Datatilsynet

KARMØY KOMMUNE
Postboks 167
4291 KOPERVIK

Deres referanse	Vår referanse	Dato
21/11153-14	21/03649-8	03.01.2023

Vedtak om overtredelsesgebyr - brudd på personopplysningssikkerheten - Karmøy kommune

1. Innledning

Vi viser til vårt varsel av 4. oktober 2022 om vedtak om overtredelsesgebyr og deres svar på varselet datert 21. november 2022. Bruddet på personopplysningssikkerheten hos Karmøy kommune ble oppdaget 14. oktober 2021.

2. Vedtak om overtredelsesgebyr

Datatilsynet har besluttet å vedta følgende overtredelsesgebyr:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 og pasientjournalloven § 29, jf. personvernforordningen artikkel 83, pålegges Karmøy kommune å betale et overtredelsesgebyr på 300 000 – trehundretusen – kroner til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32, jf. personvernforordningen artikkel 24, og pasientjournalloven §§ 22 og 23.*

3. Beskrivelse av sakens faktiske forhold

3.1 Generelt om den innmeldte hendelsen

Fra 1. januar 2019 til 5. november 2021 har det ifølge meldingen vært manglende tilgangskontroll i mapper som ligger på fellesområdet (heretter omtalt som «sikker sone») i kommunens systemer. Årsaken er at mapper har blitt opprettet av ansatte uten at IKT-avdelingen har blitt orientert, slik at mappene ikke har hatt tilgangskontroll.

Hendelsen ble oppdaget i forbindelse med opplæring da en ansatt skulle demonstrere tilgangsstyringen på sikker sone. Det ble umiddelbart varslet som et avvik internt.

Hendelsen omfatter omtrent 28 000 registrerte personopplysninger. Disse personopplysningene er imidlertid ikke knyttet til 28 000 unike brukere, da samme brukere

har personopplysninger registrert i flere mapper og i gjentakende dokumenter (fakturaer, dusjlister etc.). Dokumentasjonen fra kommunen viser likevel at det samlet sett er et høyt antall registrerte som er berørt av avviket.

Ifølge kommunen, er det vanskelig å anslå antall berørte registrerte da det vil være arbeidskrevende å koble sammen personer og personopplysninger fra de ulike mappene. Det opplyses om at noen av arkivmappene strekker seg tilbake til 1999.

Avviket omfatter omtrent 60 åpne mapper, hvorav 25 mapper inneholder personopplysninger. Personopplysningene representerer ulik grad av sensitivitet. På avvikstidspunktet var det følgende sensitive personopplysninger lagret på sikker sone:

- Opplysninger tilhørende tjenesten Rus og psykisk helsetjenesten, der seks mapper med undermapper inneholder boligkartlegging, oversikt over brukere av rus og psykiatritjeneste, med tilhørende aktivitetstiltak og kommunal bolig til hver bruker. Her fremkommer det navn, fødselsdato, adresse, personnummer, eventuelle diagnoser og gjeld til enkeltbrukere.
- To åpne mapper med opplysninger over tjenestemottakere av støttekontakt og avlastning.
- Én åpen mappe med opplysninger om egenandeler for fysioterapi knyttet til brukere.
- Ti åpne mapper med opplysninger tilknyttet hjemmetjenestene. Her fremkommer det opplysninger om brukere av hjemmetjenester med navn, fødselsdato, fødselsnummer, medisinoversikt, vektstatus, dusj- og rengjøringslister, trygghetsalarm, praktisk hjelp-lister, innleggelse på sykehus, HRL-status, informasjon om nøkkelboks, oversikt over pasienters nøkler, ernæringsinformasjon, øvrige vedtak og vaksinasjonsoversikt.
- Syv åpne mapper tilknyttet bolig- og miljøarbeidstjenesten med oversikt over navn, fødselsdato og tjenesterapporter om brukere.
- Én mappe tilknyttet bestillerkontoret som inneholder opplysninger om navn på brukere, beregningsgrunnlag, belegglister, oversikt over alle aktive tjenester, brukeroversikter og transportlister.

Kommunen opplyser at det var 2 377 tilganger til sikker sone i avviksperioden på i underkant av to år. Av disse tilgangene var den største gruppen fast ansatte bestående av 1 361 tilganger, 486 tilganger var ansatte med kode «tilfeldig timelønnede», og en siste gruppe bestod av vikarer, lærlinger og ansatte i permisjon. I svaret på varsel om vedtak presiserer kommunen at det kun er ansatte i sektor Helse og omsorg som har tilgang til «sikker sone».

Kommunen mener at det reelle antall brukere av sikker sone er betydelig lavere enn antall tilganger som var først rapportert inn. Dette begrunnes med at «tilgangshaver enten må være utstyrt med egen pc med sikkerhetskort for tilgang til Norsk Helsenett eller ha tilgang til tynnklient i «sikker-sone» bygg (også fysisk tilgangsstyrte bygg), vil eventuelt aktive brukertilganger som ikke har ansettelsesforhold i Karmøy kommune ikke ha fysisk mulighet til å få tilgang til «sikker sone» eller de personopplysningene som avviket omhandler». Dette innebærer at antallet ansatte med tilgang til «sikker sone» i avviksperioden er anslått til å være 1 727 ansatte.

Ifølge Karmøy kommune, er det ingenting som indikerer at personopplysninger har blitt kompromittert eller brukt til andre formål. Alle som har hatt tilgang har signert en taushetsplikterklæring.

3.2 Tilgangskontroll

Det fremkommer av avviksmeldingen at ansatte med tilgang til sikker sone har opprettet egne mapper på fellesområdet uten at dette er gjort via IKT-avdelingen. Manglende tilgangskontroll i mappestrukturen har ført til at et stort antall kommunalt ansatte har hatt tilgang til personopplysninger uten tjenstlig behov.

I svaret på varsel om vedtak presiserer kommunen at for å ha tilgang til «sikker sone», må den ansatte ha en PC som er satt opp med Norsk Helsenett eller benytte en tynnklient i et sikkert sone bygg for å få tilgang til den aktuelle mappestrukturen.

Kommunen gjennomførte en anonym spørreundersøkelse blant sine ansatte for å undersøke hvorvidt sikker sone benyttes av den ansatte, om vedkommende har vært oppmerksom på manglende tilgangskontroll og om den ansatte har blitt kjent med personopplysninger uten tjenstlig behov. Undersøkelsen ble sendt ut til 1 361 fast ansatte, hvorav 526 sendte inn svar.

Resultatet viste at 164 ikke bruker sikker sone, og 63 svarte at de hadde opplevd å komme seg inn på en mappe som ikke lå til deres fagfelt, herunder hadde ti av disse fått tilgang til personopplysninger. Kun to ansatte svarte at de hadde klikket seg inn på en mappe de var klar over at de ikke hadde tjenstlig behov for, men at de umiddelbart lukket mappen da de oppdaget at denne inneholdt personopplysninger.

3.3 Logging

Det har ikke vært funksjonalitet for logging av tilgang til mappestrukturen på sikker sone. Manglende logging innebærer at det heller ikke har vært mulig å avdekke uautorisert tilgang og en eventuell kompromittering av personopplysninger lagret på sikker sone.

3.4 Interne rutiner for lagring og skjerming

Ifølge avviksmeldingen manglet det interne rutiner for skjerming av mapper, for opprettelse av mappestruktur og tilgangskontroll på sikker sone.

Det angis at det er flere forhold som har ført til at mappestrukturen på sikker sone har vært uoversiktlig. Avviket har avdekket at det ikke har vært tydelig definert hvem som har ansvaret for å følge opp og kontrollere innholdet i mappene, noe som har resultert i at flere mapper har ligget lagret uten at en person har vært ansvarlig.

Videre har flere mapper og enkeltstående dokumenter blitt liggende på sikker sone etter endringer i organisasjonsstrukturen, på grunn av manglende sletterutiner. Det opplyses også om manglende kunnskap blant ansatte om funksjonalitet i pasientjournalsystemet, noe som kan ha bidratt til opprettelse av unødvendig mange dokumenter på sikker sone.

Avviksmeldingen informerer også om at det har vært manglende rutiner for å fjerne ansattes tilganger i forbindelse med bytte av jobb eller endring av tjenestested.

3.5 Iverksatte og planlagte tiltak
Avviket ble meldt av en kommunalt ansatt som oppdaget avvik i forbindelse med opplæring. Det ble deretter iverksatt en systematisk gjennomgang av mapper på fellesområdet. Sensitive opplysninger ble fjernet fra mappene som lå åpne og flyttet til mapper med tilgangskontroll. 5. november 2021 sørget IKT-avdelingen i kommunen for å opprette en ny mappestruktur med tilgangsstyring som samsvarer med tjenestested i HRM-systemet.

Samtidig ble det gjennomført sletting av overflødige og utdaterte mapper og dokumenter. Arbeid med oppdatering av rutiner for lagring og skjerming i mappestruktur og fagsystemer er satt i gang. Det opplyses også om at kommunen har gjennomgått interne prosedyrer for avvikshåndtering.

3.6 Informasjon til de registrerte
Karmøy kommune har besluttet å ikke varsle berørte personer da de vurderer at risikoen ikke er høy for de registrerte. Begrunnelsen for dette er at kommunen har strenge regler og sanksjoner for ansattes tilegnelse av informasjon uten tjenstlig behov. Det er ifølge kommunen god kultur for å varsle avvik og at ansatte i stor grad følger regler knyttet til taushetsplikten. Kommunen presiserer at alle ansatte som hadde tilgang til sikker sone hadde signert taushetserklæring.

4. Rettslig grunnlag

4.1 Datatilsynets kompetanse
Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen 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.

4.2 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.

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.

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».

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 eller i hvilket system opplysningene lagres. Dette medfører at kravene til

informasjonssikkerhet og internkontroll i pasientjournalloven gjelder ved lagring av helseopplysninger på intern sone i kommunen så vel som i journalsystemet.

4.4 Informasjon til berørte personer

Dersom det er sannsynlig at sikkerhetsbruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den dataansvarlige uten ugrunnet opphold underrette de berørte personene om bruddet, jf. personvernforordningen artikkel 34 nr. 1.

Tilsynsmyndigheten kan pålegge den dataansvarlige å informere berørte personer, jf. artikkel 34 nr. 4. De nærmere kravene til innholdet i en slik underretning fremgår av artikkel 34 nr. 2 og 3.

4.5 Overtredelsesgebyr

4.5.1 Generelt om overtredelsesgebyr og skyldkravet

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsregelverket.

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 (EMK) artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr. 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 EMK.

I forvaltningsloven § 46 første ledd 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».

Høyesterett har i dom HR-2021-797-A lagt til grunn at det objektive ansvaret for foretaksstraff som følger av straffeloven § 27 ikke er forenlig med straffebegrepet i EMK slik det er tolket av Den europeiske menneskerettsdomstolen (EMD). Høyesterett uttaler i dommen at den som har handlet på vegne av foretaket må ha utvist skyld og at alminnelig uaktsomhet er tilstrekkelig for å oppfylle dette.

Ettersom overtredelsesgebyr regnes som straff etter EMK, legger vi til grunn at vi bare kan ilegge en virksomhet overtredelsesgebyr dersom den som har opptrådt på vegne av virksomheten har utvist skyld og at alminnelig uaktsomhet er tilstrekkelig, jf. HR-2021-797-A.

4.5.2 Datatilsynets kompetanse til å ilegge overtredelsesgebyr
Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 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. De relevante delene av bestemmelsene 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 (...)».

I personopplysningsloven § 26 første ledd fremgår det at personvernforordningen artikkel 83 nr. 4 gjelder tilsvarende for overtredelser av forordningen artikkel 24.

5. Datatilsynets vurdering

I redegjørelsen for vår vurdering av avviket vil vi følge samme kronologi som under *Beskrivelse av sakens faktiske forhold* i punkt 3.

5.1 Tilgangskontroll

Avviket representerer et brudd på konfidensialitet som følge av at alle ansatte hos kommunen med tilgang til sikker sone har hatt tilgang til personopplysninger uten tjenstlig behov.

Datatilsynet har registrert at det ikke er konstatert ulovlig innsyn eller utlevering av opplysninger, men det har heller ikke vært etablert tekniske løsninger som gjorde det mulig å avdekke dette. Det avgjørende for vår vurdering av tilgangskontrollen er det faktum at personopplysninger, herunder helseopplysninger, har vært tilgjengelig for et større antall ansatte enn de som har hatt tjenstlig behov for disse.

Det faktum at alle med tilgang til mappene på sikker sone har signert erklæring for taushetsplikt er etter Datatilsynets syn ikke relevant i denne sammenheng. Taushetsplikten kan ikke spille inn i vurderingen av hvilke personopplysninger en ansatt skal ha tilgang til. Vi viser her til kravet om at ansatte ikke skal ha tilgang til personopplysninger de ikke har tjenstlig behov for, uavhengig av om den ansatte har taushetsplikt eller ikke.

Datatilsynet legger til grunn at Karmøy kommune har brutt sin plikt til å sørge for tilgangsstyring som en del av sin internkontroll og plikt til tilstrekkelig personopplysningssikkerhet, jf. personvernforordningen artikkel 32, artikkel 24 og pasientjournalloven §§ 22 og 23.

5.2 Logging

Karmøy kommune har ikke hatt funksjonalitet for å loggføre aktivitet på sikker sone. Den manglende loggføringen øker risikoen for at man mister oversikt over hvor personopplysninger befinner seg. Det har heller ikke vært mulig for Karmøy kommune å bekrefte eller avkrefte om det faktisk har skjedd uautorisert tilgang til personopplysningene på sikker sone.

Datatilsynet vurderer at Karmøy kommune har brutt sin plikt til å ha en funksjon for loggføring, slik at det ikke har vært mulig å avdekke uautorisert tilgang og eventuell kompromittering av personopplysninger, jf. personvernforordningen artikkel 32, artikkel 24 og pasientjournalloven §§ 22 og 23.

5.3 Interne rutiner for skjerming og kontroll

Basert på mottatte opplysninger, har det etablert seg en praksis i Karmøy kommune der ansatte har opprettet mapper uten å involvere IKT-avdelingen. Datatilsynet vurderer at denne praksisen kan tyde på manglende rutinebeskrivelser for regulering av tilgangsstyring og manglende opplæring av ansatte. Det er i tillegg bekreftet av Karmøy kommune at rutiner for skjerming og kontroll ikke fantes på avvikstidspunktet.

Vi presiserer at det er ledelsen i kommunen som har det overordnede ansvaret for å iverksette tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder interne rutiner for lagring, tilgangskontroll og sletting.

Datatilsynet legger til grunn at det må etableres rutiner som regulerer aktivitet på sikker sone, herunder opprettelse av mapper med tilgangskontroll, fjerning av tilganger ved endringer av ansettelser og sletting av dokumenter. I tillegg må ansvarsforhold tilknyttet mappestrukturen klarlegges. Avviksmeldingen nevner at det er behov for opplæring i journalføringssystemet slik at det ikke lagres unødvendige opplysninger på sikker sone. Denne vurderingen støttes av Datatilsynet.

Vi stiller også spørsmål ved om kommunens interne rutiner for å avdekke brudd på personopplysningssikkerheten er tilfredsstillende. Vi viser her til at det aktuelle avviket ble oppdaget ved en tilfeldighet i forbindelse med opplæring av nyansatt og at bruddet da hadde pågått i nesten to år.

Datatilsynet legger til grunn at Karmøy kommune ikke har hatt interne rutiner for skjerming av personopplysninger i samsvar med plikten til internkontroll. Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24, jf. pasientjournalloven §§ 22 og 23.

5.4 Iverksatte og planlagte tiltak

Karmøy kommune iverksatte strakstiltak etter at avviket ble oppdaget.
Det er også iverksatt langsiktige tiltak som tyder på at Karmøy kommune har forstått alvorlighetsgraden av avviket. Datatilsynet ser positivt på at det nå er etablert rutiner som regulerer tilgangsstyring til dokumenter på sikker sone.

Datatilsynet har ingen øvrige merknader til de iverksatte og planlagte tiltakene.

5.5 Informasjon til de registrerte

Etter personvernforordningen artikkel 34 utløses plikten til å underrette de berørte personene dersom sikkerhetsbruddet medfører «høy risiko» for fysiske personers rettigheter og friheter. Karmøy kommune har vurdert at det ikke foreligger behov for å varsle de berørte registrerte som følge av at risikoen knytte til avviket ikke var å anse som høy.

Risikoen for de registrerte vil som et utgangspunkt være høy når personopplysninger ligger åpent tilgjengelige for ansatte i kommunen, der flesteparten av de ansatte ikke har tjenstlig behov for opplysningene.

Datatilsynet vektlegger at opplysningene vært tilgjengelige for 1 727 ansatte som har hatt tilgang til sikker sone. Avviket omfatter sensitive opplysninger om mange registrerte, noe

som representerer et alvorlig brudd på plikten til konfidensialitet. Personer har en berettiget forventning om konfidensialitet når opplysninger om dem behandles av, og lagres i, kommunens fagsystemer. Det er videre en allmenn forventning om at tilgang til personopplysninger skal begrenses til den ansattes tjenstlig behov.

Det er imidlertid ikke mulig å etterprøve hvorvidt ansatte faktisk har gjort innsyn, om det har skjedd en spredning av personopplysninger, om personopplysninger er brukt til andre formål, eller hvor mange ansatte dette eventuelt gjelder. I mangel på loggfunksjon, har kommunen gjennomført en anonym spørreundersøkelse som avdekket liten risiko for uberettiget tilgang til personopplysninger på sikker sone. På tross av at det kun var 39 % av de 1 361 fast ansatte som svarte på undersøkelsen, gir svarene en indikasjon på at det er få ansatte som har benyttet seg av den vide tilgangen på sikker sone.

At de ansatte har taushetsplikt, er ikke relevant for vurderingen av hvilke opplysninger en ansatt skal ha tilgang til. Taushetsplikten kan likevel begrense skadevirkningene av urettmessig tilgang til personopplysninger. I taushetsplikten ligger det en forutsetning om at helsepersonell ikke skal spre taushetsbelagt pasientinformasjon.

Samlet sett har Datatilsynet kommet til at Karmøy kommune ikke plikter å underrette de registrerte som er berørte av avviket, jf. personvernforordningen artikkel 34.

5.6 Oppsummering

Karmøy kommune har en lovpålagt plikt til å sørge for at ansatte ikke har tilgang til sensitive personopplysninger de ikke har tjenstlig behov for. I tillegg skal det etableres systemer for logging og etterfølgende kontroll som gjør det mulig å avdekke avvik.

Det er et ledelsesansvar at tekniske og organisatoriske løsninger er på plass slik at kommunen er i stand til å håndtere sensitive personopplysninger.

Datatilsynet vurderer at det har vært grunnleggende mangler ved internkontrollen og informasjonssikkerheten hos Karmøy kommune tilknyttet sikker sone. Dette er et brudd på personvernforordningen artikkel 32, artikkel 24 og pasientjournalloven §§ 22 og 23.

5.7 Vurdering av skyldkravet for ileggelse av overtredelsesgebyr

For at Datatilsynet skal kunne ilegge Karmøy kommune et overtredelsesgebyr, kreves det at den eller de som har opptrådt på vegne av kommunen har utvist en form for skyld. I denne saken er vår vurdering at den aktuelle skyldformen er simpel uaktsomhet, jf. forvaltningsloven § 46 første ledd første punktum

I henhold til kravet om aktsomhet, må virksomheter sette seg inn i hvilken lovgivning som gjelder på et området og innrette virksomheten i samsvar med de rammer som følger av det aktuelle regelverket.

I denne saken har Karmøy kommune erkjent manglende tilgangskontroll, loggføring og interne rutiner for skjerming av opplysninger på sikker sone. Vi legger til grunn at kravene til

internkontroll og informasjonssikkerhet er et ledelsesansvar, jf. personvernforordningen artikkel 5 nr. 2.

Som følge av de nevnte mangler, er Datatilsynets konklusjon at kravene til informasjonssikkerhet og internkontroll ikke er overholdt av kommunens ledelse og ansatte. Lovbruddet må betegnes som uaktsomt.

Skyldkravet for å ilegge overtredelsesgebyr er dermed oppfylt.

5.8 Vurdering av om overtredelsesgebyr skal ilegges
Datatilsynet har kommet til at Karmøy kommune har brutt personvernforordningen artikkel 32, artikkel 24 og pasientjournalloven §§ 22 og 23.

Nedenfor gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges jf. personvernforordningen artikkel 83 nr. 4.

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
Konfidensialitetsbruddet har pågått i en periode på nesten to år, der sensitive opplysninger om flere hundre av kommunens brukere har vært tilgjengelige for ansatte uten tjenstlig behov. Det er tale om 1 727 unike tilganger til sikker sone i avviksperioden. Vi ser alvorlig på at kommunen ikke har hatt rutiner for å fjerne ansattes tilganger i forbindelse med permisjon, bytte av jobb eller endring av tjenestested.

Selv om det ikke finnes dokumentasjon på at ansatte faktisk har gjort urettmessig innsyn eller at personopplysninger er blitt brukt til utenforliggende formål, er det heller ikke mulig å kontrollere om dette har skjedd eller om pasientopplysninger har kommet på avveie. Disse momentene taler for at overtredelsesgebyr skal ilegges.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt
Datatilsynet viser til punkt 4.7 og konkluderer med at lovbruddet må betegnes som uaktsomt av kommunens ledelse.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd
Karmøy kommune har nå sørget for tilgangskontroll og logging av sikker sone. Datatilsynet er orientert om at det er utarbeidet interne rutiner for skjerming og håndtering av personopplysninger på sikker sone. Disse momentene taler i kommunens favør.

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
Karmøy kommune har ikke overholdt sine plikter til informasjonssikkerhet og internkontroll ved bruk av sikker sone. Datatilsynet mener det har foreligget grunnleggende mangler ved kommunens tilgangskontroll, logging og interne rutiner for skjerming av personopplysninger på sikker sone.

f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den
Datatilsynet har blitt løpende orientert i avvikssaken og mottatt god informasjon om avvikets art og omfang.

g) kategoriene av personopplysninger som er berørt av overtredelsen
I denne saken har både helseopplysninger og andre sensitive opplysninger vært tilgjengelige for et stort antall ansatte uten tjenstlig behov. Avviket omfatter blant annet opplysninger om rus og psykiatri, hjemmehjelp, kommunal bolig og personnummer.

Etter personvernforordningen artikkel 9 nr. 1 er helseopplysninger betegnet som en særlig kategori personopplysninger, det vil si svært sensitive opplysninger. 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
Karmøy kommune meldte selv fra om avviket til Datatilsynet i henhold til plikten oppstilt i personvernforordningen artikkel 33.

Datatilsynets oppsummering og vurdering
Karmøy kommune er pålagt å sørge for at ansatte ikke har tilgang til personopplysninger de ikke har tjenstlig behov for. I tillegg foreligger det en plikt til å etablere systemer for logging og etterfølgende kontroll som gjør det mulig å avdekke avvik.

Datatilsynet ser positivt på at det ble iverksatt tiltak for stanse eksisterende praksis umiddelbart.

Basert på de opplysningene vi har mottatt, mener vi at avviket er av en så alvorlig karakter at det er nødvendig å ilegge overtredelsesgebyr.

5.9 Gebyrets størrelse
I vurderingen av gebyrets størrelse er de samme momentene som nevnt under punkt 5.8 relevante å ta i betraktning.

Overtredelsens karakter, alvorlighetsgrad og varighet
Det er sentralt å se på overtredelsens karakter, alvorlighetsgrad og varighet, jf. artikkel 83 nr. 2 bokstav a. Det følger av bestemmelsen at det skal tas hensyn til den berørte handlingens art, omfang eller formål, samt antall registrerte som er berørt og omfanget av den skade de har lidd.

Helseopplysninger utgjør en særlig kategori av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1, og fortjener et særskilt vern. I denne saken har en stor mengde sensitive personopplysninger vært tilgjengelig for kommunens ansatte, uten tjenstlig behov, i nærmere to år. I tillegg, har avviket avdekket manglende opplæring og

etterfølgelse av interne rutiner hva gjelder skjerming og sletting av personopplysninger på sikker sone. Vi vurderer at det foreligger grunnleggende mangler ved kommunens tilgangskontroll, logging og interne rutiner for skjerming av personopplysninger på sikker sone. Dette ser vi på som alvorlig og et moment som taler for et overtredelsesgebyr av en viss størrelse.

Hensynet til likebehandling
Karmøy kommune har bedt Datatilsynet vurdere å redusere det varslede gebyret på NOK 300 000, basert på hensynet til likebehandling av saker. Kommunen har vist til sak 18/03623, der Datatilsynet vedtok et overtredelsesgebyr på NOK 500 000 til Oslo kommune Sykehjemsetaten. Avviket var av et større omfang, tidsrom og alvorlighetsgrad enn den aktuelle avvikssaken. I Oslo kommune Sykehjemsetaten hadde det opparbeidet seg en praksis over 11 år der helseopplysninger var lagret utenfor sikker sone og ansatte uten tjenstlig behov hadde tilgang. Datatilsynet mener at avvikets alvorlighetsgrad gjenspeiles i overtredelsesgebyrets beløp på NOK 500 000.

Argumentet til Karmøy kommune om at Oslo kommune er en større virksomhet med bedre økonomisk bæreevne, har begrenset vekt. Avviket i Karmøy kommune omhandler brudd på helt grunnleggende krav til informasjonssikkerheten som alle kommuner er forpliktet til å følge. Vi minner om at personvernforordningen legger til grunn at tilsynsmyndigheten skal ilegge overtredelsesgebyr som er virkningsfull og virker avskrekkende i hvert enkelt tilfelle, jf. artikkel 83 nr. 1.

Det er i denne sammenheng også verdt å nevne sak 20/02291 der Sykehuset Østfold HF fikk et overtredelsesgebyr på NOK 750 000, som ble nedjustert av Datatilsynet til NOK 500 000 i klageomgangen som følge av lang saksbehandlingstid. Avviket omhandlet manglende tilgangsstyring av rapportuttrekk fra elektronisk pasientjournal (EPJ) i en periode på fem år. Det var 118 ansatte helsepersonell med taushetsplikt som hadde tilgang til opplysningene, hvorav flere ikke hadde tjenstlig behov for tilgang til opplysningene. Den ulovlige behandlingen pågikk både før og etter ny personopplysningslov trådte i kraft, slik at saken ble vurdert etter ny lov, jf. personopplysningsloven § 33, og har sammenligningsverdi med den aktuelle avvikssaken. Saken ble klaget inn for Personvernnemnda som nedjusterte beløpet til NOK 400 000, se PVN-2021-16. Nemnda uttalte at NOK 400 000 var et passende beløp for et avvik av slik karakter.

Datatilsynet mener at sakene har flere likhetstrekk. I avviket hos Karmøy kommune er det tale om personopplysninger av sensitiv karakter, herunder opplysninger om rus, diagnoser, personnummer, støttekontakt, og dusjlister og ernæringsinformasjon om brukere som mottar hjemmehjelpstjeneste. Det er tale om langt flere ansatte som har hatt tilgang uten tjenstlig behov i Karmøy kommune, selv om avviket pågikk lengre i Sykehuset Østfold-saken.

Vi mener derfor at hensynet til likebehandling ikke taler for en nedjustering av det varslede overtredelsesgebyret.

Bruk av ressurser i forbindelse med avvikshåndtering

Karmøy kommune argumenterer at beløpet må settes ned som følge av at kommunen allerede har benyttet betydelige ressurser på å kartlegge ansattes bruk av «sikker sone».

Datatilsynet har tatt i betraktning at Karmøy kommune raskt sørget for skjerming av personopplysningene som var tilgjengelige og at kommunen selv meldte inn avviket til Datatilsynet. Vi ser videre positivt på at Karmøy kommune har tatt avviket på alvor og har sendt inn nødvendige opplysninger i forbindelse med vår behandling av saken.

Samtidig, vil vi understreke at Karmøy kommune er forpliktet til å ha oversikt over personopplysningene som er til behandling i kommunen samt melde inn brudd på personopplysningssikkerheten som er meldepliktige etter personvernforordningen artikkel 33. Vi vurderer at kommunens ressursbruk i forbindelse med avvikssaken har begrenset vekt.

Konklusjon
Basert på de nevnte momenter, beslutter Datatilsynet å opprettholde vår vurdering om at et overtredelsesgebyr på NOK 300 000 er rimelig i denne saken.

6. Klageadgang

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen 20. januar 2023**, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

7. Inndrivelse av overtredelsesgebyret

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

8. Innsyn og offentlighet

Alle dokumentene i saken er i utgangspunktet offentlige, jf. offentlighetsloven § 3. Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentene fra offentlig innsyn, ber vi dere om å begrunne dette.

Dersom dere har spørsmål, kan dere ta kontakt med saksbehandler Kristin Skolt på kristin.skolt@datatilsynet.no.

Med vennlig hilsen

Jørgen Skorstad
Avdelingsdirektør

Kristin Skolt
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer