Datatilsynet

MOSS KOMMUNE
Postboks 175
1501 MOSS

Deres referanse	Vår referanse	Dato
20/10671-12- INAN	20/02165-9	04.06.2021

Vedtak om overtredelsesgebyr – Moss kommune

1. Innledning

Vi viser til innsendt melding av 4. februar 2020 om brudd på personopplysningssikkerheten, samt oppfølgende e-post av 12. februar 2020, og endelig melding om brudd på personopplysningssikkerheten av 27. april 2020. Vi viser også til korrespondanse med Moss kommunes personvernombud, bl.a. e-post av 2. november 2020.

Endelig vises det til Datatilsynets varsel om overtredelsesgebyr av 9. desember 2020 og svar på dette fra Moss kommune av 21. januar 2021, samt, samt øvrig korrespondanse i saken.

På bakgrunn av kommunens svar av 21. januar 2021, og tidligere saker, har vi justert overtredelsesgebyret ned til 500 000 kroner.

I medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83, ilegger vi Moss kommune et overtredelsesgebyr på ***500 000*** *kroner for å ha unnlatt å gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet i behandlingssystemene og tjenestene, jf. pasientjournalloven § 22, jf. personvernforordningen artikkel 32 nr. 1 bokstav b), og d), jf. artikkel 5.*

Bakgrunnen og begrunnelsen for vedtaket følger under.

2. Saksforholdet

I forbindelse med sammenslåingen av Rygge og Moss kommune som fant sted 1. januar 2020, har kommunen søkt å slå sammen bruken av IT-systemer for ulike tjenesteområder i kommunen. Dette gjelder bruk av fagsystemet CGM Journal, som Moss kommune har brukt i en årrekke, og som Rygge kommunes ansatte i helsetjenesten barn og unge tok i bruk etter sammenslåingen. I den sammenheng ble det foretatt en konvertering av brukere og systemets data 13. og 14. januar 2020.

Fagsystemet håndterer personopplysninger og helsedata og omfatter personer bosatt i kommunen, og som benytter helsestasjonen. Systemet gjelder tjenester forbundet med vaksinasjonsprogrammer i kommunen, og andre helsekontroller samt oppfølging av gravide.

Moss kommune har oppdaget feil i forbindelse med konverteringen fra HSPro til CGM Journal. Planen var at alle endringer som involverer helseopplysninger skulle løses fredag 7. februar, og det øvrige torsdag 13. februar. Det ble etablert et testmiljø slik at superbruker testet løsninger før de ble tatt i bruk i produksjonsmiljøet, samt at superbruker gjorde stikkprøver på at korrigeringene fungerte som de skulle.

Det har foregått feilretting fra 7. februar til 4. mars, da det også ble avdekket noen feil ut over det som opprinnelig var meldt inn til Datatilsynet. Disse framgår av endelig rapport av 27. april 2020.

Moss kommune opplyser at noen av bruddene representer brudd på personopplysningssikkerheten, herunder brudd på konfidensialitet, integritet og tilgjengelighet. Bruddene omfatter både voksne og barn.

Bruddene som er meldt inn er som følger:

- Feil i registrering av vaksiner, herunder registrert vaksiner som personer ikke har fått, og vaksiner som personer har fått og som ikke er registrert i vaksineoversikten. Feilene representerer en fare for feilvaksinering, og risiko for feil i Nasjonalt vaksineregister

- Feil i journaldata. Feil som er funnet er knyttet til oppfølging av mødre i svangerskap, bl.a. feil i antall svangerskapsuker, vekt og mål i skolehelsetjenesten og i opplysninger om mors bruk av rusmidler.

- Pasientopplysninger er gjort tilgjengelig for helsepersonell ved en avdeling som ikke har tjenstlig behov for tilgang, uten at tilgang kunne spores.

- Feil som er funnet er knyttet til daglig drift, som f.eks. timebøker og journalansvarlig.

Antall registrerte journaler i fagsystemet som ble overført var totalt 28 000. 2 000 personer er potensielt berørt, men det er ikke avdekket at noen personer spesifikt er rammet av feilene. Feilene er rettet og under kontroll pr. 11. februar 2020.

3 Lovovertredelsen
Avvikene gjelder brudd på konfidensialitet, integritet og tilgjengelighet. I personvernforordningen artikkel 32 heter det:

«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,

a) pseudonymisering og kryptering av personopplysninger,

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,

c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.»

Pasientopplysninger har ligget tilgjengelig for helsepersonell, uten tjenstlig behov, ved avdeling Bredsand Rygge. Feilene i konverteringen har medført fare for at pasientopplysninger ikke lenger er korrekte, gyldige og fullstendige ved at det oppstod feil i registrering av vaksiner og feil i journaldata knyttet til oppfølging av mødre i svangerskap. Ved konverteringen ble det registrert feil i opplysninger om rus/alkohol/røyk i svangerskapet. Feilen oppstod som en følge av at det er feilregistrert at alle har «sluttet i svangerskapet»; noe som ville bli tolket som om at alle brukte rusmidler i svangerskapet. Dette er nå rettet opp.

Dette utgjør brudd på personvernforordningen artikkel 32 nr. 1 bokstav b), som krever at det etableres et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet, integritet og tilgjengelighet.

I forbindelse med konverteringen oppstod det mange og svært alvorlige feil som kunne hatt store konsekvenser for de berørte. Manglende risikovurdering har vært en medvirkende årsak til de oppståtte feilene i konverteringen. Dette utgjør brudd på personvernforordningen artikkel 32 nr. 1 bokstav d).

Hendelsen tyder også på mangelfulle testkjøringer i forkant av prosessen. I e-post av 2. november 2020 opplyser CGM (databehandler) at det ble utført testing på Rygge kommune sin database i forbindelse med at konverteringsverktøyet måtte videreutvikles, for å kunne håndtere akkurat denne konverteringen, men at det ikke har vært utført tilstrekkelig testing i denne saken.

I en sak som handler om konvertering av store mengder sensitive data er det rimelig å forvente at det på forhånd blir etablert et test-regime bestående av ulike testscenarier egnet for å kunne avdekke ulike typer feil som kan oppstå ved denne type konverteringsaktivitet. Resultatene av slike tester bør dokumenteres i en testrapport som godkjennes eller underkjennes av behandlingsansvarlig før den faktiske konverteringen gjennomføres. Informasjonen i en slik testrapport ville kunne gitt verdifull informasjon til superbrukere og annet testpersonell i etterkant av konverteringen og ville ha gitt et godt grunnlag for å teste at all informasjon har blitt konvertert på riktig måte.

Dette vil være et brudd på personvernforordningen artikkel 32 nr. 1 bokstav d).

5 Vurdering av personvernforordningens regler om overtredelsesgebyr

I personopplysningsloven § 26 andre ledd er det bestemt at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 58, jf. artikkel 83 nr. 7. Det heter her at *«uten at det berører tilsynsmyndighetenes myndighet til å beslutte korrigerende tiltak i henhold til artikkel 58 nr. 2, kan hver medlemsstat fastsette regler om når og i hvilken grad offentlige myndigheter og organer som er etablert i nevnte medlemsstat, kan ilegges overtredelsesgebyr».*

Adgangen til å ilegge overtredelsesgebyr skal være et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Overtredelsesgebyr er å anse som straff etter Den europeiske menneskerettskonvensjonen artikkel 6.

Datatilsynet legger derfor til grunn at det kreves klar sannsynlighetsovervekt for lovovertredelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

Vi viser i denne sammenheng til kapittel IX i forvaltningsloven om administrative sanksjoner. Med en administrativ sanksjon menes en negativ reaksjon som kan ilegges av et forvaltningsorgan, som retter seg mot en begått overtredelse av lov, forskrift eller individuell avgjørelse, og som regnes som straff etter den europeiske menneskerettskonvensjonen (EMK).

For foretak er skyldvurderingen særegen. I forvaltningsloven § 46 (1) heter det:

> *«Når det er fastsatt i lov at det kan ilegges administrativ sanksjon overfor et foretak, kan sanksjonen ilegges selv om ingen enkeltperson har utvist skyld».*

I Prop. 62 L (2015-2016) side 199 uttales det om § 46: «Formuleringen om at 'ingen enkeltperson har utvist skyld' er hentet fra paragrafen om foretaksstraff i straffeloven § 27 første ledd og skal forstås på samme måte. Ansvaret er derfor som utgangspunkt objektivt».

Artikkel 83 gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal ha særlig vekt. Det fremgår av artikkel 83 nr. 1 at Datatilsynet skal sikre at ilegging av overtredelsesgebyr i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.

I vår vurdering av om vi skal ilegge overtredelsesgebyr, har vi særlig lagt vekt på følgende momenter:

a) ***karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte handlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd***

Bruddet på personopplysningssikkerheten omfatter brudd på konfidensialitet, integritet og tilgjengelighet. Pasientopplysninger er gjort tilgjengelig for andre ved en avdeling som ikke har tjenstlig behov. Hvem som har hatt tilgang til pasientdataene er ikke sporbart.

Konverteringsfeilene har også medført at man i en periode ikke kunne være sikker på at personopplysningene var riktige. F.eks. ble alle gravide klassifisert som rusmiddelmisbrukere uten å være det.

Det har ikke vært gjennomført risikovurderinger og vurdering av personvernkonsekvensene ved konverteringen. Bruddene på personopplysningssikkerheten tyder også på mangelfull testkjøring i forkant av konverteringen.

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll på opplysninger om seg selv. Dette gjelder både i forhold opplysningenes korrekthet og hvem som har sett opplysningene. Helseopplysninger har vært tilgjengelige for helsepersonell ved Bredsand Rygge, uten at det er sporbart hvem som har sett disse.

Datatilsynet ser alvorlig på at det fra kommunens side ikke har vært iverksatt tilstrekkelige tekniske tiltak for å sikre en trygg konvertering av helseopplysninger fra system i Rygge kommune til system i Moss kommune.

b) ***hvorvidt overtredelsen ble begått forsettlig eller uaktsomt***

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll på opplysninger om seg selv. Det har ikke vært gjennomført noen risikovurdering, vurdering av personvernkonsekvensene eller tilstrekkelige testkjøringer før konverteringen ble gjennomført. Saken viser at det har vært rutinesvikt i kommunen. Bruddet omfatter særlige kategorier av personopplysninger, noe som burde ha medført ekstra forsiktighet fra kommunens side. Datatilsynet anser kommunens handling som uaktsom.

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

Kommunen har vært i kontakt med de berørte og informert om hendelsen. Kommunen vurderte først at bruddet på personopplysningssikkerheten ikke ville medføre en høy risiko for de berørtes rettigheter og friheter. Datatilsynet vurderer dette annerledes og har kommet til at omfanget og bruddets karakter gjør at Moss kommune befinner seg i kjerneområdet for varslingsplikten, jf. artikkel 34. At kommunen ikke har registrert at noen av konsekvensene har inntrådt skal tillegges betydning. Dette ble meddelt kommunen i brev av 9. mars 2020.

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***

I denne saken innrømmer CGM at de som databehandler må bære hovedansvaret for testkjøringen, men at kommunen hadde hovedansvaret for kvalitetssikring av konverterte data. Datatilsynet deler dette synet.

e) ***eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren***

Det kan ikke konstateres tidligere overtredelser som er begått av den behandlingsansvarlige eller databehandlere som er relevant for saken.

f) ***graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den***

Det har ikke vært noe samarbeid mellom Datatilsynet og Moss kommune for å bøte på skaden.

g) ***kategoriene av personopplysninger som er berørt av overtredelsen***

Bruddet på personopplysningssikkerhet omfatter helseopplysninger, som er en særlig kategori av personopplysninger, som omfattes av artikkel 9. At bruddet omfatter særlige kategorier av personopplysninger gjør hendelsen ekstra alvorlig.

h) ***hvilken måte tilsynsmyndigheten fikk kunnskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen***

Moss kommune, ved personvernombudet, varslet Datatilsynet om bruddet på personopplysningssikkerheten ved e-post av 4. februar 2020

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***

Ikke relevant for saken.

j) ***overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42***

Ikke relevant for saken.

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***

Datatilsynet ser positivt på at Moss kommune raskt tok grep da bruddet på personopplysningssikkerheten ble oppdaget. Kommunen har også iverksatt tiltak som skal forhindre lignende lovbrudd i fremtiden.

Datatilsynet har ikke konstatert at Moss kommune har hatt økonomiske fordeler, eller unngått direkte eller indirekte tap som et resultat av overtredelsen.

Datatilsynet har heller ikke tatt hensyn til Moss kommunes økonomiske evne.

6 Samlet vurdering

Det er svært alvorlig at kommunen i forbindelse med konvertering av pasientopplysninger fra Rygge kommune til Moss kommune gjennomførte denne konverteringen uten en risikovurdering eller vurdering av personvernkonsekvensene. Det har heller ikke vært gjennomført tilstrekkelig testing i forkant av konverteringen.

Etter Datatilsynets vurdering, er saken prinsipielt viktig. Moss kommune burde vært rustet til å ivareta kravene til personopplysningssikkerhet ved den hendelsen som denne saken omfatter. I denne henseende kan et vedtak om overtredelsesgebyr gi en viktig signaleffekt.

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

7 Gebyrets størrelse

I forarbeidene til ny personopplysninglov (Prop. 56 LS (2017-2018)) uttaler departementet at

> «som utgangspunkt [skal] de samme reglene for overtredelsesgebyr gjelde for offentlige organer som for private, da dette er ordningen etter gjeldende personopplysningslov.»

Departementet skriver videre at de har notert seg bekymringen som enkelte offentlige høringsinstanser har uttrykt, men departementet legger til grunn at det innenfor reglene i forordningen artikkel 83, som også angir de momenter det skal legges vekt på ved utmålingen av administrative gebyrer, ligger rom for et betydelig skjønn med hensyn til størrelsen på gebyret. Departementet uttaler at «[b]eløpsgrensene i forordningen artikkel 83 angir maksimalgrenser for utmåling av administrative gebyrer, mens det ikke er fastsatt noen minimumsgrenser.»

Når det gjelder gebyrets størrelse, skal de samme momenter som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken, samtidig som gebyrets størrelse må stå i et rimelig forhold til overtredelsen og virksomheten, jf. art. 83 nr. 1.

Datatilsynet er enig i de innspill kommunen har til størrelsen på overtredelsesgebyret, sett i forhold til lignende saker som Datatilsynet har behandlet, og finner å kunne justere dette ned til kroner 500.000.

Etter en totalvurdering av saken, og da særlig sett hen til alvorligheten i overtredelsen og lovverkets krav om at ileggelsen av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende, har vi kommet til at et overtredelsesgebyr på **500 000 NOK** anses som riktig.

8 Oppfyllelsesfrist og klageadgang

Dere kan klage på vedtaket. En eventuell klage må sendes **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.

Dersom dere ikke påklager pålegget om overtredelsesgebyr, er oppfyllelsesfristen fire uker etter klagefristens utløp, jf. personopplysningsloven § 27.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer