklusjon

Vi har tatt vedlagte oversikter over leverandørtilganger til etterretning. Vi har ikke grunnlag for å vurdere om avtalene beskrevet i vedlegg 8 er inngått i samsvar med personopplysningsloven §§ 15, 29 og 30. Vi har heller ikke undersøkt i hvilken grad helseforetakene oppfyller sine plikter til å gjennomføre planlagte og systematisk tiltak for å sørge for tilfredsstillende informasjonssikkerhet ved bruk av databehandlere etter personopplysningsforskriften § 2-11 og 2-15 jf. pasientjournalloven § 22.

Det er gitt tilgang til pasientopplysninger i strid med forutsetningene som lå til grunn for ledelsens beslutning om tjenesteutsette drift og vedlikehold av hele infrastrukturen i helseregionen. Tilgangen er gitt uten forankring i ledelsen og innebærer overtredelse av personopplysningsforskriften §§ 2-11 og 2-13 til 2-16. Tilgang gitt i strid med ledelsens beslutning viser også manglende ledelsesforankring som omtalt i punkt 6.1.

6.3 Risikovurdering

6.3.1 Rettslig grunnlag

Personopplysningsforskriften § 2-4 fastslår at den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for, og konsekvenser av sikkerhetsbrudd. Ved endringer som har betydning for informasjonssikkerheten skal det gjøres ny risikovurdering.

I bestemmelsens første ledd pålegges den behandlingsansvarlige å ha oversikt over hva slags personopplysninger som behandles. Slik oversikt er avgjørende for at virksomheten kan oppfylle sin plikt til å fastsette kriterier for akseptabel risiko forbundet med behandling av personopplysninger og for å etablere en forholdsmessig riktig sikkerhetsløsning i samsvar med kravet i § 2-1 jf. pasientjournalloven § 22.

I bestemmelsens siste ledd heter det at resultatet av risikovurderingen skal sammenliknes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av virksomhetens personopplysninger og at Datatilsynet kan gi pålegg om sikring av personopplysninger, herunder fastsette kriterier for akseptabel risiko forbundet med behandling av personopplysninger jf. § 2-2. Datatilsynet har derfor kompetanse til å overprøve vurderinger gjort av den databehandlingsansvarlige når det gjelder kriterier for akseptabel risiko.

Kravet til å gjennomføre risikovurdering gjelder i alle tilfeller der en behandlingsansvarlig virksomhet ønsker å overføre opplysninger til en tredjepart, uavhengig av formålet med overføringen. Med overføring mener vi også tilfeller der det skal gis tilgang til opplysninger.

Regelverket skiller ikke mellom utlevering i form av overføring, fysisk utlevering eller tilgang.

For å gjøre en tilstrekkelig risikovurdering må den behandlingsansvarlige først kartlegge hvilke opplysninger det dreier seg om og hvilken verdi disse opplysningene har for virksomheten selv. Verdivurderingen er også viktig for å kartlegge den potensielle verdien opplysningene kan ha for andre (trusselaktører) som kan ha interesse av å få tak i opplysningene og hvilken potensiell skade det kan få for de som eier opplysningene dersom noen ønsker å misbruke dem.

Opplysningenes karakter, verdi og omfanget har derfor betydning når man analyserer risiko. Risikobildet vil også påvirkes av faktorer som endrer seg for eksempel over landegrenser. Slike faktorer kan være rettsikkerhet, finansiell og politisk stabilitet, teknisk infrastruktur, hendelseshåndtering, levestandard, kultur og samfunnsstruktur som hver for seg kan ha betydning for risikoanalysen.

I personopplysningsloven § 29 om grunnleggende vilkår for overføring av personopplysninger til utlandet heter det at personopplysninger bare kan overføres til stater som sikrer en forsvarlig behandling av opplysningene. Videre legger bestemmelsen til grunn at stater som har gjennomført EUs personverndirektiv oppfyller kravet til forsvarlig behandling. I bestemmelsens annet ledd beskrives hvilke forhold som kan legges vekt på når det skal vurderes om kravet til forsvarlig behandling er sikret. Andre forhold som må tas i betraktning er opplysningenes art, den planlagte behandlingens formål og varighet samt de rettsregler, regler for god forretningsskikk og sikkerhetstiltak som gjelder for vedkommende stat. Uavhengig av hvilke forhold som gjør seg gjeldende har den behandlingsansvarlige plikt til å forsikre seg om at kravene til konfidensialitet, integritet og tilgjengelighet ivaretas før opplysningene overføres til en databehandler.

Ved vurdering av om opplysninger kan overføres til et tredje land må det foretas en konket vurdering av om leverandøren har et system som sikrer etterlevelse av kravene som gjelder for forsvarlig behandling av personopplysninger, herunder den behandlingsansvarliges plikter etter personopplysningsforskriften kapittel 2.

6.3.2 Nærmere om formålet med risikovurdering og når den må gjennomføres

Risikovurdering er nødvendig for å vurdere om behandling av personopplysninger kan skje i samsvar med lovpålagte krav

Formålet med pasientjournalloven er at behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at opplysninger er tilgjengelige for helsepersonell samtidig som vernet mot at opplysninger gis til uvedkommende ivaretas. Formålet med loven er også å sikre at helseopplysninger behandles på en måte som sikrer pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.

Pasientjournalloven § 8 pålegger virksomheter som yter helsehjelp å ha behandlingsrettede helseregistre for gjennomføring av helsepersonells dokumentasjonsplikt, jf.

helsepersonelloven § 39. De behandlingsrettede registrene skal være utformet og organisert slik at krav fastsatt i eller i medhold av lov kan oppfylles.

Pasientjournalloven § 22 pålegger den databehandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

I tillegg til at pasientjournalloven stiller strenge krav til journalsystemenes funksjonalitet, tilgjengelighet og konfidensialitet følger det av personopplysningsforskriftens kapittel 2 jf. pasientjournalloven § 22 en rekke plikter den databehandlingsansvarlige skal oppfylle for å sørge for slik informasjonssikkerhet som er nødvendig for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet.

Dersom fare for slik tap som nevnt over er til stede, skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften stå i forhold til sannsynligheten for, og konsekvensen av sikkerhetsbruddet.

Helseforetakenes plikt til å sikre pasienters og brukeres personvern er et grunnkrav og en forutsetning for at behandlingen av opplysninger skjer i samsvar med lovpålagte krav.

Lovpålagte krav som helsepersonellets taushetsplikt og pasientjournallovens krav til konfidensialitet, tilgjengelighet og integritet vil være førende for helseforetakenes sikkerhetsmål og risikotoleranse.

Disse føringene kommer klart til uttrykk i Helse- og omsorgskomiteens innstilling til Stortinget (Innst. 295 L – 2013-2014) der vi blant annet finner følgende sitater:

- *«Flertallet vil understreke at behandling og bruk av helseopplysninger alltid må skje på en måte som sikrer pasienters og brukeres personvern.»*
- *«Tillit mellom pasient og behandlende helsepersonell er en forutsetning for å yte helsehjelp av god kvalitet (...) Helsetjenestens taushetsplikt er et av de eldste og viktigste tiltak for å ivareta denne tilliten, ved å beskytte pasientens opplysninger fra å bli spredt.»*
- *«Flertallet vil understreke betydningen av at regelverket til enhver tid ivaretar et godt og framtidsrettet personvern, at man sørger for gode og forutsigbare rammebetingelser for utviklere av systemer og legger til rette for den teknologiske utviklingen i sektoren. Her må det spesielt legges vekt på sikkerhet og personvern i all kommunikasjon der pasientopplysninger er involvert, og at løsningene må være brukervennlige og effektive.»*

Helseforetakenes handlingsrom ved anskaffelser av IKT-tjenester er derfor begrenset i den forstand at de alltid må vurdere om, eller i hvilken grad tjenesten de ønsker levert påvirker deres mulighet til å etterleve det regelverket som gjelder særskilt for behandling av helseopplysninger i helsetjenesten. Personopplysningsforskriften § 2-4 pålegger derfor helseforetakene å fastlegge kriteriene for akseptabel risiko forbundet med behandling av personopplysninger i egen virksomhet.

Bestemmelsen i § 2-4 inneholder ingen tidsanvisning om når risikovurdering skal være utført, men formålet med bestemmelsen er å sikre at virksomheten klarlegger sannsynlighet for og konsekvenser av sikkerhetsbrudd og sammenlikner resultatet av vurderingen med virksomhetens fastlagte kriterier for akseptabel risiko.

Risikovurderinger skal for å oppfylle formålet med bestemmelsen, gjøres når det er nødvendig for å ta stilling til et endret risikobilde. Endret risikobilde kan forårsakes av ytre faktorer eller av planlagte endringer internt.

Risikovurdering i forkant av en anskaffelse er nødvendig for å klarlegge forhold som kan påvirke helseforetakenes evne til å sikre etterlevelse av regelverket. Ved å gjøre denne vurderingen i forkant blir det tydelig for oppdragsgiveren hvilke risikoreduserende tiltak som må gjennomføres eller kreves, for at tjenesten skal kunne leveres av en ekstern leverandør.

I denne konkrete saken mener vi en risikovurdering er nødvendig for å klarlegge om, eller i hvilken grad det er mulig å etterleve lovens krav dersom man overlater ansvaret for driften og tilgangen til IKT-infrastrukturen til en ekstern leverandør. Dersom leverandøren i tillegg er utenlandsk må det i forkant vurderes om, og i hvilken grad avtaleregulering av databehandlerens plikter er tilstrekkelig for å sikre etterlevelse av den databehandlingsansvarliges lovpålagte plikter. Det må også vurderes hvilke konsekvenser det kan få dersom opplysninger behandles i strid med avtalen utenfor nasjonal jurisdiksjon.

Risikovurderingen er nødvendig for å sikre forsvarlig sikkerhetsledelse

Plikten til å gjennomføre risikovurdering må også ses i sammenheng med plikten til å sørge for sikkerhetsledelse i samsvar med bestemmelsene i personopplysningsforskriften § 2-3. I bestemmelsen fastslås det at det er den som har den daglige ledelsen av virksomheten som har ansvaret for at forskriftens bestemmelser om informasjonssikkerhet følges.

Videre heter det at virksomhetens formål med behandlinger av personopplysninger og overordnede føringer for bruk av informasjonsteknologi skal beskrives i sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Sikkerhetsmål og sikkerhetsstrategi er igjen avgjørende for å vurdere om endringer i informasjonssystemet er innenfor det man på forhånd har vurdert som akseptabel risiko.

Bruken av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Resultatet fra gjennomgangen dokumenters og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.

Systematiske og planlagte tiltak skal sikre at virksomheten kontinuerlig arbeider med å sikre at behandlingen av personopplysninger til enhver tid skjer i samsvar med lovens krav.

Dersom helseforetaket vurderer å gjøre en endring som vil ha konsekvenser for informasjonssikkerheten og dermed påvirker foretakets evne til å oppfylle sin plikt til å sikre pasientenes personvern, må disse forholdene klarlegges slik at ledelsen kan ta stilling til om

konsekvensen av endringen er innenfor det akseptable og i samsvar med virksomhetens sikkerhetsstrategi.

Dersom det eksister en oversikt over hvilke tiltak som er nødvendige for å sikre fortsatt etterlevelse av regelverket, herunder muligheten til å nå virksomhetens sikkerhetsmål, og disse tiltakene vurderes som gjennomførbare innenfor rammene av fastsatt budsjett m.v. kan beslutningen om utkontraktering fattes.

Det følger av kravet til sikkerhetsledelse i forskriftens § 2-3 at beslutninger som har betydning for informasjonssikkerheten må være forankret i virksomhetens ledelse før arbeidet med å iverksette endringen starter.

Lovens system bygger på en risikobasert tilnærming og krav om forholdsmessighet

Lovens system er at behandling av personopplysninger i utgangspunktet er forbudt, med mindre den registrerte samtykker eller behandlingen er tillatt ved lov. Den behandlingsansvarlige må derfor forsikre seg selv og tilsynsmyndigheten om at behandlingen kan gjennomføres på en måte som tilfredsstiller vilkårene fastsatt i regelverket. Derfor skal risikovurderinger dokumenteres.

At risikobasert tilnærming til etterlevelse av regelverket er en forutsetning kommer også frem i personopplysningsforskriften § 2-1. Tiltakene som iverksettes for å oppnå tilstrekkelig informasjonssikkerhet skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Hva som er forholdsmessig vil avhenge av hvor stor fare det er for tap av blant annet personlig integritet og hvor nødvendig det er å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene som skal behandles.

Risikovurdering er etter gjeldende rett en nødvendig forutsetning for at den behandlingsansvarlige skal vite hvilke tiltak som er nødvendige for å sikre tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Hvilke tiltak som er iverksatt eller vurdert som nødvendige for å sikre forsvarlig behandling skal etter gjeldende rett presenteres for tilsynet dersom en behandling krever forhåndsgodkjenning.

I saker som krever forhåndsgodkjenning legges den behandlingsansvarliges beskrivelse av nødvendig sikkerhetstiltak til grunn for vurderingen av om behandling av personopplysninger kan tillates. Dersom tilsynet finner at personvernulempen ved en behandling i tilstrekkelig grad er avhjulpet kan det gis tillatelse til behandlingen jf. personopplysningsloven §§ 33-35.

Helseforetakene trenger ikke forhåndsgodkjenning for å behandle pasientopplysninger som ledd av det å yte helsehjelp, men må selv vurdere om de behandler opplysninger i samsvar med lovpålagte krav. Risikovurdering er en forutsetning for at ledelsen kan foreta disse vurderingene og dokumentere hvilke vurderinger de har lagt til grunn for sine valg.

Risikovurdering og personvernkonsekvensvurdering etter nytt regelverk

Systemet med risikobasert tilnærming kommer enda klarere til uttrykk i det nye personvernregelverket som trer i kraft 25. mai 2018. Et viktig virkemiddel for å sikre

etterlevelse av personvernforordningens krav er den behandlingsansvarliges plikt til å gjennomføre risiko- og personvernkonsekvensvurderinger.

I forordningens artikkel 32 omtales behovet for risikovurdering slik: «Idet det tas hensyn til *nåværende* utvikling i teknikken, *gjennomføringskostnadene* og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene og varierende sannsynlighets- og alvorlighetsgrad *for fysiske personers rettigheter og friheter*, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er *egnet i forhold til risikoen*, herunder blant annet, alt etter hva som er relevant

- Pseudonymisering og kryptering av personopplysninger
- Evnen til å sikre *vedvarende* fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og –tjenestene
- Evne til å gjenopprette tilgjengeligheten og tilgangen til opplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
- En *prosess* for *regelmessig* prøving, analysering og vurdering av hvor effektive behandlingens tekniske og organisatorisk sikkerhetstiltak er.

Forordningens tekst er mer utfyllende enn dagens ordlyd når det gjelder risikovurderinger og det fremgår tydelig at man for å oppnå formålet med slike vurderinger må gjøre dem før man bestemmer at et tiltak kan gjennomføres og fortløpende for å kontrollere om og i hvilken grad de tiltakene man anså som nødvendige gir tilstrekkelig sikkerhet over tid. Det fremgår også klart av teksten at sannsynligheten for, og hvor alvorlige konsekvenser et tiltak kan få for enkeltindividers rettigheter og friheter skal vurderes.

Forordningens artikkel 35 omhandler i tillegg plikten til å gjennomføre personvernkonsekvensvurdering. Slik vurdering må også gjøres i forkant av en beslutning om å behandle personopplysninger: «Dersom det er *trolig* at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, *vil medføre* høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige *før* behandlingen foreta en vurdering av hvilke konsekvenser den *planlagte behandlingen* vil ha for personopplysningsvernet.»

Datatilsynet ser at kravene til å vurdere risiko og personvernkonsekvenser er tydeliggjort og presisert i det nye regelverket, men det er ikke grunnlag for å tolke det nye regelverket annerledes enn det eksisterende når det gjelder risikovurderingens formål og tidspunktet for når slike vurderinger må gjennomføres

Risikovurderingens betydning på tilstøtende rettsområder

Sikkerhetsloven

Datatilsynet vurdering er at utkontrakteringen som det er snakk om i denne saken, på grunn av sitt omfang, ligger nær opp til eller i grenseland til sikkerhetslovens virkeområde. Sikkerhetsloven er relevant i vår vurdering av denne saken selv om den ikke kommer direkte til anvendelse.

Vi har vurdert det som relevant å drøfte om det er forsvarlig eller ønskelig å overlate den daglige kontrollen med disse opplysningene til en ekstern leverandør. Vi har tatt kontakt med Nasjonal sikkerhetsmyndighet i forbindelse med denne saken for å diskutere forholdet mellom sikkerhetsloven og stadig større samlinger av helsedata og eventuelle konsekvenser dette kan ha i et nasjonalt sikkerhetsperspektiv.

Etter sikkerhetslovens bestemmelser er det er opp til virksomheten selv å vurder om den virksomheten man driver er skjermingsverdig. Den laveste graden av skjermingsverdige objekter omfatter virksomheter som kan skade rikets selvstendighet og sikkerhet og andre vitale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse av uvedkommende (sikkerhetsloven § 17 a).

Selv om helseforetakene ikke har definert konsolideringen av pasientopplysninger i helseregionen som skjermingsverdig etter sikkerhetsloven, mener vi at helseforetakene som et minimum burde tatt i betraktning hvordan risikovurderinger utføres i saker som er omfattet av sikkerhetsloven.

I sikkerhetsloven er det presisert at virksomheten må vurdere hvilke konsekvenser det kan ha dersom funksjonaliteten reduseres, blir utsatt for skadeverk eller opplysninger rettstridig kommer uvedkommende i hende. Det burde vært avklart om tjenesteutsetting øker risikoen for eller konsekvensen av at noen av disse hendelsene inntreffer og hvilke krav som kan stilles for å redusere eventuell risiko.

Formålet med risikovurdering etter sikkerhetsloven er det samme som formålet med slik vurdering etter personopplysningsloven. Vi viser særlig til lovens § 29 a*: «Ved anskaffelser til kritisk infrastruktur skal det foretas en risikovurdering. I vurderingen skal det tas stilling til om anskaffelsen innebærer en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført mot eller ved bruk av infrastrukturen. Plikten til å gjennomføre risikovurdering gjelder ikke dersom det fremstår som åpenbart at anskaffelsen ikke kan innebære noen slik risiko.»*

Utredningsinstruksen

Vi har også sett hen til Utredningsinstruksen (Instruks om utredning av statlige tiltak) sist endret 1. mars 2016. Formålet med utredningsinstruksen er å legge et godt grunnlag for beslutninger om statlige tiltak, som for eksempel reformer, regelendringer og investeringer. Utredningsinstruksen gjelder ikke for egne rettssubjekter som for eksempel helseforetak, men det fremgår av veiledningen til instruksen at *«instruksen bør i alle tilfeller sees på som en god standard for involvering i og utredning av tiltak. Eierdepartementet kan for eksempel gjennom vedtekter pålegge statlige selskaper å følge instruksen.»* Instruksen er uansett et eksempel på at det stilles krav om at omfattende konsekvensutredninger skal være en del av beslutningsgrunnlaget når statlige forvaltningsorganer vedtar å iverksette for eksempel store investeringer.

Instruksen kommer til anvendelse ved tiltak, eller kombinasjoner av tiltak. I veiledningen er et gitt en oversikt over relevante kategorier av tiltak. Her finner vi offentlige tilbud av produkter

og tjenester, for eksempel infrastruktur og helsetjenester og offentlige anskaffelser, for eksempel IKT-tjenester og kontorutstyr.

Terskelen for hva instruksen er ment å omfatte av statlige gjøremål er altså ikke satt særlig høyt. Om Utredningsinstruksen står det at det er viktig at statlige beslutninger er velbegrunnede og gjennomtenkte. Ufullstendige eller manglende utredning øker risikoen for at det fattes beslutninger som ikke kan gjennomføres, som gir uønskede virkninger eller som innebærer sløsing med samfunnets ressurser. Instruksen gjelder for utarbeiding av beslutningsgrunnlag for statlige tiltak som utføres i, eller i oppdrag for statlige forvaltningsorganer.

Utredningen skal omfatte virkninger for enkeltpersoner, privat og offentlig næringsvirksomhet, statlig , fylkeskommunal og kommunal forvaltning og andre berørte. Det fremgår av veiledningen til instruksen at et av de seks viktige spørsmålene som skal besvares gjennom utredningen er hvilke prinsipielle spørsmål tiltakene reiser. En type prinsippspørsmål er slike som gjelder den enkeltes personvern og integritet. I veilederen står det følgende*: «Noen ganger utreder man tiltak som skal imøtekomme slike prinsipper. Andre ganger kan prinsippene legge begrensninger på hvilke tiltak som kan gjennomføres. Hvis et tiltak medfører virkninger som er i strid med ett eller flere prinsipp, kan utredningen måtte konkludere med at tiltaket ikke kan gjennomføres uansett hvilken nytteverdi det ellers måtte ha.»*

Dersom tiltakene berører prinsipielle spørsmål skal utredningen drøfte disse på en balansert, systematisk og helhetlig måte.

Det er utarbeidet en egen veileder til utredningsinstruksen som gjelder vurdering av personvernkonsekvenser. Hensikten med denne veilederen er å bidra til at statlige etater på en god måte kan utrede de personvernmessige konsekvensene av sine forslag.

Det er liten grunn til å anta at helseforetak er unntatt fra plikten til å utrede hvilke konsekvenser deres tiltak (tjenesteutsetting) har for den enkeltes personvern før det besluttes at tiltaket kan gjennomføres.

Finanssektoren

Vi har også innhentet informasjon fra Finanstilsynet for å undersøke hvilke føringer som gjelder innen finanssektoren når det gjelder utkontraktering av IKT-tjenester og vurdering av risiko i slike tilfeller. I forskrift om IKT-systemer i banker mv. § 2 fjerde ledd heter det at «avtaler om utkontraktering av IKT-virksomhet og endringer av slike avtaler skal behandles av styret. Styret skal forelegges planer for utkontrakteringen, med risikovurdering, og en beskrivelse av hvordan foretaket skal sikre leveransen.»

Finanssektoren har et regelverk der utkontraktering er behandlet flere steder. I helsesektoren er spørsmålet om utkontraktering i et slikt omfang som vi ser i denne saken nytt og regelverket har ingen særbestemmelser som regulerer spørsmålet.

Når helseforetakene problematiserer hvorvidt kravet om risikovurdering gjelder før eller etter beslutning om tjenesteutsetting, kontraktsinngåelse eller iverksetting av drift, mener vi det er relevant å vise til annet relevant regelverk der det stilles klare krav om at risikovurdering skal være en del av beslutningsgrunnlaget.

Lov om offentlige anskaffelser

Datatilsynet har også i forbindelse med denne saken vært i dialog med Direktoratet for forvaltning og ikt (Difi) og diskutert grenseflatene mellom kravene til risikovurderinger i personopplysningsforskriften og plikten til å gjennomføre anskaffelser i tråd med anskaffelsesregelverket. Difi uttrykte klart at risikovurderinger også er en nødvendig forutsetning for planlegging av anskaffelser, særlig i forbindelse med anskaffelser der det stilles krav til sikring av konfidensialitet, integritet og tilgjengelighet. Formålet med lov om offentlige anskaffelser er presisert i § 1: Den skal fremme effektiv bruk av samfunnets ressurser og bidra til at det offentlige opptrer med integritet, slik at allmennheten har tillit til at offentlige anskaffelser skjer på en samfunnstjenlig måte.

I forskrift om offentlige anskaffelser § 2-2 er det presisert at anskaffelsesloven og forskriften ikke gjelder anskaffelser som kan unntas etter EØS-avtalen artikkel 123. I denne artikkelen heter det at bestemmelsene i denne avtalen (EØS-avtalen) ikke skal hindre en avtalepart i å treffe tiltak som den anser som nødvendige for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser.

Regelverket gjelder heller ikke for anskaffelser som bare kan utføres under særlige sikkerhetstiltak i henhold til lov, forskrift eller forvaltningsvedtak, og de aktuelle vesentlige interessene ikke kan sikres gjennom mindre inngripende tiltak.

Regelverket gjelder heller ikke dersom anvendelsen av det vil forhindre oppdragsgiveren fra å ivareta vesentlige sikkerhetsinteresser. Regelverket gjelder likevel dersom oppdragsgiveren kan ivareta disse interessene ved mindre inngripende tiltak (enn å unnta fra regelverket), for eksempel ved å pålegge leverandørene taushetsplikt.

I dette ligger at oppdragsgiver i forkant av en anskaffelse må vurdere om og i hvilken grad anskaffelsen kan eller bør unntas fra regelverket hel eller delvis som følge av at det stilles spesielle sikkerhetskrav til leveransen. Det må også vurderes om sikkerhetsrisikoen kan avhjelpes i tilstrekkelig grad ved at det for eksempel stilles krav i forbindelse med kvalifikasjon av leverandører. Dette betyr at oppdragsgiver må gjøre en konkret vurdering av anskaffelsen i forhold til eventuelle andre lovpålagte krav som påhviler virksomheten og dermed anskaffelsen. For å gjøre denne vurderingen må oppdragsgiver foreta en risikovurdering før det besluttes hvilke prosedyrer som skal benyttes i anskaffelsesprosessen. En anskaffelse kan unntas i sin helhet, eller man kan ende på et resultat som tilsier at regelverket kommer til anvendelse forutsatt at det stilles klare kvalifikasjons- og sikkerhetskrav.

Det er derfor ikke slik at plikten til å gjennomføre en anskaffelse i tråd med forskriftens kapittel III går foran oppdragsgiverens plikt til å sørge for etterlevelse av øvrig regelverk og sikkerhetskrav som gjør seg gjeldende i det konkrete tilfellet. Det er heller ikke slik at det kun

er anskaffelser som er omfattet av sikkerhetslovens bestemmelser som kan unntas fra regelverk om offentlige anskaffelser helt eller delvis. Bestemmelsene i anskaffelsesregelverket viser også at det er en forutsetning at risikovurderinger gjennomføres som en del av planleggingsfasen, før man iverksetter en anskaffelsesprosess som har utkontraktering av IKT-tjenester som mål.

6.3.3 Opplysninger fremkommet i saken

Risikovurderingen som ble gjort i forkant av beslutningen om tjenesteutsetting

I redegjørelsen vises det til at det i forkant av beslutningen om å benytte en kommersiell aktør for å modernisere regionens infrastruktur ble gjennomført en risikovurdering av alternativer for moderniseringen. Alternativene som ble vurdert var «gjør det selv» alternativet mot «ekstern partner». Analysen er vedlagt og betegnes «Risikoanalyse av alternativer for modernisering av infrastruktur». Analysen tar utgangspunkt i måloppnåelsen som er definert som alternativenes evne til å levere en modernisert infrastruktur på planlagt tid , til planlagt kostnad og med samme tjenestenivå til sykehusene ved ferdigstillelse. Risikomålene som er vurdert som relevante for Helse Sør-Øst er

- Tid: i hvilken grad risikoen vil påvirke gjennomføring av moderniseringen innenfor planlagt tidshorisont,
- Kost: i hvilken grad risikoen vil påvirke kostnadene for valgt alternativ,
- Kvalitet: i hvilken grad risikoen vil påvirke kvaliteten på leveransen, basert på kvalitetskrav i avtalen og
- Omdømme: i hvilken grad risikoen vil påvirke omdømmet til Helse Sør-Øst og Sykehuspartner.

Rapporten definerer to scenarioer som har konsekvenser for personvern og informasjonssikkerhet. I alternativet «ekstern partner» er det påpekt at det er en risiko for at man ved gjennomføring av avtale med ekstern partner øker Sykehuspartner sin synlighet i IT-verden og attraktiviteten for cyber angrep kan øke (R-0048). Sannsynligheten er satt til 1 og konsekvensen er vurdert som høy (5) for omdømmetap. Det er også satt som risiko i pkt. R-0037 at dersom personopplysninger aksesseres fra utlandet og ikke behandles i henhold til norsk lov kan personinformasjon komme på avveie. Sannsynligheten er satt til 2 og konsekvensen er vurdert lav (2) for økte kostnader og høyere (4) for omdømmetap. Vi kan ikke se at det er gjort nærmere analyser av i hvilken grad dette er forhold som kan få betydning for lovpålagte krav til informasjonssikkerhet og foretakenes plikt til å sikre den enkeltes personvern.

Særlig om helseforetakenes vurdering av risiko ved valg av underleverandør

Sykehuspartner gjennomførte en landvurdering av Bulgaria i februar 2017. Vurderingen ble gjort i etterkant av at det var besluttet å benytte valgte underleverandør. Vi har ikke mottatt ny dokumentasjon som viser at landvurderingen ble forelagt de behandlingsansvarlige før valg av leverandør ble bestemt.

Vurderingen som ble gjort tar opp en rekke relevante problemstillinger. Vi visert til følgende uttrekk:
Fra kapittel 1 Landrisiko:

- *«På europakommisjonens nettsider er det publisert det som skal være lov om beskyttelse av personopplysninger i Bulgaria og det legges derfor til grunn at dette faktisk er gjeldende lov. Denne loven stiller ikke eksplisitte krav til internkontroll, men dekker sentrale rettigheter for den registrerte. En viss usikkerhet vil det derimot være frem til en reell avklaring foreligger på lovens gyldighet i Bulgaria.»*
- *«Forholdet mellom den bulgarske personopplysningsloven og andre lover som eventuelt undergraver den registrertes rettigheter eller er til hinder for at databehandlingsansvarlige kan ivareta sine forpliktelser er ikke kartlagt som del av denne risikovurderingen.(…) Derfor er det usikkert hvorvidt personopplysninger om norske pasienter og ansatte er skjermet for bulgarske eller samarbeidende lands myndigheter.»*
- *«I følge Transparency International vurderes Bulgaria å ha relativt store utfordringer knyttet til korrupsjon ved at de rangeres på 75. plass på deres korrupsjonsindeks. Problemet med korrupsjon vurderes å redusere virksomhetens evne til å ivareta krav til informasjonssikkerhet og internkontroll, og vurderes å være en trussel mot personvernet.»*

Kapittel 6 Økonomiske forhold knyttet til endringer i internkontroll:

- *«Ved bruk av tjenesteleverandører fra utlandeske selskaper, er det naturlig å anta at dette vil medføre økte kostnader til å gjennomføre kontrollhandlinger som følge av reisevirksomhet, bruk av nye leverandører (som revisorer) og behov for ressurser til oppfølging av regulatoriske forskjeller. Det er uklart hvorvidt Sykehuspartner HF for 2017 har budsjettert med økte rammer for å gjennomføre kontroll av leverandører i utlandet, og dersom dette ikke korrigeres vil det redusere foretaksgruppens evne til å inkludere tjenesteleverandører fra utlandet i internkontrollen.»*

Vi har mottatt møtereferat fra ekstraordinært RSV-møte 19. mai der landvurderingen ble diskutert med representanter fra helseforetakene. Konklusjonen i vurderingen var at risikonivået samlet sett ville øke og at det derfor var nødvendig å iverksette tiltak for å lukke avvik.

Formålet med møtet var å bli enige om hvilke tiltak som måtte implementeres for å avhjelpe de sårbarhetene som var identifisert i landvurderingen. I dette referatet fremgår det at noen av representantene fra de ulike helseforetak var bekymret som følge av risiko knyttet til å legge driften til Bulgaria. Flere etterspurte personvernkonsekvensvurderinger og det ble reist spørsmål om i hvilken grad ledelsen og politikere var tilstrekkelig informert om at opplysninger ville bli utlevert til medarbeidere i Bulgaria.

Det ble også understreket i møtet at det ikke var aktuelt å stille spørsmål om det var forsvarlig å benytte leverandøren i Bulgaria, men at temaet kun var å vurdere hvilke tiltak som var nødvendig å implementere for å redusere den økte risikoen. Dette ble sagt til tross for at det i risikovurderingen står på side 2, at målsetningen med den er å vurdere hvorvidt risikonivået prinsipielt endrer seg utenfor risikoakseptkriterier ved *eventuell* databehandling fra Bulgaria, samt eventuelt identifisere nødvendige tiltak/forutsetninger for å kunne gjennomføre databehandling.

Det er uklart i hvilken grad ledelsen i helseforetakene har vært forelagt landvurderingen og de risikoer som der er avdekket før beslutningen om å gå videre med Bulgaria som land ble tatt. Vi finner ikke dokumentasjon som tilsier at risikovurderingen om Bulgaria ble forelagt ledelsen i henholdsvis Sykehuspartner, helseforetakene eller Helse-sør-øst.

Andre forhold i saken som viser at risikovurdering skulle vært utført

Etter at Datatilsynet første gang ba om å se de risiko- og personvernkonsekvensvurderingene som lå til grunn for beslutningen om å tjenesteutsette driften av IKT-infrastrukturen, har det vist seg at mangel på slike vurderinger har fått alvorlige konsekvenser for prosjektet. Vi nevner særlig potensielle økonomiske konsekvenser som følge av at det er inngått avtale med en tjenesteleverandør uten i forkant å ha klarlagt hvilke forutsetninger som må være på plass før avtalen kan inngås. I Helse Sør-Øst er moderniseringsprosjektet satt på vent inntil videre i påventa av at det blir vurdert om det er forsvarlig å fortsette prosjektet. Alminnelig avtalerett tilsier at dette kan få uønskede konsekvenser for oppdragsgiver.

6.3.4 Datatilsynets vurdering

Vår vurdering er at risikovurderingen som ble gjort i forkant av beslutningen om tjenesteutsetting ikke har som mål å analysere risiko relatert til behandling av personopplysninger og plikten til å sikre tilfredsstillende informasjonssikkerhet og personvern ved behandlingen. Formålet med vurderingen er å synliggjøre forhold som kan ha betydning for om prosjektet når målet om å ferdigstille moderniseringen til ønsket kvalitet, innen en gitt tidsperiode, innenfor et gitt budsjett uten å skade Sykehuspartners omdømme. Vi omtaler ikke denne vurderingen nærmere.

Datatilsynet legger til grunn at både beslutningen om å gjennomføre tjenesteutsettingen og selve avtaleinngåelsen innebærer endringer som har konsekvenser for informasjonssikkerheten i de behandlingsansvarliges virksomhet. Avtaleinngåelsen er en naturlig konsekvens av igangsatt anskaffelsesprosess. Anskaffelsesprosessen er et direkte resultat av at det ble besluttet å tjenesteutsette det aktuelle oppdraget. I det følgende forklarer vi hvorfor denne beslutningen må betraktes som en endring som omfattes av kravet i § 2-4.

Utkontrakteringen innebærer at en ekstern leverandør vil få tilgang til hele infrastrukturen og dermed pasientopplysningene i helseregionen. Den eksterne leverandøren vil ha ansvaret for at pasientopplysninger og medisinsk infrastruktur er tilgjengelig når det er nødvendig for å yte helsehjelp. Samtidig innebærer utkontrakteringen at den behandlingsansvarlige kan få redusert kontroll med infrastrukturen og bruken av informasjonssystemet, altså redusert tilgangskontroll. Endrede muligheter for å kontrollere etterlevelse av lovpålagte krav er også en naturlig konsekvens av utkontrakteringen. .

Den planlagte sentraliseringen av all infrastruktur innebærer i tillegg at konsekvensen av sikkerhetsbrudd kan bli omfattende og få alvorlige konsekvenser for mange berørte. Den omfattende samlingen av sensitive personopplysninger på et sted betyr også at verdien av opplysningene øker betraktelig med tanke på misbruk, manipulering og skade, og at konsekvensen av sikkerhetsbrudd potensielt vil ramme halve Norges befolkning.

Avtalen omfatter overføring av store mengder sensitive personopplysninger til utlandet og stiller derfor ekstra strenge krav til behandlingsansvarlige når det gjelder å sikre forsvarlig og trygg behandling av pasientopplysninger.

Om sikkerhetsbrudd skjer i Norge eller i utlandet trenger ikke å være av betydning, men det skulle vært vurdert om og i hvilken grad utlevering til tredjeland innebærer økt risiko.

Basert på den kommunikasjonen vi hadde med Helse Sør-Øst høsten 2016 og fremover har vi lagt til grunn at det ikke har vært utført slike vurderinger som loven krever i forkant av beslutning om valg av tjenesteleverandør/underleverandør i Bulgaria.

Risikovurderingen skulle for å være tilstrekkelig utført, synliggjøre trusselbildet og ta høyde for at denne samlingen pasientopplysninger er den største samlingen helseopplysninger som noen gang har blitt vurdert tilgjengeliggjort for utenlandske leverandører. I denne vurderingen skulle det vært tatt høyde for at personopplysningene har avgjørende verdi for dem som trenger dem for å utføre sine oppgaver, og at opplysningene kan ha svært stor verdi for andre som ikke i utgangspunktet er berettiget tilgang til dem

En snever tolkning av kravet til risikovurdering i personopplysningsforskriften § 2-4 vil være uforenelig med lovens og bestemmelsens formål og øvrige bestemmelser som pålegger den databehandlingsansvarlige å sikre personvern i alle ledd av virksomheten.

Vi viser også til revisjonsrapporten fra PwC der det blant annet i punkt 6 oppsummeres at sentrale informasjonssikkerhetsrisikoer knyttet til ESN-avtalen ikke er tilstrekkelig vurdert.

Aksept av restrisiko ut over de kriteriene som på forhånd er fastsatt, kan aldri delegeres fra den behandlingsansvarlige til en databehandler. Basert på den dokumentasjonen vi er forelagt ser det ut som at landvurdering og aksept av restrisiko ikke er forankret hos ledelsen i det enkelte helseforetak som er databehandlingsansvarlig.

Vår vurdering er derfor at opplysningene som er fremkommet i saken og i svaret fra helseforetakene viser at de behandlingsansvarlige ikke har tatt det ansvaret de har overfor databehandler som er gitt ansvaret for avtaleinngåelsen.

Vi er derfor ikke enig i helseforetakenes vurderinger vedrørende kravene til å gjennomføre risikovurdering. Vi er overrasket over at og Sykehuspartner har lagt til grunn at denne avtalen om tjenesteutsetting ikke skiller seg fra andre avtaler de har inngått med underleverandører.

Vår vurdering støttes av funn i revisjonen utført av PwC på vegne av Helse Sør-Øst. I rapporten er det konkludert med at systemet for vurdering av risiko ikke har fungert som et effektiv kontrollmekanisme. Vi viser til rapporten s. 5 og PWCs vurderinger, særlig i kapittel 5.

6.3.5 Konklusjon

Datatilsynets konklusjon er at beslutningen om å tjenesteutsette IKT-drift og fornying av infrastrukturen innebærer endring som er omfattet av kravet om å gjennomføre risikovurdering i personopplysningsforskriften § 2-4.

Manglende etterlevelse av plikten til å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten er i strid med kravet i pasientjournalloven § 22 jf. personopplysningsforskriften §§ 2-4 jf. 2-1.

Vi har ikke mottatt dokumentasjon som viser at det enkelte helseforetak har oppfylt kravene i personopplysningsforskriften §§ 2-15 jf. 2-1 (forholdsmessighet), 2-3 (sikkerhetsledelse), 2-4 (Risikovurdering), 2-5 (Sikkerhetsrevisjon), og 2-7 (organisering) i forkant av at det ble tatt beslutning om å legge drift av IKT til underleverandøren i Bulgaria.

7 Varsel om vedtak -Overtredelsesgebyr

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven og pasientjournalloven. Vi har konstatert at det foreligger overtredelse av bestemmelsene i pasientjournalloven §§ 22 jf. 5 jf. personopplysningsforskriften §§ 2-1, 2-3, 2-4, 2-7 og 2-11 og 2-15.

7.1 Datatilsynets vurdering

Helseforetakene har som følge av overtredelsene akseptert at drift og vedlikehold av hele helseregionens IKT-infrastruktur skal tjenesteutsettes, uten å ha vurdert hvilken risiko denne endringen vil ha med tanke på informasjonssikkerhet og personvern. Helseforetakene har heller ikke vurdert om risikoen ved å endre driften av informasjonssystemet er akseptabel i forhold til virksomhetens fastsatte mål for akseptabel restrisiko. Ansvaret for de beslutningene som er tatt er i sin helhet overlatt til moderniseringsprosjektet som er gjennomført i regi av Sykehuspartner etter instruks fra Helse Sør-Øst RHF. Dette har skjedd til tross for at ansvaret for å sikre etterlevelse av pasientjournalloven og personopplysningslovens bestemmelser påhviler helseforetakene som databehandlingsansvarlige for virksomhetens behandling av personopplysninger.

Overtredelsene innebærer at helseforetakene ikke har oppfylt sin plikt etter pasientjournalloven § 22 til gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet, samt å påse at andre som får tilgang til helseopplysninger også oppfyller pasientjournallovens krav om å sikre konfidensialitet og personvern i samsvar med lovens formål.

Prosjektet «Digital fornying» har i for liten grad fokusert på helseforetakenes plikt til å sikre personvern jf. pasientjournalloven § 1 bokstav b) og plikten til å sikre tilstrekkelig informasjonssikkerhet samtidig som målet om bedre kvalitet, effektivitet og tilgjengelighet oppnås.

7.1.1 Konklusjon

Vi mener det er nødvendig å reagere på overtredelsene som har funnet sted i denne saken, og varsler med dette ileggelse av overtredelsesgebyr med hjemmel i pasientjournalloven § 29 jf. §§ 27 og 5.

I samsvar med Høyesteretts praksis (jf. Rt. 2012 side 1556) legger vi til grunn at overtredelsesgebyr er å anse som straff etter den europeiske menneskerettighetskonvensjonen art 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

I vurderingen av om overtredelsesgebyr skal ilegges skal det særlig legges vekt på momentene som er listet opp i pasientjournalloven § 29 annet ledd bokstav a-h.

7.2 Vurdering av om overtredelsesgebyr skal ilegges

7.2.1 Alvorlighetsgrad, vurdering av §29 a

Modernisering og digitalisering på mange områder i helsesektoren er nødvendige forutsetninger for å nå de politiske målsetningene om bedre kvalitet i helsetjenesten, økt pasientmedvirkning og bedre personvern.

Sektoren fikk nytt regelverk i 2015 der det ble åpnet opp for nye muligheter til behandling av helseopplysninger på tvers av virksomheter. Det ble gitt nye bestemmelser om felles journal, tilgang på tvers av virksomheter, nasjonal kjernejournal og andre nasjonale journalsystemer som skal erstatte virksomhetsinterne journalsystemer. I tillegg skjer det store endringer i systemet for digital reseptformidling der det også skal registreres legemidler i bruk i tillegg til at flere brukere av systemet får tilgang til opplysningene. Det legges også til rette for brukertilpassede løsninger som skal gi befolkningen enklere tilgang til egne opplysninger og mulighet for å kontrollere hvem som har hatt tilgang til opplysninger, samt mulighet for økt kontroll med hvem som skal få tilgang til hvilke opplysninger.

Slike løsninger er helt nødvendig for å etterleve plikten til å sikre pasienters og brukeres personvern samtidig som det utvikles effektive systemer for å sikre tilgang til relevant informasjon når det er nødvendig for å yte helsehjelp. Det overordnede politiske målet er «En innbygger –en journal». Utviklingen i sektoren innebærer at pasientens en til en forhold til helsepersonell og helsepersonells taushetsplikt slik vi kjenner den, er under stort press. Argumentene som benyttes for å berolige de som er bekymret for at pasientopplysninger kommer på avveie er at personvernet skal bli bedre ved bruk av moderne informasjonsteknologi. Dersom målet om bedre personvern ved bruk av moderne teknologi skal nås er det en forutsetning at aktørene i sektoren tar sin plikt til å sikre personvernet på alvor når de iverksetter prosjekter med digital fornying som målsetting.

Utviklingen i sektoren bidrar til at vi stadig ser større samlinger av pasientopplysninger lagret på ett sted. Historisk sett har risikoen for at opplysninger skal komme på avveie vært begrenset i den forstand at helseopplysninger om relativt få pasienter var spredd og lagret lokalt i ulike virksomheter. Nå er trenden at opplysningene samles i felles systemer. Det skjer i Helse Vest, Helse Midt og Helse Sør-Øst i tillegg til at det skjer gjennom nasjonale systemer som reseptformidleren, kjernejournal, mv.

Datatilsynets oppfatning er at modernisering som kan bidra til tilgjengeliggjøring av opplysninger som er nødvendige for å yte helsehjelp og dermed bedre kvalitet i helsetjenesten er positivt. Vi ønsker muligheter og initiativer velkommen, forutsatt at aktørene samtidig ivaretar sin plikt til å sørge for godt personvern gjennom blant annet å sørge for tilstrekkelige informasjonssikkerhetstiltak.

Vår vurdering er at denne saken om tjenesteutsetting tydelig har vist at personvernperspektivet ikke i tilstrekkelig grad er ivaretatt. Vi ser det som svært alvorlig at Helse Sør-Øst RHF ikke har sørget for at prosjektet er gjennomført på en måte som sikrer forankring i de behandlingsansvarlige helseforetakene.

Vi ser også svært alvorlig på at helseforetakene som er pliktsubjekter etter pasientjournalloven og personopplysningsloven ikke har etablert systemer som sikrer at de har nødvendig kontroll med beslutninger som ligger under deres ansvarsområde.

Overtredelsene som er avdekket i denne saken er også alvorlige fordi den behandlingsansvarliges oversikt over risikobildet og kontroll med behandling av opplysninger er nødvendige forutsetninger for å sikre etterlevelse av de øvrige bestemmelsene i regelverket.

Helseforetakene i Helse Sør-Øst er ulike med tanke på størrelse og det er individuelle forskjeller med tanke på tilgjengelige ressurser og nødvendig kompetanse om informasjonsteknologi og personvern. Vi regner allikevel alle som profesjonelle aktører som har behandling av personopplysninger og etterlevelse av bestemmelsene i pasientjournalloven og personopplysningsloven som en viktig del av sin kjernevirksomhet.

At helseforetakene må regnes som profesjonelle aktører innebærer at forventningene til at regelverket etterleves er store. Etterlevelse er også av stor betydning for å bevare befolkningens tillitt til at heletjenesten behandler pasientopplysninger på en trygg og sikker måte. Omfanget av sensitive opplysninger som skal forvaltes gjennom avtalen som er inngått mellom Sykehuspartner og ekstern leverandør er svært stort og skiller seg i så måte fra alle forutgående saker om tjenesteutsetting i helsesektoren.

Saken har vist mangelfull kompetanse om gjennomføring av risikovurdering og nødvendigheten av å vurdere restrisiko i tillegg til manglende sikkerhetsledelse og ledelsesforankring.

Oppsummert mener vi overtredelsene er svært alvorlige fordi de viser mangelfull etterlevelse og forståelse av grunnleggende krav som er nødvendige forutsetninger for å sikre etterlevelse av regelverket. I tillegg dreier det seg om profesjonelle aktører i en sektor i utvikling hvor det er helt nødvendig at aktørene har systemer og kompetanse som sikrer at behandling av personopplysninger skjer i samsvar med regelverket og grunnleggende prinsipper om personvern.

7.2.2 I hvilken grad den databehandlingsansvarlige har utvist skyld, vurdering av §29b

Det fremkommer av forarbeidene til bestemmelsen (Ot.prp. nr. 72 (2007-2008) Om lov om endring i personopplysningsloven mv.) at det med graden av skyld siktes til hvor

klanderverdig handlingen er, for eksempel om den bærer preg av uhell eller om den har et mer systematisk eller planmessig preg.

Ansvaret for etterlevelse av regelverket ligger hos den behandlingsansvarlige, men en databehandler har også en selvstendig plikt til å sikre at opplysninger behandles i samsvar til regelverket i databehandlerens virksomhet.

Overtredelsene kan skyldes mangelfull kompetanse i linjen og/eller uklare rutiner eller manglende system for å sikre forankring i ledelsen. Helseforetaksstrukturen, styringsmodellen i RHFet, prosjektorganiseringen, sykehuspartners rolle som databehandler og ansvarlig for kontraktsinngåelsen er faktorer som samlet sett bidrar til viske ut de klare ansvarslinjene som det stilles krav om i personopplysningsforskriften § 2-7.

Det er allikevel slik at det er helseforetakene som er pliktsubjekter etter personopplysningsloven. Hvert foretak er et selvstendig rettssubjekt og det er i foretakenes interesse å sørge for etterlevelse av gjeldende rett. Vi kan ikke se at det foreligger omstendigheter som tilsier at helseforetakene ikke har utvist skyld i denne saken.

Det kan diskuteres om eller i hvilken grad Helse Sør-Øst RHF har medvirket til overtredelsene gjennom sine føringer og måten moderniseringsprosjektet er organisert og styrt. RHFet har selv uttrykt at det må utarbeides nye rutiner som sikrer nødvendig forankring i helseforetakene. Med dette erkjenner ledelsen i Helse Sør-Øst at prosjektet ble styrt på en måte som ikke har gitt helseforetakene nødvendig kontroll med de beslutningene som ble tatt.

Vi reiser denne problemstillingen fordi vi mener det er viktig at den diskuteres i regionshelseforetaket, slik at det etableres rutiner som ivaretar helseforetakenes autonomi ved felles beslutninger.

Oppsummert er vår vurdering at de behandlingsansvarlige har utvist skyld ved å overlate beslutninger som har betydning for virksomhetens plikter etter personopplysningsforskriften og pasientjournalloven til moderniseringsprosjektet uten å sikre at beslutninger som ble tatt var akseptable i forhold til virksomhetens risikotoleranse og uten å sørge for ledelsesforankring før beslutninger ble tatt.

7.2.3 I hvilken grad kunne overtredelsen vært unngått , vurdering av §29 c

Vår vurdering er at overtredelsene kunne vært unngått dersom foretakene hadde hatt rutiner for å sikre etterlevelse av kravene i personopplysningsforskriften i forbindelse med konsernovergripende avtaleinngåelser og i alle saker som har betydning for virksomhetens plikter til å etterleve kravene i personopplysningsforskriften kapittel 2.

Overtredelsene kunne også vært unngått dersom prosjektledelsen hadde sørget for å etabler rutiner som sikret ledelsesforankring ved beslutninger og dersom risikovurderinger hadde vært forelagt de databehandlingsansvarlige før beslutninger ble tatt.

Kompetanse om den databehandlingsansvarliges plikt til å etterleve kravene i personopplysningsloven og forskriften jf. pasientjournalloven § 22 i foretaksledelsen kunne

også bidratt til at kravene om ledelsesforankring og organisering, plikten til å gjennomføre restrisiko og ledelsen plikt til å akseptere restrisiko hadde blitt ivaretatt i moderniseringsprosjektet.

Dersom det hadde blitt gjennomført en risikovurdering med fokus på prosjektets konsekvenser for personvern og informasjonssikkerhet, i tillegg til fokus på å nå målet om effektivisering og modernisering innenfor prosjektets rammer, kunne dette også ha bidratt til en annen styringsmodell.

Vi understreker at ansatte i konsernet, fagforeningsrepresentanter, pasienter med flere tidlig i prosessen varslet om at de planlagte endringene måtte vurderes med tanke på personvern og informasjonssikkerhet, uten at dette fikk konsekvenser for prosjektets fremdrift.

Datatilsynets involvering i saken skyldes først og fremst at vi mottok en rekke henvendelser fra enkeltindivider og interesseorganisasjoner som hadde uttrykt bekymring for prosjektet, uten å bli hørt.

Overtredelsene kunne også vært unngått dersom prosjektet hadde rådført seg med Datatilsynet i forkant.

Oppsummert er vår vurdering at overtredelsene kunne vært unngått dersom helseforetakenes plikt til å oppfylle kravene i pasientjournalloven og personopplysningsforskriften kapittel 2 hadde vært inntatt som en forutsetning for å nå målet med prosjektet.

7.2.4 Har overtredelsen fremmet den de behandlingsansvarliges interesser? Vurdering av §29 d)

Overtredelsen har sannsynligvis bidratt til en smidigere prosjektledelse ved at beslutninger har blitt tatt på vegne av alle helseforetakene uten at helseforetakene har tatt nødvendig stilling til om beslutningene er i samsvar med foretakets sikkerhetsstrategi og fastsatt risikotoleranse. Overtredelsene kan ha bidratt til at prosjektet har resultert i en avtale basert på en løsning som er rimeligere enn den ville vært dersom det var klart for alle parter at den eksterne leverandøren måtte få tilgang til pasientopplysninger for å utføre sine oppgaver.

Dersom en risikovurdering for eksempel hadde klarlagt at kryptering er nødvendig for å sikre konfidensialitet, fordi helseforetakene vurderer det som nødvendig for å hindre tilgang til pasientopplysninger, hadde løsningen blitt en annen, mest sannsynlig mer kostbar. En risikovurdering kunne også resultert i et krav om kontrolltiltak som kunne fått betydning for resultatet.

Overtredelsen har bidratt til at prosjektet kunne arbeide etter en styringsmodell og inngå avtale uten at de behandlingsansvarlige har brukt mye tid eller ressurser på prosjektet. Ved å overlate ansvar til Sykehuspartner i prosessen har de dermed oppnådd en ressursbesparelse. Slik ressursbesparelse er mest sannsynlig også noe av begrunnelsen for å gjennomføre konsernovergripende anskaffelser. Da blir det problematisk at man ikke samtidig sikrer nødvendig forankring i spørsmål som krever det.

Overtredelsene har i større grad fremmet interessene til det regionale helseforetaket, siden det er RHFet som har lagt føringer for gjennomføringen uten å ta høyde for regelverkets krav om ledelsesforankring.

Ønsket om effektiv prosjektledelse, samordning og ressursbesparelser har vært styrende for hvordan prosjektet er gjennomført og dette har gått på bekostning av helseforetakenes plikt til å sikre etterlevelse av regelverket.

Målet for prosjektet har vært modernisering og effektivisering til lavest mulig kostnad.
Det er uklart om resultatet vill blitt annerledes dersom overtredelsene ikke hadde funnet sted, men det er grunnlag for å si at manglende risikovurderinger og forankring av disse kan ha bidratt til et resultat som oppfyller helseforetakenes plikt til å sikre effektivitet og tilgjengelighet på bekostning av personvernkonsekvenser.

7.2.5 Har de behandlingsansvarlige oppnådd en fordel ved overtredelsen? Vurdering av §29 e)

Vurderingen av om de behandlingsansvarlige har oppnådd en fordel ved overtredelsene sammenfaller i stor grad med vurderingen av om overtredelsen har fremmet de behandlingsansvarliges interesser.

7.2.6 Foreligger gjentakelse? Vurdering av §29 f)

Saken er enestående i den forstand at det er første gang en samlet helseregion har besluttet å tjenesteutsette drift og vedlikehold av hele IKT-infrastruktur til en ekstern leverandør i utlandet.

Saken er også spesiell fordi den løfter en rekke problemstillinger som oppstår som følge av organisasjonsstrukturen i helseforetaksmodellen.

Det foreligger ikke gjentakelse, men saken belyser en rekke problemstillinger som også vil gjelde for en rekke andre prosjekter som vurderer tjenesteutsetting av IKT-tjenester i helsesektoren.

7.2.7 Andre reaksjoner? Vurdering av §29 g)

Saken er behørig omtalt i media og den har fått konsekvenser internt i konsernet blant annet ved at styret i Sykehuspartner er skiftet ut. Saken har medført reaksjoner i den forstand at prosjektet er midlertidig stanset i påvente av nye vurderinger internt i konsernet. Da saken ble offentlig kjent fikk dette konsekvenser i den forstand at Helse Sør-Øst RHF har igangsatt revisjon, samt pålagt Sykehuspartner å gjennomføre tiltak for å vurdere risiko og sårbarhet samt å sikre forankring i helseforetakene.

Vår vurdering er at offentlig omtale av saken har bidratt til å begrense konsekvensene av de feil som er begått ved at Helse Sør-Øst har stanset fremdriften av prosjektet.

Vår vurdering er at Helse Sør-Øst gjennom sine reaksjoner har erkjent at avvik har skjedd og at de har iverksatt tiltak for å avhjelpe situasjonen.

Datatilsynet har etter dette kommet til at overtredelsesgebyr bør ilegges.

7.3 Vurdering av gebyrets størrelse

Vi kan ilegge gebyr på inntil 10 ganger folketrygdens grunnbeløp, for tiden maksimalt 936.340,- NOK. Datatilsynet har per i dag ikke gitt overtredelsesgebyr i denne størrelsen. Vi har heller ikke behandlet saker som kan sammenliknes med denne når det gjelder kontraktens størrelse, opplysningenes sensitivitet, omfanget av registrerte eller virksomhetens art.

Ved vurdering av beløpets størrelse skal det gjøres en konkret vurdering der de samme momentene som nevnt over skal avveies i tillegg til den behandlingsansvarliges økonomiske bæreevne.

Som vist i drøftelsen av om overtredelsgebyr skal ilegges mener vi at overtredelsene er svært alvorlige og at etterlevelse av de bestemmelsene som her er overtrådt er helt avgjørende for å sikre at de behandlingsansvarlige etterlever sine plikter til å sikre forsvarlig behandling av personopplysninger og sørge for at personvern ivaretas, samtidig som det utvikles nye løsninger der moderne teknologi tas i bruk.

Kontraktens verdi tilsier at det legges store ressurser i å nå målet om effektivisering og modernisering. I denne sammenhengen forsterkes alvoret av overtredelsene fordi det blir så tydelig at grunnleggende krav til vurdering av restrisiko, ansvarlighet og kontroll ikke er hensyntatt i en ellers så viktig og ressurskrevende kontraktsinngåelse.

Helseforetakene er profesjonelle aktører som bærer et betydelig ansvar for å sikre ivaretakelse av befolkningens personvern. Dette ansvaret kan aldri overføres til en databehandler eller til en annen virksomhet.

Avtalen som er inngått har en verdi på NOK 6.9 milliarder over en periode på 7 år. Vi legger til grunn at helseforetakenes økonomiske bæreevne er solid og at et overtredelsesgebyr i den størrelsesorden vi maksimalt kan gi først og fremst vil ha en viktig signaleffekt. Signaleffekten er viktig for å synliggjøre at det ikke aksepteres at helseforetakene i landets største helseregion unnlater å sørge for ansvarlighet og veloverveide beslutninger i saker som har stor betydning for personvern og informasjonssikkerhet i helsetjenesten.

Herværende sak skiller seg fra tidligere saker der vi har ilagt overtredelsesgebyr ved at omfanget av opplysninger som behandles tilsvarer halve Norges befolkning i tillegg til at det dreier seg om helseopplysninger, altså svært sensitive opplysninger. Tilliten til helsetjenesten er og må være stor. Befolkningen skal ha tillit til at opplysninger behandles på en trygg måte og tilsynsorganer skal ha tillit til at de behandlingsansvarlige ser det som en egeninteresse å etterleve regelverket for å sikre pasientenes personvern.

Vår vurdering er at det ikke finnes formildende omstendighet i denne saken. Det er positivt at tilgangene som ble gitt i et avgrenset tidsrom er stanset, at prosjektets fremdrift er satt på vent og at Helse Sør-Øst har tatt grep for å rette opp i de feil som er begått. Dette innebærer at overtredelsene ikke har fått de konsekvensene som de kunne fått dersom prosjektet hadde fortsatt som planlagt med full drift fra 1. mai 2017.

Hva som er årsaken til at prosjektet ble stanset vet vi ikke. Det kan være medias søkelys på saken. Basert på dokumentasjon vi har mottatt og henvendelser vi har fått, mener vi det er klart at prosjektet ikke ble stanset som følge av interne prosesser. Selv om det er positivt at prosjektet ble stanset, er vår vurdering at dette først og fremst uttrykker RHFets erkjennelse av alvorlige avvik som ikke skulle funnet sted.

8 Orientering om videre fremdrift

Dette er et forhåndsvarsel (jf. forvaltningsloven § 16). Dersom dere har merknader til dette varselet, må dere sende oss en tilbakemelding om dette så snart som mulig og senest innen **24. november 2017.**

9 Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3), men understreker samtidig at sikkerhetsdokumentasjon som hovedregel er unntatt offentlighet (jf. offentlighetsloven § 13, jf. personopplysningsloven § 45).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Grete Alhaug
seniorrådgiver

Kopi: Helse Sør-Øst RHF, Postboks 404, 2303 HAMAR
Sykehuspartner HF, Postboks 3562, 3007 DRAMMEN