Datatilsynet

OSLO KOMMUNE SYKEHJEMSETATEN
Postboks 435
0103 OSLO

Deres referanse	Vår referanse	Dato
AR287711144	18/03623-7/SLI	11.10.2019

Vedtak om overtredelsesgebyr - Melding om avvik i Oslo kommune Sykehjemsetaten

Vi viser til vårt varsel av 05.04.2019 om vedtak om overtredelsesgebyr. Datatilsynet viser også til Sykehjemsetatens svar datert 20.05.2019, hvor dere besvarte spørsmål knyttet til årsaken til avviket, avvikets omfang, konsekvenser av avviket, tiltak fra kommunens side og informasjon til de registrerte.

Datatilsynet har vedtatt å gi Oslo kommune et overtredelsesgebyr med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven (2018) § 26 andre ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven (2018) § 26 andre ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83, pålegges Oslo kommune å betale et overtredelsesgebyr på 500 000 NOK – norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og pasientjournalloven §§ 22 og 23.*

Bakgrunnen og begrunnelsen for vedtaket følger under.

1. Saksforholdet

Datatilsynet mottok 08.11.2018 en melding om avvik fra Sykehjemsetaten i Oslo kommune. Avviksmeldingen beskrev en praksis med bruk av såkalte arbeidslister som ble benyttet ved siden av/i tillegg til pasientjournalsystemet på sykehjem og helsehus underlagt Sykehjemsetaten.

Arbeidslistene var et hjelpemiddel for de ansatte som ga oversikt over den mest nødvendige informasjonen om den enkelte beboer ved institusjonene.

1.1 Nærmere om arbeidslistene

Det antas at praksisen med arbeidslister har eksistert siden før Sykehjemsetaten ble opprettet i 2007. Det er derfor uklart hvor mange pasienter som har vært berørt. Sykehjem har i tiden siden 2007 blitt opprettet og lagt ned, og antall beboere på hvert sykehjem har til enhver tid

variert. Eksempeltall fra 2018/2019 viser at Sykehjemsetaten hadde 19 kommunale institusjoner som alle hadde slike arbeidslister. I tillegg har ni private helseinstitusjoner meldt at de har hatt samme praksis. Hver institusjon har fra 150 til 390 ansatte, og det er mellom 32 og 163 beboere per institusjon, til sammen ca. 2 200 beboere. For ca. 600 av disse beboerne har arbeidslistene kun vært lagret på ledelsens fellesområde.

De ansatte brukte listene for å kunne utføre arbeidet på en effektiv måte uten å måtte bruke tid på å gjøre oppslag i journalen. Arbeidslistene i de ulike institusjonene inneholdt ulik informasjon. Listene ga oversikt over stellerutiner og daglige gjøremål, og enkelte steder var i tillegg diagnose og andre helseopplysninger oppgitt. Noen har kun brukt romnummer eller initialer på pasientene, mens andre har brukt fullt navn.

Oslo kommune har en felles IKT-plattform der hver virksomhet har sine egne lagringsområder i en intern og en sikker sone. Arbeidslistene har blitt utarbeidet i Word og lagret på den enkelte institusjons fellesområde i intern (ikke sikker) sone. Sykehjemsetatens ansatte har tilgang til alle institusjonenes internområder. I tillegg har de ansatte ved den enkelte institusjon tilgang der de jobber. Ni private sykehjem med avtale med Oslo kommune har hatt tilsvarende praksis, der arbeidslistene har blitt lagret på den private institusjonens interne lagringsområde.

Tilgang til arbeidslistene forutsatte en aktiv handling fra brukere i systemet ved at de måtte gå inn på et tilgangsstyrt fellesområde, men listene var tilgjengelige for de som måtte ønske å gjøre oppslag. Selv om den enkelte ansatte kun har hatt tilgang til opplysninger om beboere ved institusjonen der de jobber, har de likevel hatt tilgang til informasjon som de ikke har hatt tjenstlig behov for, for eksempel opplysninger om beboere ved en annen avdeling.

Ettersom opplysningene befant seg utenfor sikker sone, finnes det ikke logg over hvem som har gjort oppslag. Det er dermed ikke mulig å finne ut om, og eventuelt i hvilken grad, opplysningene har blitt lest av eller videreformidlet til uvedkommende.

I motsetning til praksisen ved sykehjemmene og helsehusene, har mobile verktøy (nettbrett) med sikker tilgang til arbeidslister direkte via journalsystemet (Gerica) vært utbredt i hjemmetjenesten. Dette systemet (eRom) har vært under utrulling siden 2015.

1.2 Om Sykehjemsetatens rutiner

Oslo kommune har opplyst at Sykehjemsetaten i lengre tid har hatt fokus på kompetanseheving, informasjonssikkerhet og opplæring i dokumentasjon i journalsystemet, særlig etter at personvernforordningen trådte i kraft i juli 2018. Lagring av informasjon utenfor journalsystemet har ikke vært et tema, ettersom det ikke har vært fanget opp som et risikoområde. Risikoanalysene som har vært gjennomført, har hatt fokus på journalsystemet.

Sykehjemsetaten er underlagt Instruks for informasjonssikkerhet i Oslo kommune fra 2013 og Instruks for virksomhetsstyring i Oslo kommune fra 2015. Instruksene gir overordnede og generelle føringer for krav til informasjonssikkerhet og ledelsens oppfølging.

1.3 Om konsekvensene av avviket
Sykehjemsetaten angir at praksisen med oppdaterte arbeidslister har innebåret at listene løpende har blitt overskrevet, og i arbeidslistene skal det til enhver tid kun ha vært tilgjengelig opplysninger om nåværende beboere. Det angis at opplysninger om tidligere pasienter ikke har vært lagret der. Ansatte som har jobbet lenge ved en institusjon, har likevel hatt tilgang til opplysninger om et høyt antall pasienter.

Det er opplyst at ca. 90 % av de ansatte ved sykehjemmene/helsehusene er helsepersonell som er bundet av helsepersonells taushetsplikt samt forbudet mot urettmessig tilegnelse av taushetsbelagt informasjon. De resterende 10 % (vaktmestere, renholdere m.v.) har undertegnet taushetserklæring og har i tillegg begrenset tilgang til PC i arbeidet. Vedlagt redegjørelsen fulgte kopi av taushetserklæringen som benyttes.

Sykehjemsetaten er ikke kjent med at ansatte uberettiget har benyttet seg av tilgangene eller at taushetsbelagt informasjon fra arbeidslistene har kommet på avveie. Etaten vurderer at det på bakgrunn av taushetsplikten er lav risiko for at ansatte har spredd informasjon videre.

En konsekvens av den avvikende praksisen er at helseopplysninger har vært tilgjengelige for personer som ikke har hatt tjenstlig behov for informasjonen. Enkelte vil kunne oppleve det som en belastning i seg selv at uvedkommende ansatte har hatt tilgang til informasjon om dem. Mest alvorlig er muligheten for at svært sensitive opplysninger kan ha blitt spredd til utenforstående. Dette vil oftest kunne være en stor belastning for den det gjelder.

1.4 Om iverksatte og planlagte tiltak
Etter at avviket ble oppdaget, fikk alle institusjonssjefene e-post med klar beskjed om at ulovlig praksis for lagring av personopplysninger måtte opphøre umiddelbart. Arbeidslistene ble raskt slettet fra lagringsområdene. Backup foreligger som tape backup, og disse lagres med samme sikkerhetsnivå som for andre backupfiler i kommunen. Kun et lite antall ansatte hos driftsleverandøren og internleverandøren har tilgang til filene.

I etterkant av at avviket ble oppdaget, har temaet informasjonssikkerhet vært oppe i ledermøtet i Sykehjemsetaten, hvor institusjonssjefene deltar. Internrevisjon knyttet til praksis med arbeidslister på institusjonene er del av Sykehjemsetatens revisjonsplan for 2019. Sykehjemsetaten har også utarbeidet et årshjul som skal sikre oppfølging av risikoanalyser, leverandører, behandling av personopplysninger/personvernkonsekvensvurderinger, tilgangsstyring, kompetanseplan og ledelsens gjennomgang. Det vil bli ansatt en person for å håndtere personvernområdet i etaten.

Sykehjemsetaten ser behov for ytterligere kompetanseheving hos alle ansatte, og det arbeides med en helhetlig kompetanseplan der sikker informasjonshåndtering og melding av avvik vil inngå. Det har blitt sendt ut e-læringsmateriell til de ansatte, og enkelte kurs er avholdt. Videre har utrullingen av eRom til helsehusene blitt fremskyndet, ettersom disse institusjonene har opplevd praksisendringen som mest problematisk.

1.5 Om informasjon til de registrerte

Sykehjemsetaten antar at flertallet av de berørte beboerne ikke lenger er i live. Av eventuelle gjenlevende, vil en stor andel ha betydelig kognitiv svikt. Arbeidslistene er slettet, og den enkelte kan dermed ikke få innsyn i hvilke opplysninger som var lagret der. Videre antar Sykehjemsetaten at informasjon om avviket er egnet til å skape usikkerhet snarere enn å hjelpe den enkelte til å ivareta sine rettigheter. Dette ville stilt seg annerledes dersom man var kjent med konkrete tilfeller der informasjon var kommet på avveie.

2. Datatilsynets kommentarer til Sykehjemsetatens uttalelse

Datatilsynet legger til grunn at arbeidslistene i dag er slettet og at backup-filene er lagret med et sikkerhetsnivå som tilfredsstiller kravene i personopplysningsloven og personvernforordningen. Risikoen for videre brudd på kravene til informasjonssikkerhet knyttet til arbeidslistene, anses derfor tilstrekkelig minimert.

Når det gjelder Oslo kommunes instrukser som Sykehjemsetaten er underlagt, er disse helt overordnede, og de er skisserer ikke konkrete systemer og tiltak tilpasset den enkelte etats behov. Vi påpeker at gode risikovurderinger og løpende oppfølging av behandlingen av personopplysninger er sentralt for å ivareta informasjonssikkerheten lokalt.

Datatilsynet tar til etterretning at Sykehjemsetaten arbeider med en plan for heving av de ansattes kompetanse, en ny strategi for oppfølging fra ledelsens side samt gjennomføring av en internrevisjon i løpet av inneværende år. Vi forutsetter at disse tiltakene videreutvikles og implementeres, i tillegg til at etaten må følge opp at tiltakene fungerer som planlagt.

Sykehjemsetaten har fremhevet helsepersonells individuelle plikt til å ha et bevisst forhold til håndtering av sensitiv informasjon. Helsepersonells taushetsplikt er et viktig element i personvernet, men vi vil for ordens skyld påpeke at denne individuelle plikten ikke påvirker virksomhetens ansvar for å ha sikre informasjonssystemer og god tilgangsstyring. Dette gjelder ikke minst ved håndtering av svært sensitive opplysninger, som helseopplysninger.

Man er ikke kjent med at ansatte uberettiget har benyttet seg av tilgangene eller at taushetsbelagt informasjon har kommet på avveie. Dette kan vi imidlertid kun tillegge begrenset vekt, ettersom det ikke er mulig å ettergå om urettmessig innsyn eller spredning av taushetsbelagte opplysninger har forekommet.

Etter personvernforordningen artikkel 34, har den behandlingsansvarlige ved enkelte tilfeller av brudd på personopplysningssikkerheten en plikt til å informere de registrerte. Det er antatt at alle de berørte pasientene i dag er døde, eventuelt har en grad av kognitiv svikt som gjøre dem ute av stand til å forstå situasjonen. I alle tilfeller er arbeidslistene slettet, slik at det ikke lar seg gjøre å finne ut med sikkerhet hvilke pasienter det er tale om.

Datatilsynet legger til grunn at Sykehjemsetaten ikke har noen praktisk mulighet til å informere pasientene om avviket. Etter vår vurdering har etaten som behandlingsansvarlig truffet etterfølgende tiltak som gjør at det ikke lenger er sannsynlig at det vil oppstå en høy risiko for de tidligere beboernes rettigheter og friheter, jf. personvernforordningen artikkel 34

nr. 3 bokstav b. Vi finner derfor at Sykehjemsetaten ikke har plikt til å informere de tidligere beboerne om bruddet på personopplysningssikkerheten.

Når det gjelder etatens taushetserklæring, påpeker vi at lovhenvisningene i denne i all hovedsak er utdaterte. Dette gjelder henvisningene til bestemmelser i straffeloven (1902), lov om sosiale tjenester, lov om godkjenning av helsepersonell, lov om godkjenning av sykepleiere, lov om fysioterapeuter og mensendiecksykegymnaster og lov om leger. Alle disse lovene er opphevede, eller bestemmelsene det vises til er videreført i endret form. Vi forutsetter at Sykehjemsetaten snarest oppdaterer taushetserklæringen i tråd med gjeldende regelverk.

3. Rettslig grunnlag for vurderingen

3.1 Om lovvalg

Den nye personopplysningsloven (2018), 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 før ikrafttredelsen av personopplysningsloven (2018), men som vedvarte minst frem til avviket ble oppdaget 05.11.2018. 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:

> «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 behandlingen av personopplysningene var brakt i samsvar med regelverket – i dette tilfellet frem til arbeidslistene ble slettet. Vi har ikke fått opplyst nøyaktig dato for sletting av arbeidslistene, men dette kunne tidligst skje da avviket ble oppdaget 05.11.2018. Ettersom handlingstidspunktet i denne saken vedvarte over tid og i tiden etter 20.07.2018 (da personopplysningsloven (2018) trådte i kraft), følger det av personopplysningsloven (2018) § 33 at saken skal vurderes etter personopplysningsloven (2018).

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.

Tilsvarende vil vi vurdere saken etter pasientjournalloven, som trådte i kraft 01.01.2015 og erstattet helseregisterloven (2001).

3.2 Om informasjonssikkerhet og behandlingsansvarliges ansvar

Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32 nr. 1:

> «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 (…)».

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

Kravene til den behandlingsansvarlige ved behandling av opplysninger i pasientjournal fremgår også av pasientjournalloven.

Pasientjournalloven § 22 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.
>
> Departementet kan i forskrift fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger.»

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.»

3.3 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven (2018) § 26 annet ledd og pasientjournalloven § 29, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i de respektive lovene.

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 størrelsesorden. Vi viser i denne forbindelse til artikkel 83 nr. 4, som lyder:

«4. 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 (…)».

4. Datatilsynets vurderinger og begrunnelse for vedtak

4.1 Vurdering av lovbrudd

Datatilsynet har vurdert om Oslo kommune ved Sykehjemsetaten har brutt kravene til tekniske og organisatoriske sikkerhetstiltak samt internkontroll som fremgår av personvernforordningen artikkel 32 og pasientjournalloven §§ 22 og 23.

Av forarbeidene til pasientjournalloven (Prop. 72 L (2013-2014)) fremgår det at loven gjelder ved behandling av helseopplysninger i forbindelse med ytelse av helsehjelp, uavhengig av hvor/i hvilket system opplysningene lagres. Dette medfører at kravene til informasjonssikkerhet og internkontroll i pasientjournalloven gjelder ved lagring av helseopplysninger på usikret intern sone så vel som i journalsystemet.

Datatilsynet legger til grunn at Sykehjemsetaten og de underliggende/samarbeidende institusjonene har hatt en høy bevissthet når det gjelder bruk av, og dokumentasjon i, pasientjournalsystemet. Videre er helsepersonells taushetsplikt grunnleggende kunnskap for størstedelen av de ansatte i etaten og de enkelte institusjonene. Den systemtekniske sikkerhetstenkningen synes imidlertid ikke å ha vært til stede i samme grad. Lagring av identifiserbare journalopplysninger om enkeltpasienter i en usikret sone, bryter klart med kravene til informasjonssikkerhet i personvernforordningen og pasientjournalloven.

Tilgangen til helseopplysningene på intern sone har til en viss grad vært tilgangsstyrt, ved at den enkelte ansatte har måttet logge seg inn for å tilgang. Det er imidlertid ubestridt at tilgangsstyringen til arbeidslistene ikke har vært god nok, ettersom opplysningene har vært tilgjengelige for et større antall ansatte som ikke har hatt tjenstlig behov for dem, herunder personer som ikke er helsepersonell. Det har heller ikke vært ført logg over systemet, og Sykehjemsetaten har dermed ikke hatt mulighet til å føre kontroll med tilgangen til, eller bruken av, arbeidslistene med tilhørende helseopplysninger.

Sykehjemsetatens overordnede styring av sykehjemmene/helsehusene gjennom ca. 11 år har ikke avdekket den avvikende praksisen med lagring av arbeidslister utenfor sikker sone. Forholdet har ikke vært gjenstand for risikovurdering eller på annen måte vært del av styringen. Vi legger til grunn enn at etaten ikke har hatt en tilstrekkelig bred tankegang i

oppfølgingen av de underliggende/samarbeidende institusjonenes praksis for informasjonssikkerhet.

Etter Datatilsynets vurdering har Oslo kommune ved Sykehjemsetaten brutt kravene til sikkerhet og internkontroll i personvernforordningen artikkel 32 og pasientjournalloven §§ 22 og 23.

4.2 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at Oslo kommune ved Sykehjemsetaten har brutt personvernforordningen artikkel 32 og pasientjournalloven §§ 22 og 23.

Lovbruddet har for 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. 1 000 000 NOK). Vi viser imidlertid til drøftelsen under punkt 3.1 og legger til grunn at gebyret skal utmåles etter nytt regelverk.

Det er dermed grunnlag for å ilegge Oslo kommune et overtredelsesgebyr på inntil 10 000 000 euro (p.t. ca. 105 000 000 NOK), jf. forordningens artikkel 83 nr. 4.

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

Den usikre lagringen av helseopplysninger ved sykehjemmene/helsehusene har foregått over lang tid, i minst 11 år. Lovbruddet har rammet et høyt, men ukjent antall pasienter, og mange ansatte – både helsepersonell og ikke-helsepersonell – har hatt tilgang på til dels store mengder helseopplysninger som de ikke har hatt tjenstlig behov for. Bruddet på kravene til informasjonssikkerhet anses omfattende og langvarig. Datatilsynet har ikke holdepunkter for at taushetsbelagt informasjon har kommet på avveie, men dette kan ikke være avgjørende for vår vurdering av lovbruddets alvorlighetsgrad.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Sykehjemsetaten har gjennomført risikovurderinger knyttet til informasjonssikkerhet og har hatt fokus på temaet over tid. Lagringen av helseopplysninger utenfor sikker sone har likevel ikke kommet frem gjennom etatsledelsens oppfølging av de underliggende/samarbeidende institusjonene i årene 2007-2018. Lovbruddet må betegnes som uaktsomt.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd

Sykehjemsetaten har sørget for at arbeidslistene nå er slettet, slik at opplysningene ikke lenger er tilgjengelige for uvedkommende.

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

Datatilsynet forutsetter at virksomheter som håndterer svært sensitiv informasjon, som for eksempel helseopplysninger, har særlig fokus på kravene til informasjonssikkerhet. Vi har ikke holdepunkter for at det er mangler ved Sykehjemsetatens styring og oppfølging av bruken av journalsystemet, men dette har ikke vært tilstrekkelig til å ivareta kravene til sikkerhet. Dette illustrerer behovet for en bred tenkning når det gjelder håndtering og lagring av helseopplysninger.

g) kategoriene av personopplysninger som er berørt av overtredelsen

I denne saken har helseopplysninger vært tilgjengelige for uvedkommende, herunder personer som ikke er helsepersonell. Etter personvernforordningen artikkel 9 nr. 1 er helseopplysninger betegnet som en særlig kategori personopplysninger, det vil si svært sensitive opplysninger. Dette øker alvorligheten 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

Sykehjemsetaten meldte selv avviket til Datatilsynet.

4.3 Samlet vurdering

Datatilsynet ser positivt på at Sykehjemsetaten raskt tok grep da den usikre lagringen ble oppdaget samt meldte fra om avviket til Datatilsynet. Etaten har også iverksatt tiltak som skal forhindre lignende lovbrudd i fremtiden.

Etter Datatilsynets vurdering, er saken imidlertid prinsipielt viktig. Oslo kommune er landets største kommune målt i innbyggertall, og Sykehjemsetaten burde vært rustet til å ivareta kravene til informasjonssikkerhet. Vi er ikke kjent med om bruk av arbeidslister praktiseres i landets andre kommuner, men det er gode grunner til å tro at Oslo kommune ikke er alene om en slik praksis. I dette henseende kan et vedtak om overtredelsesgebyr gi en viktig signaleffekt.

Noe som etter vår vurdering må tillegges stor vekt, er dessuten varigheten og omfanget av lovbruddet; en uoverskuelig mengde helseopplysninger har vært tilgjengelig for et stort antall ansatte gjennom minst 11 år, herunder ansatte som ikke er helsepersonell og dermed ikke er underlagt helsepersonellovens særskilte regler for håndtering av taushetsbelagt informasjon. Sykehjemsetatens overordnede styring har ikke vært egnet til å fange opp lovbruddet på et tidlig nok tidspunkt.

Etter en samlet vurdering har Datatilsynet kommet til at Oslo kommune skal ilegges et overtredelsesgebyr.

5. Vedtak om overtredelsesgebyr

5.1 Utmålingen av gebyret

I vurderingen av gebyrets størrelse, har vi sett hen til at Sykehjemsetaten raskt sørget for sletting av arbeidslistene og at etaten selv meldte avviket til Datatilsynet. Det er heller ikke kjent at praksisen har fått konkrete konsekvenser for enkeltpasienter, selv om dette tillegges mindre vekt.

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

Oslo kommune er landets største kommune etter innbyggertall og har tilsvarende økonomiske ressurser.

Datatilsynet har kommet til at et overtredelsesgebyr på 500 000 kr er rimelig i denne saken.

5.2 Vedtak om overtredelsesgebyr

Datatilsynet har vedtatt å gi Oslo kommune et overtredelsesgebyr med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. pasientjournalloven (2018) § 26 annet ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven (2018) § 26 andre ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83, pålegges Oslo kommune å betale et overtredelsesgebyr på 500 000 NOK – norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og pasientjournalloven §§ 22 og 23.*

5.3 Inndrivelse av overtredelsesgebyret

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig, jf. personopplysningsloven (2018) § 27. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

6. Klageadgang

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

7. 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 og forvaltningsloven § 13 første ledd nr. 2.

Dersom dere har spørsmål, kan dere ta kontakt med saksbehandler Susanne Lie.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Kopi til: OSLO KOMMUNE SYKEHJEMSETATEN, Linn Skorge, Postboks 435, 0103 OSLO
FYLKESMANNEN I OSLO OG VIKEN, Postboks 325, 1502 MOSS (ref. 2019/30779)