Datatilsynet

HØYLANDET KOMMUNE
Vargeia 1
7877 HØYLANDET

Deres referanse	Vår referanse	Dato
19/7825-9-EJF	20/01879-7	20.09.2021

Vedtak om overtredelsesgebyr

Datatilsynet viser til tidligere korrespondanse om avviksmelding datert 20.11.2019.

Vi beklager den lange saksbehandlingstiden.

1. Vedtak om overtredelsesgebyr

Med hjemmel i personopplysningsloven § 26 og personvernforordningen artikkel 58 nr. 2 bokstav i, jf. artikkel 83, har Datatilsynet i dag fattet følgende vedtak:

> *Høylandet kommune ilegges et overtredelsesgebyr på 400 000 NOK – fire hundre tusen norske kroner – for brudd på kravene til sikkerhet ved behandlingen av personopplysninger, herunder særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 32 nr. 1 bokstav b og nr. 2, jf. artikkel 24.*

2. Saksgangen

Etter å ha mottatt avviksmeldingen den 20.11.2019, ba Datatilsynet om ytterligere opplysninger i saken ved brev av 21.02.2020.

Høylandet kommune besvarte ikke brevet. Vi sendte derfor en purring i brev datert 29.05.2020. Kommunen besvarte denne henvendelsen i brev av 08.06.2020.

I vårt brev av 20.10.2020 ble Høylandet kommune gitt forhåndsvarsel om vedtak om overtredelsesgebyr og pålegg.

Kommunen har uttalt seg til varselet i brev datert 26.11.2020.

3. Nærmere beskrivelse av avviket

Det aktuelle avviket oppsto ved en helsestasjon i helse- og omsorgstjenesten i Høylandet kommune og forekom i perioden 01.01.2018 til 15.11.2019.

Avviket knytter seg til at en ansatt fikk tilgang til flere bildefiler (Bitmap) da hun skulle opprette nye brevmaler og sette inn en bildelogo fra fil.

Helsestasjonen (og også skolehelsetjenesten i kommunen) benytter et system levert av CompuGroup Medical Norge AS (CGM). Den ansatte ved helsestasjonen logget seg inn på administrasjon (CGM admin).

Bildefilene den ansatte fikk tilgang til inneholdt sensitive opplysninger om personer som ikke har tilknytning til Høylandet kommune. Informasjonen omfattet opplysninger om reelle personers timeavtaler, svar på henvisning, epikrise og diverse undersøkelser.

4. Redegjørelser fra Høylandet kommune

Datatilsynet ba Høylandet kommune om en redegjørelse for kommunens eventuelle dialog med CGM om saken. Vi spurte også om hvilke tiltak kommunen hadde igangsatt i forbindelse med avviket.

I brev av 08.06.2020 forklarte kommunen at man på grunn av avvikets alvorlighetsgrad valgte ikke å kontakte CGM. Når det gjelder tiltak, hadde kommunen informert øvrige ansatte som benytter det aktuelle dataprogrammet om funnet, og de ansatte var bedt om å unngå åpning av Bitmap-filer som ikke er opprettet av Høylandet kommune.

I brev datert 26.11.2020 har kommunen uttalt seg til varselet om vedtak om overtredelsesgebyr og pålegg.

Høylandet kommune angir at de forsto at avviket var meget alvorlig. Kommunen fikk forståelsen av at avviket lå hos CGM som leverandør/databehandler og at avviket mest sannsynlig også berørte andre kommuner. Kommunen valgte derfor å varsle Datatilsynet og ikke CGM. Høylandet kommune beklager på det sterkeste at de ikke hadde god nok kunnskap om Datatilsynets rolle og at kommunen ved en feil unnlot å varsle CGM.

Etter å ha mottatt Datatilsynets varsel om vedtak, har kommunen vært i kontakt med CGM og varslet om avviket.

I brev til kommunen datert 26.11.2020, har CGM forklart hvilke tiltak som er gjennomført samt gitt en grundig begrunnelse for skadepotensialet. CGM påtar seg ansvaret for feilen som har oppstått og anser feilen som løst. Filene ble slettet umiddelbart. Årsaken til avviket ble oppdaget og skyldes et feil konfigurert script. Det fremgår at CGM ikke har mottatt melding om lignende avvik. Det finnes imidlertid ikke logger som kan utelukke at lignende åpning av bildefiler har forekommet.

Høylandet kommune angir at deres rolle som behandlingsansvarlig burde vært tydeligere for dem og mer avklart på det tidspunktet avviket ble oppdaget.

Når det gjelder kommunens rutiner for tilgangsstyring og skjerming av helseopplysninger, er det vist til at Høylandet kommune har tatt i bruk Compilo som internkontrollsystem. I systemet er det blant annet tatt inn prosedyrer for administrering av autorisasjoner, tilgang til

helseopplysninger og skjerming av disse samt system for melding om avvik. Kommunen har prosedyre for oppretting av databrukerkontrakt med alle ansatte som har tilgang til kommunens datanettverk.

Kommunen angir at en utfordring har vært å sikre kontinuitet i implementeringen av internkontrollsystemet i hele organisasjonen. Dette arbeidet er nå gitt høy prioritet, med spesielt fokus på å bevisstgjøre alle ansatte på informasjonssikkerhet og avvikshåndtering. Høylandet kommune har også inngått avtale med ekstern ekspertise som skal bistå med å øke kommunens forståelse av ansvaret som behandlingsansvarlig.

Høylandet kommune ber om at det ikke ilegges overtredelsesgebyr. Kommunen viser til arbeidet det er redegjort for. Videre viser kommunen til at andre kommuner som har brukt CGMs løsning har hatt tilgang til samme helseopplysninger uten at det har medført samme økonomiske konsekvens for dem.

5. Rettslig grunnlag

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57 flg.

5.1 Om lovvalg

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

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

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

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

Spørsmålet om lovvalg må altså vurderes ut fra hva som regnes som handlingstidspunktet. Det aktuelle avviket oppsto før ikrafttredelsen av nytt regelverk den 20.07.2018, men vedvarte frem til avviket ble oppdaget i november 2019. Handlingstidspunktet i denne saken har altså vedvart over tid og hovedsakelig i tiden etter at personopplysningsloven (2018) trådte i kraft. Det følger da av personopplysningsloven (2018) § 33 at saken skal vurderes etter denne loven.

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

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

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

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

5.2 Om helseopplysninger

Helseopplysninger om pasienter er en såkalt særlig kategori av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1. Denne typen opplysninger har ut fra sin karakter et særskilt krav på vern.

5.3 Grunnprinsippene

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 behandlingsansvarliges ansvar at prinsippene overholdes, og den behandlingsansvarlige skal kunne påvise dette, jf. artikkel 5 nr. 2.

5.4 Kravene til personopplysningssikkerhet og styringssystemer

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 (…).
>
> 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 behandlingsansvarliges ansvar særskilt.

5.5 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 annet ledd, fremgår det at Datatilsynet ved brudd på regelverket kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83. 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 artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

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 i vurderingen av 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.

6. Datatilsynets vurdering

6.1 Vurdering av avviket

Helseopplysninger skal ikke lagres slik at ansatte uten tjenstlig behov har tilgang til dem. I Høylandet kommune har bildefiler med helseopplysninger om personer uten tilknytning til kommunen vært tilgjengelige for ansatte ved en helsestasjon.

Kommunen oppdaget dette avviket, men gjorde ingen adekvate tiltak. En oppfordring til de ansatte om ikke å åpne de aktuelle bildefilene, er ikke et tilstrekkelig informasjonssikkerhetstiltak eller en tilfredsstillende avviksoppfølging. Dette tilsier at kommunen ikke har vært kjent med personvernregelverkets krav til personopplysningssikkerhet eller innholdet i behandlingsansvaret.

Som behandlingsansvarlig for helseopplysninger og andre personopplysninger må kommunen ha etablert rutiner som ivaretar kravene til personvern og informasjonssikkerhet. Rutinene må omfatte prinsipper for skjerming og tilgangsstyring. Det er et ledelsesansvar at rutiner er etablert og fungerer som forutsatt.

Vi mener at håndteringen av avviket tilsier at det har vært grunnleggende mangler ved Høylandet kommunes rutiner for skjerming av helseopplysninger ved den aktuelle helsestasjonen så vel som kommunens avvikshåndtering. Vi ser alvorlig på at kommunen ikke iverksatte adekvate tiltak da avviket ble oppdaget, herunder ikke søkte å avdekke hvordan opplysninger om personer uten tilknytning til kommunen hadde kommet inn i systemet.

Datatilsynet har kommet til at Høylandet kommune har brutt kravene til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. artikkel 24. Vi legger til grunn at rådmannen, som øverste ansvarlig for kommunen, har handlet uaktsomt og dels også forsettlig – se nærmere om dette under punkt 6.1 b) under.

Høylandet kommune har nå tatt i bruk internkontrollsystemet Compilo, hvor det er tatt inn prosedyre for tilgang til/skjerming av helseopplysninger og system for melding om avvik. Videre oppretter kommunen databrukerkontrakter med alle ansatte, og de ansatte gjøres samtidig kjent med kommunens prosedyrer og retningslinjer. Kommunen har prioritert arbeidet med implementering av rutinene for informasjonssikkerhet og avvikshåndtering, og kommunen har innhentet ekstern bistand.

På dette grunnlag har vi ikke funnet grunnlag for å gi pålegg om ytterligere tiltak til Høylandet kommune. Se imidlertid punkt 8 om krav om redegjørelse.

6.2 Vurdering av om overtredelsesgebyr skal ilegges
Datatilsynet har kommet til at kommunen har brutt personvernforordningen artikkel 24 og 32.

Lovbruddet har dels 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. I utgangspunktet er det dermed grunnlag for å ilegge kommunen et overtredelsesgebyr på inntil 10 000 000 euro (p.t. ca. 107 000 000 NOK), jf. forordningen artikkel 83 nr. 4. Vi vil se hen til at lovbruddene har skjedd også i perioden da tidligere personvernregelverk gjaldt.

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

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd
Avviket har pågått i nærmere to år, og helseopplysninger om et ukjent antall personer uten tilknytning til kommunen har ligget tilgjengelig for et ukjent antall ansatte uten tjenstlig behov for opplysningene. Det finnes ikke logg over området, er det er dermed umulig å avdekke hvorvidt, eller i hvilket omfang, ansatte eventuelt har fått urettmessig tilgang til informasjonen.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt
Vi anser det som uaktsomt at bildefiler med helseopplysninger om personer uten tilknytning til kommunen har blitt gjort tilgjengelige i systemet ved helsestasjonen. Det gikk lang tid før

det ble gjort tiltak for å fjerne bildefilene. Etter at avviket ble oppdaget, har dermed lovbruddet mer karakter av å være forsettlig.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd
Høylandet kommune iverksatte innledningsvis ingen tiltak utover å oppfordre ansatte til ikke å åpne de aktuelle bildefilene.

Først da kommunen mottok Datatilsynets varsel om overtredelsesgebyr og pålegg, det vil si ca. 11 måneder etter at avviket ble oppdaget, tok kommunen grep for å rette opp i situasjonen.

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
Høylandet kommune gjorde som nevnt ingen adekvate tiltak for å forhindre videre lovbrudd etter at avviket ble oppdaget. Vi mener dette taler i retning av grunnleggende mangler ved rutinene for skjerming av helseopplysninger og håndtering av avvik.

Senere har kommunen, ved hjelp av CGM, gjort et større arbeid for å rette opp i avviket.

f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den
Datatilsynet måtte purre på Høylandet kommune for å få svar på spørsmålene i vårt krav om redegjørelse. Kommunens første svarbrev bar også preg av at kommunen ikke forsto alvoret i og omfanget av avviket.

g) kategoriene av personopplysninger som er berørt av overtredelsen
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. Vi ser også alvorlig på at helseopplysningene gjaldt personer som er uten tilknytning til kommunen og at det var ukjent hvordan disse opplysningene har kommet inn i kommunens system.

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen
Høylandet kommune meldte selv fra om avviket til Datatilsynet.

Konklusjon
Datatilsynet har kommet til at Høylandet kommune skal ilegges et overtredelsesgebyr. I vurderingen har vi særlig vektlagt at det er tale om svært sensitive opplysninger og at kommunen ikke gjorde adekvate tiltak for å forhindre videre lovbrudd etter at avviket ble oppdaget. Kommunen forsto først alvoret i saken da de mottok vårt varsel om mulig overtredelsesgebyr og pålegg.

6.3 Utmåling av gebyret

I vurderingen av gebyrets størrelse, har vi sett hen til at Høylandet kommune ikke sørget for sletting av de aktuelle bildefilene eller gjorde tiltak for å forhindre lignende avvik før etter ca. 11 måneder. Adekvate tiltak ble først iverksatt etter at kommunen ble varslet om mulig overtredelsesgebyr og pålegg.
Etter vårt syn, har ikke kommunen håndtert avviket på en adekvat måte, og vi legger til grunn at kommunens rutiner for skjerming av helseopplysninger og avvikshåndtering ikke har vært tilstrekkelige.

Kommunen meldte selv avviket til Datatilsynet, noe som skal telle i kommunens favør. Det er heller ikke kjent at den manglende skjermingen av helseopplysninger har fått konkrete konsekvenser for enkeltpersoner, selv om dette tillegges mindre vekt.

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

Datatilsynet har kommet til at et overtredelsesgebyr på 400 000 NOK er rimelig i denne saken.

7. Klageadgang

Vedtaket om overtredelsesgebyr kan påklages **innen tre uker** etter at dere har mottatt dette brevet, jf. forvaltningsloven §§ 28 og 29.

En eventuell klage sendes til Datatilsynet. Dersom vi opprettholder vår avgjørelse, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

8. Krav om redegjørelse

Høylandet kommune har informert om det pågående arbeidet med å innarbeide nye rutiner for skjerming av personopplysninger og avvikshåndtering.

- Vi ber om en redegjørelse for status for dette arbeidet, herunder en redegjørelse for opplæringsplaner e.l.
- Videre ber vi om å få oversendt kopi av nye rutiner/retningslinjer som er relevante for denne saken, herunder databrukerkontrakten kommunen inngår med de ansatte.

Vi viser for ordens skyld til at Datatilsynet i medhold av personopplysningsloven § 23 og personvernforordningen artikkel 58 nr. 1 kan kreve de opplysningene vi anser nødvendige for å løse våre lovpålagte oppgaver.

Etter at redegjørelsen og dokumentasjonen er mottatt, vil vi ta stilling til om det er behov for videre tilsynsmessig oppfølging.

Hvis dere har spørsmål, kan dere ta kontakt med saksbehandler Susanne Lie (e-post suli@datatilsynet.no).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer