Datatilsynet

ST. OLAVS HOSPITAL HF
Postboks 3250 Torgarden
7006 TRONDHEIM

Deres referanse	Vår referanse	Dato
2020/16384 2	20/01813-4	20.09.2021

Vedtak om overtredelsesgebyr

Datatilsynet viser til tre avviksmeldinger fra St. Olavs hospital HF mottatt den 10.03.2020. Avvikene knytter seg til manglende skjerming av personopplysninger.

Den 20.11.2020 ble St. Olavs hospital HF varslet om mulig vedtak om overtredelsesgebyr og pålegg. Foretaket har kommentert varselet i brev med vedlegg av 15.12.2020.

Vi beklager den lange saksbehandlingstiden.

1. Vedtak om overtredelsesgebyr

Datatilsynet har i dag fattet følgende vedtak:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 og pasientjournalloven § 29, ilegges St. Olavs hospital HF et overtredelsesgebyr på 750 000 NOK – syv hundre og femti tusen norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og artikkel 24, jf. personopplysningsloven § 26 første ledd, og pasientjournalloven §§ 22 og 23.*

2. Beskrivelse av avviksmeldingene

2.1 Avviksmelding 1

Avviket forekom i perioden 13.01.2011 til 27.01.2020 og ble oppdaget den 21.11.2019.

I avviksmeldingen fremgår det at avviket oppsto ved hjertemedisinsk avdeling. Ca. 21 000 rapporter (pdf-filer) hadde blitt lagret i mapper på testserver.

Rapportene hadde følgende innhold:

- anamnese (pasientens egen redegjørelse)
- utførte prosedyrer
- hemodynamisk trykk
- koronar arteriografi

- utstyrssammendrag
- komplikasjoner
- medisinering under prosedyre
- hemo-bilder
- navn på utførende lege og sykepleier

Avviket oppsto i forbindelse med oppgradering til nytt behandlingsrettet helseregister for hjertemedisinsk laboratorium. I forbindelse med konvertering av rapporter fra det utgående systemet til det nye systemet ble det benyttet en testserver. Da rapportene var ferdig konvertert, ble de lagt i en mappe på serveren som skulle være midlertidig frem til rapportene var kopiert over til nytt system. Rapportene i mappen har likevel ikke blitt slettet. I tillegg ble det gjort en feil slik at alle autentiserte brukere fikk tilgang til mappen.

Mappen har ikke blitt distribuert ut, men man har aktivt kunnet søke opp filene. Potensielt har alle autentiserte brukere i Helse Midt-Norge RHF kunnet gå inn og lese og/eller kopiere innholdet i mappen uten at dette har blitt logget. Omfanget av pasienter som potensielt er rammet er stort, og sykehuset har ingen logger som kan si noe om hvorvidt noen har vært inne i filene.

Rapportfilene er nå slettet. Sykehuset har gjennomgått de systemene som er i bruk i dag og som har delte mapper. Tilgangsstyringen til mappene er gjennomgått og kontrollert, slik at kun de med tjenstlige behov har tilgang.

2.2 Avviksmelding 2

Avviket forekom i perioden 17.05.2015 til 28.01.2020 og ble oppdaget den 21.11.2019.

I avviksmeldingen fremgår det at rapporter fra medisinsk utstyr (pulsoksymeter for langtidsmåling av oksygenmetning og puls) har blitt lagret på et filområde som har vært tilgjengelig for alle i Helse Midt-Norge RHF med autentisert og aktiv AD-bruker. Oppkobling via Remote Desktop har ikke vært aktivt tilgjengeliggjort, men alle med kunnskap til det har kunnet prøve oppkobling mot serveren og søke opp mappen. Det finnes ikke logg som kan gi informasjon om hvorvidt noen har benyttet seg av tilgangen. Sykehuset opplyser at rutinene for tilgangsstyring ikke er fulgt.

Rapportene har følgende innhold:

- fornavn og etternavn
- personnummer
- dato for måling
- graf og tabell som viser puls og oksygenmetning

Rapportene ligger i dag på samme område, men området er blitt tilgangsstyrt. Videre er det utført revisjon av tilganger til mapper for lagring av rapporter fra medisinsk utstyr, og det er kontrollert at kun de med tjenstlig behov har tilgang.

Sykehuset har planlagt å ta i bruk en teknisk løsning som automatisk importerer rapportene til pasientens hovedjournal og så sletter rapporten fra mappeområdet.

2.3 Avviksmelding 3

Avviket forekom i perioden 01.01.2018 til 09.12.2019 og ble oppdaget den 21.11.2019.

I avviksmeldingen fremgår det at passord til databaser lå i klartekst i fil på server. Aktive brukere i Helse Midt-Norge RHFs infrastruktur har hatt mulighet til å koble seg opp, først via Remote Desktop mot server for så å lete opp fil med passord til databasen. Tilgangen til server er nå begrenset til kun de som har tjenstlig behov. Etter gjennomgang av databaselogger er det ingen indikasjoner på at noen har benyttet brukernavn/passord til å logge på databasene.

Det fremgår at avviket omfatter helse- og personopplysninger om personer behandlet på RUS- og BUP-klinikken, der detaljer om behandlingsforløp fremkommer.

St. Olavs hospital HF har skissert følgende tiltak for de to omtalte databasene:

- Tilgang til Bupdata-applikasjonen er begrenset til et gitt antall brukere (innmeldt av BUP-ene), i henhold til delegeringsmodell.
- Tilgang til Bup-databaser er begrenset til administrative brukere som har ansvar forbundet med systemet (også i henhold til delegeringsmodellen).
- Tilgang til Rusdata-applikasjonen er begrenset til et gitt antall brukere (innmeldt av klinikkene), i henhold til delegeringsmodell.
- Tilgang til serverpålogging via Remote Desktop er nå styrt av delegeringsmodell. Kun administratorbrukere som trenger tilgang i forbindelse med drift og konvertering har tilgang.

3. Redegjørelse fra St. Olavs hospital HF

I forbindelse med varselet om vedtak datert 20.11.2020, stilte vi St. Olavs hospital HF flere spørsmål knyttet til sykehusets rutiner:

- Hvilke rutiner for tilgangsstyring hadde St. Olavs hospital HF på tidspunktet da avvikene ble oppdaget, og hvilke rutiner har sykehuset i dag?
- Hadde St. Olavs hospital HF en behandlingsprotokoll på tidspunktet da avviket ble oppdaget? Vi ber i tilfelle om at protokollen oversendes. Vi ønsker også oversendt oppdatert behandlingsprotokoll per i dag.
- Det fremgår av avviksmeldingene at avvikene ble oppdaget i november 2019, mens de først ble meldt til Datatilsynet i mars 2020. Vi ber om sykehusets kommentar til dette.
- Det fremgår av avviksmeldingene at to av avvikene vedvarte til slutten av januar 2020, det vil si drøyt to måneder etter at de ble oppdaget. Vi ber om sykehusets kommentar til dette.

I svarbrevet datert 15.12.2020 har sykehuset redegjort for forholdene. Vedlagt brevet fulgte kopi av St. Olavs hospital HFs skriftlige rutiner/prosedyrer.

Når det gjelder rutinene for tilgangsstyring, har sykehuset knyttet svaret til tilgangsstyring for opprettelse av filområder for lagring av opplysninger til forskning, kvalitetssikring eller studentprosjekter. Vedlagt fulgte rutinene for informasjonssikkerhet for forsknings- og

studentprosjekter som gjaldt fra henholdsvis oktober 2015 til mai 2020 og fra mai 2020. Vi forstår det slik at St. Olavs hospital HF ikke har hatt egne rutiner for tilgangsstyring av kvalitetssikringsdata.

Videre fremgår det at St. Olavs hospital HF kom sent i gang med arbeidet med å etablere en behandlingsprotokoll i tråd med personvernforordningen artikkel 30. På tidspunktet for avviket, hadde sykehuset ikke samlet oversikt over all behandling av personopplysninger. Sykehuset bruker nå Normens[1] mal for protokoll, som skal benyttes på klinikknivå.

Når det gjelder forsinkelsen i meldingen av avvik til Datatilsynet og at avvikene vedvarte en tid etter at de ble oppdaget, viser sykehuset til at avvikene ble avdekket i forbindelse med Riksrevisjonens kontroll av helseforetakenes forebygging av angrep mot sine IKT-systemer. Riksrevisjonen avla en rapport etter kontrollen. St. Olavs hospital HF måtte sammen med Helse Midt-Norge IKT analysere rapporten for å identifisere hvilke avvik som eventuelt forelå og var meldingspliktige.

Etter Riksrevisjonens kontroll utarbeidet sykehuset en prioritert tiltaksplan, og flere tekniske sikkerhetstiltak ble iverksatt av Helse Midt-Norge IKT. Blant annet innførte sykehuset ny passordrutine, begrensning av tillatt antall mislykkede påloggingsforsøk, system for overvåking og logganalyse, reduksjon av antall brukere og opprydning i brukertilganger samt sikring av informasjonsdeling i systemer der dette ikke var tilstrekkelig innebygd.

4. Rettslig grunnlag for vurderingen

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personopplysnings-loven § 20 og personvernforordningen artikkel 57.

Vi er også tilsynsmyndighet etter pasientjournalloven, jf. lovens § 26. Pasientjournalloven gjelder for all behandling av helseopplysninger som er nødvendig for blant annet å yte og kvalitetssikre helsehjelp til enkeltpersoner, jf. lovens § 3.

4.1 Om lovvalg

Den nye personopplysningsloven, som inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20.07.2018. Loven opphevet samtidig personopplysningsloven (2000) og reglene i personopplysningsforskriften (2000).

Denne saken gjelder forhold som oppsto i 2015, altså før ikrafttredelsen av personopplysningsloven (2018), men som har vedvart i tiden etterpå. Vi må derfor ta stilling til om saken skal vurderes etter personopplysningsloven (2018) eller personopplysningsloven (2000).

I personopplysningsloven (2018) § 33 første ledd finnes en særskilt overgangsregel om overtredelsesgebyr, som lyder:

[1] https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

> «Reglene om behandling av personopplysninger som gjaldt på handlingstidspunktet, skal legges til grunn når det treffes vedtak om overtredelsesgebyr. Lovgivningen på tidspunktet for avgjørelsen skal likevel anvendes når dette fører til et gunstigere resultat for den ansvarlige».

Spørsmålet om lovvalg må altså vurderes ut fra hva som regnes som handlingstidspunktet.

Det aktuelle avviket oppsto før ikrafttredelsen av nytt regelverk den 20.07.2018, men vedvarte frem til avviket ble oppdaget i januar 2019. Handlingstidspunktet i denne saken har altså vedvart over tid og i tiden etter at personopplysningsloven (2018) trådte i kraft. Det følger da av personopplysningsloven (2018) § 33 at saken skal vurderes etter denne loven.

Vi viser også til forarbeidene til personopplysningsloven (2018), Prop. 56 LS (2017-2018) side 196, hvor departementet blant annet uttaler følgende om spørsmålet om lovvalg mellom personopplysningsloven (2000) og personopplysningsloven (2018):

> «Utgangspunktet vil være at vedtak hos Datatilsynet og Personvernnemnda vil måtte fattes på grunnlag av de til enhver tid gjeldende materielle regler».

Det samme følger av Personvernnemndas praksis i saker som ble oversendt nemnda før ny lov trådte i kraft, men som ble behandlet etter ikrafttredelsen; se for eksempel PVN-2018-05 og PVN-2018-06.

På denne bakgrunn er det etter vår vurdering klart at saken må vurderes etter personopplysningsloven (2018) og personvernforordningen.

4.2 Grunnprinsippene for behandling av personopplysninger

De grunnleggende prinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. Vi viser særlig til artikkel 5 nr. 1 bokstav f, hvor det fremgår:

> «1. Personopplysninger skal (…)
> f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling (…), ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».

Det er den dataansvarliges ansvar at prinsippene overholdes, og den dataansvarlige skal kunne påvise dette, jf. artikkel 5 nr. 2.

Helseopplysninger er en såkalt særlig kategori av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1. Helseopplysninger der barn er pasienter må regnes som særlig sensitive, ettersom barn har særskilt krav på vern etter personvernregelverket. [2]

[2] Se fortalepunkt 38 til personvernforordningen.

4.3 Kravene til personopplysningssikkerhet og styringssystemer

4.3.1 Personvernforordningen

Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32:

> «1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av 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 med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet, (…)
>
> b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, (…)
>
> d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.
>
> 2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av (…) ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Plikten til å gjennomføre egnede tekniske og organisatoriske tiltak fremgår tilsvarende av personvernforordningen artikkel 24, som regulerer den dataansvarliges ansvar særskilt.

Etter personvernforordningen artikkel 30 nr. 1 har den dataansvarlige plikt til å føre protokoll over behandlingsaktivitetene som utføres. Protokollen skal blant annet inneholde en beskrivelse av kategoriene av personopplysninger som behandles, jf. artikkel 30 nr. 1 bokstav c, og kategoriene av mottakere som personopplysningene vil bli utlevert til, jf. artikkel 30 nr. 1 bokstav d.

4.3.2 Pasientjournalloven

Kravene til den dataansvarlige ved behandling av journalopplysninger fremgår også av pasientjournalloven.

Pasientjournalloven § 22 første ledd om informasjonssikkerhet lyder:

> «Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll.».

Pasientjournalloven § 23 om internkontroll lyder:

> «Den dataansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, personopplysningsloven og denne loven, jf. forordningen artikkel 24.

Den dataansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den dataansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.

Departementet kan i forskrift gi nærmere bestemmelser om internkontroll».

4.4 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 annet ledd, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i regelverket.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både når det vurderes hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyrets størrelse. De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

«1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.

2. (…) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,
e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,
f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
g) kategoriene av personopplysninger som er berørt av overtredelsen,
h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,
i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes,

j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelse. Vi viser i denne forbindelse til artikkel 83 nr. 4. De relevante delene av bestemmelsene lyder:

«Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro (…):
a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 samt 42 og 43».

5 Datatilsynets vurdering

I det følgende vil vi redegjøre for vår vurdering av hvordan ulike deler av personopplysningssikkerheten og personvernet er ivaretatt når det gjelder de tre avvikene ved St. Olavs hospital HF.

5.1 Tilgangsstyring

St. Olavs hospital HF har angitt at rutinene for tilgangsstyring ikke er fulgt i de tre avvikssakene. Som følge av dette har alle aktive/autoriserte brukere i Helse Midt-Norge RHF kunnet tilegne seg pasientopplysninger de ikke har hatt tjenstlig behov for. Dette tyder på at rutinene ikke har vært egnet til å fange opp den manglende tilgangsstyringen.

Datatilsynet legger til grunn at St. Olavs hospital HF ikke har hindret urettmessig tilgang til et omfattende antall helseopplysninger om pasienter ved sykehuset. Selv om opplysningene har vært lagret på et område det krever noe kunnskap å søke opp/finne frem til, har risikoen for brudd på opplysningenes konfidensialitet og integritet like fullt vært til stede.

Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 1 bokstav f, og pasientjournalloven § 22.

5.2 Logging

I to av avvikssakene har ikke St. Olavs hospital HF logget aktiviteten på fil-/mappeområdet. Det er dermed ikke mulig å bekrefte og/eller avkrefte om ansatte har benyttet seg av tilgangene. Dersom sykehuset hadde sørget for logging av aktiviteten og fulgt opp loggene på en systematisk måte, kunne sykehuset ha fulgt opp aktiviteten og avdekke uautorisert tilgang og eventuell kompromittering av pasientopplysningene. Den manglende loggingen øker risikoen for at man mister oversikt over hvor pasientopplysninger befinner seg.

Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 2, og pasientjournalloven § 23.

5.3 Samlet vurdering av avvikene

I november 2019 avdekket St. Olavs hospital HF tre ulike avvik der detaljerte pasientopplysninger har ligget tilgjengelig for ansatte uten tjenstlig behov. Avvikene har vedvart gjennom flere år (fra ca. to til ca. ni år).

Selv om det konkrete antallet er ukjent, er et stort antall pasienter berørt, ettersom avviket fra hjertemedisinsk avdeling alene gjelder ca. 21 000 rapporter. Videre gjelder ett avvik opplysninger om rusbehandling og behandling i barne- og ungdomspsykiatrien. Dette er helseopplysninger som oftest oppfattes som særlig sensitive. Vi viser også til at barn har et særlig krav på vern etter personvernregelverket. Dette gjør avviket alvorlig.

Ettersom alle aktive/autoriserte brukere i Helse Midt-Norge RHF potensielt har kunnet gjøre oppslag, legger vi til grunn at det også er tale om et stort antall ansatte som har hatt urettmessig tilgang.

Logg finnes ikke for to av avvikene, og det er dermed ikke mulig å avdekke hvorvidt urettmessige oppslag er gjort. Dette gjør det vanskelig å bedømme konsekvensene av avviket for de som er berørt.

Sykehuset har gjennomgått de systemene som er i bruk i dag og som har delte mapper. Det er nå kontrollert at kun ansatte med tjenstlig behov har tilgang. Gjennomgang av tilgangsstyringen er et av tiltakene St. Olavs hospital HF har iverksatt i samarbeid med Helse Midt-Norge IKT. Datatilsynet ser positivt på at avvikene er rettet opp og at systemet for deling av mapper er gjennomgått.

Vi legger også til grunn at St. Olavs hospital HF har innført ytterligere internkontroll- og sikkerhetstiltak som ny passordrutine og begrensning av tillatt antall mislykkede påloggingsforsøk, system for overvåking og logganalyse.

Videre fremgår det at sykehuset nå har utarbeidet en behandlingsprotokoll i tråd med kravet i personvernforordningen artikkel 30.

Samlet sett ser Datatilsynet positivt på de iverksatte tiltakene og arbeidet St. Olavs hospital HF har gjort med å rette opp i avvikene i etterkant.

Dette endrer likevel ikke vår konklusjon om at sykehuset har brutt grunnleggende krav til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. artikkel 24 og 5, og pasientjournalloven §§ 22 og 23.

5.4 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at St. Olavs hospital HF har brutt personvernforordningen artikkel 32, jf. artikkel 24 og 5, og pasientjournalloven §§ 22 og 23.

Lovbruddet har for en stor del skjedd før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Datatilsynet kunne også tidligere ilegge

overtredelsesgebyr, jf. personopplysningsloven (2000) § 46, men beløpet var da begrenset til inntil 10 ganger folketrygdens grunnbeløp (p.t. ca. 1 010 000 NOK).

Vi viser imidlertid til drøftelsen under punkt 3.1 og legger til grunn at gebyret skal utmåles etter nytt regelverk. I utgangspunktet er det dermed grunnlag for å ilegge St. Olavs hospital HF et overtredelsesgebyr på inntil 10 000 000 euro (p.t. ca. 106 000 000 NOK), jf. personvernforordningen artikkel 83 nr. 4. Vi vil likevel se hen til at lovbruddene har skjedd også i perioden da tidligere personvernregelverk gjaldt.

Under gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges.

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd
Alle avvikene har vedvart over flere år uten at de ble avdekket. Helseopplysninger om et stort antall pasienter er berørt; ca. 21 000 rapporter fra hjertemedisinsk avdeling alene er omfattet. Videre har opplysningene ligget tilgjengelig for alle aktive/autoriserte brukere i Helse Midt-Norge RHF. For to av avvikene finnes det ikke logg, slik at det ikke er mulig å avdekke hvorvidt ansatte har gjort urettmessig innsyn i opplysningene og/eller om pasientopplysninger har kommet på avveie.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt
St. Olavs hospital HF har opplyst at rutinene for tilgangsstyring er brutt i forbindelse med avvikene. Vi anser lovbruddet som uaktsomt. Administrerende direktør vil, som sykehusets øverste leder, være ansvarlig for det uaktsomme lovbruddet, jf. også ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd
St. Olavs hospital HF har gjort tiltak i forbindelse med de tre avvikene, slik at opplysningene ikke lenger ligger tilgjengelig for ansatte uten tjenstlige behov.

Sykehuset har også igangsatt flere sikkerhetstiltak knyttet til passord og pålogging, fildeling, overvåking og logganalyse.

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32
St. Olavs hospital HF har angitt at rutinene for tilgangsstyring er brutt. Vi har merket oss at alle avvikene gjelder lagring av pasienters helseopplysninger utenfor pasientjournal. Rutinene har dermed ikke vært egnet til å fange opp avvik ved denne typen lagring.

Vi forutsetter at sykehusets arbeid med å rette avvikene har rettet seg mot lagring av helseopplysninger utenfor pasientjournal, til bruk for kvalitetssikring.

g) kategoriene av personopplysninger som er berørt av overtredelsen
Helseopplysninger vært tilgjengelige for et stort antall ansatte uten tjenstlig behov. Etter personvernforordningen artikkel 9 nr. 1 er helseopplysninger betegnet som en særlig kategori personopplysninger, det vil opplysninger med særskilt krav på vern. Opplysningene har også knyttet seg til barne- og ungdomspsykiatrien. Dette øker alvorlighetsgraden av lovbruddet.

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen
St. Olavs hospital HF meldte selv fra til Datatilsynet om avvikene etter at sykehuset hadde kartlagt at avvikene var meldepliktige.

5.5 Vurdering av overtredelsesgebyrets størrelse
I vurderingen av gebyrets størrelse, har vi vektlagt at St. Olavs hospital HF har iverksatt tiltak for å sørge for at delte mapper kun er tilgjengelige for ansatte med tjenstlig behov. Sykehuset har også gjort et større arbeid for å innføre flere relevante tiltak for å bedre personopplysningssikkerheten.

Vi har også sett hen til at sykehuset selv meldte avviket til Datatilsynet, selv om avvikene først ble oppdaget etter en ekstern kontroll fra Riksrevisjonen.

Det er ikke kjent at avvikssakene har fått konkrete konsekvenser for enkeltpasienter, selv om dette tillegges mindre vekt.

Vi har vektlagt at lovbruddet dels har funnet sted før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Etter tidligere gjeldende personopplysningslov (2000) var gebyret avgrenset til maksimalt ca. 1 010 000 NOK.

I denne saken har en større mengde helseopplysninger har ligget tilgjengelig for alle aktive/autoriserte brukere i Helse Midt-Norge HF gjennom flere år. St. Olavs hospitals HFs rutiner for tilgangsstyring har ikke vært egnet til å fange opp de aktuelle avvikene, som alle gjelder lagring av helseopplysninger utenfor pasientjournal.

Datatilsynet har kommet til at et overtredelsesgebyr på 750 000 NOK er rimelig i denne saken.

6 Klageadgang
Vedtaket om overtredelsesgebyr kan påklages innen tre uker etter at dere mottar dette brevet, jf. forvaltningsloven §§ 28 og 29.

Dersom vi opprettholder vårt vedtak etter en eventuell klage, vil saken bli oversendt til Personvernnemnda for avgjørelse, jf. personopplysningsloven § 22.

Ved eventuelle spørsmål kan dere ta kontakt med saksbehandler Susanne Lie (tlf. 22 39 69 57, e-post suli@datatilsynet.no).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: ST. OLAVS HOSPITAL HF, Stein Gilde