Personvernnemnda

PVN-2023-09 Brudd på personopplysnings- og informasjonssikkerheten i Karmøy kommune - overtredelsesgebyr

Personvernnemndas vedtak 7. november 2023 (Mari Bø Haugstad, Bjørnar Borvik, Hans Marius Graasvold, Ellen Økland Blinkenberg, Hans Marius Tessem, Morten Goodwin, Malin Tønseth)

Datatilsynets referanse: 21/03649-8

Saken gjelder klage fra Karmøy kommune på Datatilsynets vedtak 3. januar 2023 der kommunen ble ilagt et overtredelsesgebyr på 300 000 kroner for brudd på kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og artikkel 24, samt pasientjournalloven §§ 22 og 23.

Sakens bakgrunn

Karmøy kommune oppdaget 14. oktober 2021 at det var manglende tilgangskontroll i mappestrukturen i kommunens systemer. Mapper på systemets fellesområde (sikker sone) var opprettet på egen hånd av ansatte og enhetsledere i kommunens enheter uten at IKT-avdelingen ble involvert og fikk etablert tilgangskontroll på mappene.

Den mangelfulle tilgangskontrollen ble oppdaget da en ansatt i barneverntjenesten skulle demonstrere tilgangsstyringen i sikker sone og det viste seg at den ansatte likevel hadde tilgang til andre avdelingers mapper. Det dreide seg om totalt 60 mapper hvorav 25 mapper (noen med undermapper) inneholdt personopplysninger. Hendelsen omfatter omtrent 28 000 registrerte personopplysninger. Antall registrerte som er berørt var imidlertid færre enn 28 000 da samme registrert har personopplysninger registrert i flere mapper.

Opplysningene i mappene omfattet helseopplysninger, herunder blant annet opplysninger om kommunens brukere av rus- og psykiatritjeneste og hjemmetjeneste (medisinlister og sykehusinnleggelser). Behandlingen av opplysningene omfattes av pasientjournallovens saklige virkeområde, jf. pasientjournalloven § 3. For slike opplysninger følger det av pasientjournalloven § 22, jf. pasientjournalforskriften at den dataansvarlige og databehandleren blant annet skal «sørge for tilgangsstyring, logging og etterfølgende kontroll». Helseopplysninger tilhører gruppen særlig kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1.

Opplysningene var tilgjengelig for ansatte i sektor Helse og omsorg, også ansatte uten tjenstlig behov, i perioden fra 1. januar 2019 til 5. november 2021. Det reelle antallet ansatte med tilgang til mappene var 1 727. Alle hadde signert taushetserklæring. Det var ikke etablert noen funksjonalitet for logging av tilgang til mappestrukturen på sikker sone. Det er derfor ikke konstatert at ansatte faktisk har gjort urettmessig innsyn eller at personopplysninger er

blitt brukt til utenforliggende formål, og det er heller ikke mulig å kontrollere om dette har skjedd eller om personopplysninger har kommet på avveie.

Da avviket ble oppdaget iverksatte kommunen tiltak for å kartlegge omfanget av avviket, foretok en systematisk gjennomgang av mapper på fellesområdet og fjernet sensitive opplysninger fra mapper som lå åpne og flyttet dem til mapper med tilgangskontroll. Fra 5. november 2021 var det etablert en ny katalogstruktur med tilgangskontroll.

Kommunen anså risikoen for de berørte registrerte sine rettigheter og friheter ikke for å være høy, og så ikke behov for å varsle de berørte, jf. personvernforordningen artikkel 34.

Kommunen sendte avviksmeldinger til Datatilsynet 5. og 24. november 2021 og sendte ytterligere opplysninger om avviket i e-post til tilsynet 2. mai 2022.

Datatilsynet varslet Karmøy kommune 4. oktober 2022 om at tilsynet ville treffe slikt vedtak:

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

Kommunen ga sine merknader til varselet 21. november 2022. Datatilsynet traff 3. januar 2023 vedtak om overtredelsesgebyr i tråd med utsendt varsel.

Kommunen klaget rettidig på Datatilsynets vedtak 20. januar 2023. Klagen gjaldt overtredelsesgebyrets størrelse. Datatilsynet vurderte klagen, men fant ikke grunn til å endre sitt vedtak. Datatilsynet oversendte saken til Personvernnemnda 28. april 2023. I brev fra nemnda 4. mai 2023 fikk kommunen anledning til å komme med kommentarer. Kommunen har ikke inngitt kommentarer.

Saken ble behandlet i nemndas møte 7. november 2023. Personvernnemnda hadde følgende sammensetning: Mari Bø Haugstad (leder), Bjørnar Borvik (nestleder), Hans Marius Graasvold, Ellen Økland Blinkenberg, Hans Marius Tessem, Morten Goodwin og Malin Tønseth. Utredningsleder Anette Klem Funderud var også til stede.

Kort om Datatilsynets vedtak

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.

Det faktum at alle med tilgang til mappene på sikker sone har signert erklæring for taushetsplikt er ikke relevant. De ansatte skal ikke ha tilgang til personopplysninger de ikke har tjenstlig behov for, uavhengig av om den ansatte har taushetsplikt eller ikke.

Den etablerte praksisen i kommunen tyder på manglende rutinebeskrivelser for regulering av tilgangsstyring og manglende opplæring av ansatte. Tilsynet stiller også spørsmål ved om kommunens interne rutiner for å avdekke brudd på personopplysningssikkerheten er tilfredsstillende.

Datatilsynet ser positivt på de tiltakene kommunen nå har iverksatt, både strakstiltak og langsiktige tiltak.

Etter personvernforordningen artikkel 34 utløses plikten til å underrette de berørte personene dersom sikkerhetsbruddet medfører «høy risiko» for fysiske personers rettigheter og friheter. Datatilsynet er enig med kommunen i at kommunen ikke hadde underretningsplikt etter personvernforordningen artikkel 34.

Etter å ha konkludert med at Karmøy kommune har brutt personvernforordningen og fastslått at skyldkravet for å ilegge overtredelsesgebyr er oppfylt (uaktsomhet), går Datatilsynet gjennom de momentene tilsynet anser som relevante for vurderingen av om overtredelsesgebyr skal ilegges etter personvernforordningen artikkel 83 nr. 2 bokstav a til k. Datatilsynet kommer til at bruddet, som omfatter særlige kategorier opplysninger (helseopplysninger), er av så alvorlig karakter at det er nødvendig å ilegge et overtredelsesgebyr.

Datatilsynet ila kommunen et overtredelsesgebyr på 300 000. Tilsynet opprettholdt sin vurdering etter å ha mottatt klagen fra Karmøy kommune.

Karmøy kommunes syn i korte trekk

Klagen gjelder gebyrets størrelse. Den ilagte reaksjonen er for streng ved at gebyret er for høyt.

Hensynet til likebehandling tilsier en reduksjon av gebyret. Datatilsynet kunne hatt klarere retningslinjer for fastsettelse av gebyr ved noenlunde like overtredelser. Tilsynets praksis innebærer at gebyrer oppleves som strengere og mer virkningsfulle for mindre kommuner. Dette til tross for at de største kommunene har bedre forutsetninger for effektiv drift og lettere vil kunne rekruttere mer spesialisert kompetanse.

I Datatilsynets sak 18/03623, ble Oslo kommune Sykehjemetaten ilagt et gebyr på 500 000 kroner. Avviket i Oslo kommune var mer alvorlig enn i foreliggende sak. Pr. oktober 2022 var innbyggertallet i Karmøy kommune 42 541, i Oslo 707 531. Oslo kommune har 16 ganger større befolkning enn Karmøy kommune. Forskjellen gjenspeiles ikke i gebyret Karmøy er ilagt. Mindre økonomisk bæreevne tilsier et lavere gebyr. Det vil likevel oppleves virkningsfullt og avskrekkende. Tilsynet ila Karmøy kommune et gebyr som utgjør 60 % av det Oslo kommune ble ilagt, samtidig utgjør Karmøys befolkning ca. 6 % av Oslo kommunes. Når alt annet er noenlunde likt, innebærer det at reaksjonen overfor Karmøy kommune er 10 ganger strengere enn reaksjonen overfor Oslo kommune. Det skal være en sammenheng mellom virksomhetens omsetning og størrelse på gebyret, jf. artikkel 83 nr. 4.

I tilsynets sak 18/2140 ble Bergen kommune ilagt et gebyr på 1 600 000 kroner for brudd på personopplysningssikkerheten. I forhold til kommunenes innbyggertall er gebyret Karmøy kommune er ilagt en strengere reaksjon enn gebyret til Bergen kommune, til tross for at avviket i Bergen kommune var mer alvorlig.

Det må tas hensyn kommunens bruk av betydelige ressurser i forbindelse med avvikshåndteringen ved utmåling av gebyret, jf. artikkel 83 nr. 2 bokstavene f og k.

Karmøy kommune fastholder etter dette at det foreligger en forvaltningsmessig forskjellsbehandling mellom de avvikene som er nevnt ovenfor til hhv Oslo og Bergen kommune og det gebyret som nå er vedtatt overfor Karmøy kommune. Karmøy kommune mener at denne forskjellsbehandlingen ikke er saklig begrunnet. Det anføres videre at forskjellsbehandlingen ligger utenfor det skjønnsmessige spillerom Datatilsynet har ved fastsettelsen av slike gebyrer.

Kommunen kan heller ikke se at Datatilsynet har hensyntatt at Karmøy kommune i sitt svar på varselet redegjorde for at antall reelle tilganger for ansatte som hadde tilgang til opplysningene i avviket var en god del lavere enn først antatt (1 727 mot tidligere varslet 2 377). Ansatte med tilgang til sikker sone anses som helsepersonell og er underlagt taushetsplikt. Det reduserer risikoen for faktisk tilegnelse av opplysninger uten tjenstlig behov.

Personvernnemndas vurdering

Overtredelsesgebyr

Ved brudd på bestemmelser i personvernforordningen kan tilsynsmyndigheten ilegge overtredelsesgebyr, jf. artikkel 58 nr. 2 bokstav i, jf. artikkel 83. Overtredelse av artikkel 32 kan sanksjoneres med gebyr, jf. artikkel 83 nr. 4 bokstav a. Det samme gjelder brudd på artikkel 24, jf. personopplysningsloven § 26 som gir artikkel 83 nr. 4 tilsvarende anvendelse for overtredelser av blant annet denne bestemmelsen. For brudd på pasientjournalloven § 22 (informasjonssikkerhet) og § 23 (internkontroll) følger det samme av pasientjournalloven § 29.

Det følger av artikkel 83 nr. 1 at ileggelse av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Både ved vurderingen av om det skal ilegges gebyr og ved utmålingen av gebyret, skal det tas hensyn til momentene i personvernforordningen artikkel 83 nr. 2 bokstavene a til k.

Det er for denne vurderingen 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 aktuelle behandlingens 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. artikkel 9 nr. 1 og fortjener et særskilt vern, jf. forordningen artikkel 5 og forordningens fortalepunkt 51. At kommunen har behandlet helseopplysninger i strid med personvernreglene over en periode på nesten tre år, er i seg selv alvorlig, jf. forordningen artikkel 83 nr. 2 bokstav g.

Datatilsynet har lagt til grunn at kommunen ikke plikter å informere berørte brukere idet bruddet på personopplysningssikkerheten ikke medfører «høy risiko» for fysiske personers

rettigheter og friheter, jf. personvernforordningen artikkel 34. Nemnda slutter seg til tilsynets vurdering, og viser til at det er tale om et høyt, men likevel avgrenset antall ansatte i kommunen (innen sektoren helse og omsorg), som hadde tilgang til opplysningene uten tjenstlig behov. Alle har taushetsplikt.

Etter artikkel 83 nr. 2 bokstav b skal det videre legges vekt på hvorvidt overtredelsen ble begått forsettlig eller uaktsomt. Nemnda slutter seg til Datatilsynets vurdering av at det dreier seg om en uaktsom overtredelse. Det er imidlertid skjerpende at bruddet varte over en periode på nesten tre år og at kommunen ikke avdekket dette gjennom etablerte internkontrollrutiner i løpet av perioden.

Etter personvernforordningen artikkel 83 nr. 2 bokstav h skal det i hvert enkelt tilfelle tas behørig hensyn til:

> «på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen.»

Bestemmelsen er i tråd med det alminnelige strafferettslige prinsippet i norsk rett om at varsling og egenrapportering skal tillegges vekt ved reaksjonsfastsettelsen. Den konkrete vektleggingen vil imidlertid blant annet avhenge av hvor alvorlig overtredelsen er, og også sannsynligheten for at overtredelsen ville blitt oppdaget av tilsynsmyndigheten likevel. I dette tilfellet mener nemnda at det må vektlegges i formildende retning at den behandlingsansvarlige selv avdekket den ulovlige behandlingen og iverksatte tiltak for å unngå eller minimere skaden. I skjerpende retning legger nemnda vekt på at det tok tre uker fra kommunen oppdaget avviket til dette ble lukket. I samme retning trekker at avviket først ble meldt til Datatilsynet på dette tidspunktet, lenge etter fristen på 72 timer, jf. artikkel 33.

Det foreligger begrenset forvaltningspraksis om fastsettelse av gebyrets størrelse. De sakene Karmøy kommune har vist til i klagen viser også at nivået i sammenlignbare saker kan variere og ikke er helt entydig. Det følger av artikkel 83 nr. 4 at det ved utmåling av gebyr skal ses hen til virksomhetens omsetning. Overført til en kommune er nemnda enig i at det kan være relevant å se hen til kommunens økonomi og antallet innbyggere i en kommune når gebyret skal utmåles.

Karmøy kommune har blant annet vist til to saker der både Oslo og Bergen kommuner ble ilagt overtredelsesgebyr for brudd på noenlunde like overtredelser.

Datatilsynet har ved oversendelsen av saken til nemnda redegjort for sin vurdering av disse to sakene, samt for noen flere saker. Saken mot sykehjemsetaten i Oslo kommune gjaldt også lagring av helseopplysninger på et fellesområde hvor ansatte uten tjenstlig behov hadde tilgang. Datatilsynet uttaler at den var av større omfang, pågikk over lengre tidsrom (11 år) og med en høyere alvorlighetsgrad enn avvikssaken i Karmøy. Oslo kommune ble ilagt et overtredelsesgebyr på 500 000 kroner. I vurdering av utmåling av gebyret, uttales det som et moment at «Oslo kommune er landets største kommune etter innbyggertall og har tilsvarende økonomiske ressurser».

En annen sak gjaldt Bergen kommune, som ble ilagt et overtredelsesgebyr på 1 600 000 kroner. Saken i Bergen gjaldt en hendelse hvor filer med brukernavn og passord til over 35 000 brukere i Bergen kommune hadde ligget åpent tilgjengelig for elever. Det hadde vært

mulig å logge seg inn på skolens ulike informasjonssystem som en elev, ansatt eller administrator på skolen og dermed få opplysninger om elever og ansatte. Som et moment i utmålingen av gebyrets størrelse uttaler Datatilsynet at det er av betydning at «Bergen kommune er Norges nest største kommune målt i antall innbyggere» og at kommunen hadde et betydelig overskudd i foregående år.

Datatilsynet trekker også fram en sak der Moss kommune ble ilagt et overtredelsesgebyr på 500 000 kroner. Avviket omfattet brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet. Pasientopplysninger til over 2 000 registrerte var gjort tilgjengelige for ansatte uten tjenstlig behov og uten loggfunksjon. Avviket varte imidlertid kun i én måned. Tilsynet viser til at Moss kommune hadde et innbyggertall på 51 013 i 2022, som er ca. 10 000 flere personer enn Karmøy kommune.

Endelig viser Datatilsynet til saken som gjaldt Sykehuset Østfold (PVN-2021-16). Den saken gjaldt manglende tilgangsstyring av rapportuttrekk fra elektronisk pasientjournal i en periode på fem år. Det var 118 ansatte helsepersonell som hadde tilgang til opplysningene, hvorav flere ikke hadde tjenstlig behov. Nemnda uttalte at gebyret i utgangspunktet lå rundt 500 000 kroner. Det var da hensyntatt at overtredelsen delvis skjedde under gammel lov. Gebyret ble, på grunn av lang saksbehandlingstid, satt til 400 000 kroner.

Etter en konkret, samlet vurdering konkluderer nemnda med at et overtredelsesgebyr på 300 000 kroner står i et rimelig forhold til overtredelsen og virker tilstrekkelig avskrekkende. Datatilsynets gebyrfastsettelse anses å være i tråd med loven. Hensynet til likebehandling, samt kommunens størrelse og økonomi er ivaretatt i Datatilsynets vurdering.

Kommunens klage har ikke ført fram.

Vedtaket er enstemmig.

Konklusjon
Datatilsynets vedtak opprettholdes.

Oslo, 7. november 2023

Mari Bø Haugstad
Leder