Datatilsynet

GRUE KOMMUNE
Postboks 94
2261 KIRKENÆR

Deres referanse	Vår referanse	Dato
24/128-21 / OFM	24/00754-6	21.10.2024

Vedtak om overtredelsesgebyr - Melding om avvik - Grue kommune

Vi viser til vårt varsel om vedtak om overtredelsesgebyr 4. september 2024. Vi mottok kommentarer til vårt varsel datert 12. september 2024 som har ført til at vi har redusert vårt varslede overtredelsesgebyr.

Saken gjelder en melding om brudd på personopplysningssikkerheten (avviksmelding) som Grue kommune sendte inn 12. februar 2024 og etterfølgende tiltaksrapport 21. februar 2024.

1. Vedtak om overtredelsesgebyr

Datatilsynet har i dag fattet følgende vedtak:

> *Grue kommune gis, i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, et overtredelsesgebyr til statskassen på 250 000 NOK – to hundre og femti tusen norske kroner*
>
> - *for ikke å ha gjennomført tilstrekkelige tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet til å oppnå vedvarende konfidensialitet, jf. personvernforordningen artikkel 32 nr. 1 bokstav b, jf. artikkel 24, jf. personopplysningsloven § 26 første ledd, og*
>
> - *for å ha publisert personopplysninger, herunder særlige kategorier av personopplysninger, på kommunens offentlige postjournal, uten rettslig grunnlag, jf. personvernforordningen artikkel 6, jf. artikkel 9.*

2. Beskrivelse av avviket

2.1 Generelt om avviket

Datatilsynet mottok melding om brudd på personopplysningssikkerheten 12. februar 2024 fra personvernombudet i Grue kommune.

Ifølge avviksmeldingen ble kommunen gjort oppmerksom på at det fantes to journalposter på offentlig postjournal med sensitive personopplysninger. Disse ble umiddelbart skjermet. De hadde da ligget offentlig tilgjengelig på postjournalen siden 16. januar 2024, altså en treukers periode.

De aktuelle journalpostene bestod av svarbrev fra Grue kommune til Statsforvalteren i forbindelse med et tilsyn knyttet til skolemiljø. Dokumentene inneholdt informasjon om såkalte 9A-vedtak[1], skolens aktivitetsplaner, møtereferater og korrespondanse mellom skolen og foreldre. Personopplysningene som er berørt av avviket er elevers navn, fødselsdato og sensitiv informasjon knyttet til 9A-vedtak. I fire tilfeller fremkom det personnummer til elever. I tillegg er foresattes telefonnummer og adresser omfattet av avviket. Antall berørte registrerte i disse to journalpostene inkluderer 14 elever og deres foreldre.

Etter nærmere gjennomgang av postjournalen tilbake til 2020, ble det avdekket ytterligere åtte avvik. Kommunen informerer om at disse avvikene omfatter personnummer eller kontonummer som fremkommer i ulike søknadsdokumenter. I ett tilfelle har kommunen mottatt brev fra politiet hvor det fremkommer et navn i en straffesak.

Totalt er det snakk om 14 elever og deres foreldre samt åtte øvrige registrerte.

Ifølge kommunen er det samlet sett grunn til å anta at det er et begrenset antall personer som har fått tilgang til opplysningene. Dette er basert på undersøkelser av digitale spor som har identifisert antall visninger av journalpostene. Eksempelvis er et av dokumentene med personopplysninger om elever vist 29 ganger gjennom innsyn, hvorav 20 av disse vurderes å være gjort i tilknytning til kommunens avvikshåndtering. Et annet dokument er vist 23 ganger gjennom innsyn, hvorav 11 av disse vurderes å være gjort i tilknytning til kommunens avvikshåndtering.

Årsakene til at avviket oppstod beskrives som menneskelig svikt og systemsvakhet. Arkivsystemet skjermer automatisk elevmapper, og ansatte har derfor oversett behovet for skjerming i journalmappene som var utenfor kategorien elevmappe. I tillegg opplyses det om at arkivsystemet ikke aktivt etterspør skjermingsinformasjon, men at dette aktivt må oppsøkes i en undermeny.

Grue kommune hadde på avvikstidspunktet rutiner for arkivering av brev. Det blir likevel informert om at manglende kunnskap og bevissthet om arkivsystemet kan ha vært en medvirkende årsak til at behovet for skjerming ble oversett.

2.2 Iverksatte og planlagte tiltak

Journalpostene ble skjermet raskt etter at kommunen ble oppmerksom på avvikene. Kommunen satte deretter i gang med et kontrollarbeid for å avdekke ytterligere avvik tilbake til 2020. Etter få dager ble det utarbeidet en tiltaksrapport som ble sendt til Datatilsynet og gjort tilgjengelig for offentligheten.

[1] Enkeltvedtak om elevers rett til et forsvarlig skolemiljø.

Kommunen hadde allerede før avvikstidspunktet et etablert system for informasjonssikkerhet, som i 2023 ble styrket med et felles samarbeidsområde for planer, rutiner og dokumentasjon tilknyttet informasjonssikkerhet og personvern.

Kommunen har videre revidert rutinene for arkivering av brev slik at disse automatisk blir merket som unntatt offentlighet. Det har også blitt utført en revisjon av prosedyre for kontroll av postjournalen. Databehandler er videre kontaktet for å se på mulige programforbedringer av funksjonalitet av arkivsystemet. Det er satt i gang tiltak for ytterligere opplæring av saksbehandlere som håndterer postlistene.

Kommunen informerte berørte registrerte gjennom personlig brev raskt etter avdekket avvik. Kommunen har også informert om avviket i lokalavis og på sine egne nettsider. Tiltaksrapporten er gjort offentlig tilgjengelig for innbyggerne på kommunens nettsider.

3. Relevante rettsregler

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

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

3.2 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, (…)

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 behandlingsansvarliges ansvar særskilt.

3.3 Kravene til et rettslig grunnlag

Etter artikkel 5 nr. 1 bokstav a skal enhver behandling av personopplysninger være lovlig. En forutsetning for at en behandling av personopplysninger er lovlig er at behandlingen har rettslig grunnlag i personvernforordningen artikkel 6 nr. 1.

Dersom det er tale om særlige kategorier av personopplysninger, for eksempel helseopplysninger, må i tillegg et av vilkårene i artikkel 9 nr. 2 være oppfylt for at opplysningene skal kunne behandles lovlig.

3.4 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i og personopplysningsloven § 26 annet ledd, 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 gebyret.
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. 5. De relevante delene av bestemmelsene lyder:

> «5. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 20 000 000 euro eller, dersom det dreier seg om et foretak, på opptil 4 % av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes:
>
> a. de grunnleggende prinsippene for behandling, herunder vilkår for samtykke, i henhold til artikkel 5, 6, 7 og 9»

I personopplysningsloven § 26 annet ledd legger til grunn at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83, jf. artikkel 83 nr. 7.

4. Datatilsynets vurdering

4.1 Vurdering av om regelverket er brutt

Avviket representerer et brudd på kravene til konfidensialitet. Personopplysninger som skulle vært skjermet er blitt gjort tilgjengelig for uvedkommende på kommunens offentlige postjournal. Hendelsen tydeliggjør at de tekniske og organisatoriske tiltakene ikke har vært

tilstrekkelige. Dette innebærer et brudd på kommunens plikt for å sørge for tilstrekkelig personopplysningssikkerhet i samsvar med personvernforordningen artikkel 32 og artikkel 24.

Personopplysningene som fremkom av 9A-vedtak (eksempelvis vedtak knyttet til skolemiljø og saker om mobbing mm.) og referat fra møter mellom foreldre og skolen var taushetsbelagt etter forvaltningsloven § 13 og skulle ikke vært offentliggjort på kommunens postjournal.

Helseopplysninger er definert som en særlig kategori av personopplysninger etter artikkel 9 og er som utgangspunkt forbudt å behandle. Publisering av opplysningene på postjournalen representerer et brudd på kravene til et rettslig grunnlag i personvernforordningen artikkel nr. 1 og artikkel 9 nr. 2.

I tillegg ble det publisert fødselsnummer til fire elever og fødselsnummer og/eller kontonummer i ulike søknadsdokumenter til kommunen. Det følger av personopplysningsloven § 12 at fødselsnummer og andre entydige identifikasjonsmidler bare kan behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering. Publisering av fødselsnummer på kommunens postjournal innebærer et brudd på kravene til rettslig grunnlag etter artikkel 6 nr. 1.

Oppsummering
Datatilsynet vurderer at det har vært manglende rutiner hos Grue kommune knyttet til behandling av personopplysninger på offentlig postjournal. Dette innebærer et brudd på personvernforordningen artikkel 32 og artikkel 24.

Som en konsekvens, ble taushetsbelagte personopplysninger publisert på offentlig postjournal. Dette innebærer et brudd på kravet til rettslig grunnlag i henhold til artikkel 6 nr. 1 og artikkel 9 nr. 2.

4.2 Vurdering av skyldkravet for ileggelse av overtredelsesgebyr

For at Datatilsynet skal kunne ilegge Grue 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.

Bestemmelsen om uaktsomhet er lovhjemlet i straffeloven § 22 som uttrykker at:

> «Den som handler i strid med kravet til forsvarlig opptreden på et område, og som ut fra sine personlige forutsetninger kan bebreides, er uaktsom».

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

I tiltaksrapporten som Grue kommune har utarbeidet står det at «[d]et kan enkelt fastslås at kommunen har gjort alvorlige feil i behandlingen av personopplysninger, og at det er kommunedirektøren som har overordnet ansvar for dette».

Kommunen har erkjent at de hadde mangelfulle interne rutiner for skjerming av opplysninger på offentlig postjournal. Vi legger til grunn at kravene til internkontroll og informasjonssikkerhet er et ledelsesansvar, jf. personvernforordningen artikkel 5 nr. 2.

Kommunen argumenterer i kommentarene til varselet for at den systemtilnærming de valgte i avvikshåndteringen ikke kan benyttes som et skjerpende moment i vurderingen av uaktsomhet. Kommunen skriver at de allerede før avviket hadde et system for informasjonssikkerhet, rutiner for postmottak og postjournal med internkontroll samt gjennomført opplæring av saksbehandlere.

Vi står likevel fast ved at skyldgraden ved lovbruddet anses som simpelt uaktsomt av kommunens ledelse. Avvikene omfatter ni lovbrudd over en periode på tre år. Årsakene til avvikene beskrives som saksbehandleres manglende kunnskap og bevissthet om arkivsystemet samt en systemsvakhet. Det er Grue kommunes ansvar å gi sine ansatte tilstrekkelig opplæring samt velge et arkivsystem som oppfyller de lovpålagte pliktene kommunen har på en hensiktsmessig måte.

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 simpelt uaktsomt.

Skyldkravet for å ilegge overtredelsesgebyr er dermed oppfylt.

4.3 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at Grue kommune har brutt personvernforordningen artikkel 32, artikkel 24, artikkel 6 nr. 1 og artikkel 9 nr. 2.

Nedenfor gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges, jf. personvernforordningen artikkel 83 nr. 2.

Vi har tatt hensyn til Grue kommunes kommentarer til vårt varsel om overtredelsesgebyr i det 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*

Det er tale om 14 berørte elever, i tillegg til deres foreldre, i alt omtrent 40 registrerte. I tillegg ble det avdekket at åtte ytterligere avvik med åtte registrerte hadde funnet sted mellom 2020 og 2023. Dette innebærer at et større antall registrerte er berørt av avviket.

Bruddet på personopplysningssikkerheten omfatter personopplysninger av sensitiv art i form av informasjon om skolens 9A-vedtak og referat fra møter mellom skole og foreldre. Kommunen har ikke presisert hvilke spesifikke typer av opplysninger som fremkommer i

disse dokumentene, men ifølge kapittel 9A i gammel opplæringslov, så gjelder dette opplysninger om elevens skolemiljø, mobbing, vold, diskriminering, bortvisning, skolebytte mm.

Datatilsynet ser alvorlig på at uvedkommende kan ha fått tak i taushetsbelagt informasjon som kan ha store konsekvenser for den enkelte elev, eksempelvis tap av omdømme og stigmatisering. Ifølge kommunen er det samlet sett grunn til å anta at det er et begrenset antall personer som har fått tilgang til opplysningene. Kommunen viser til at det kun var 10-20 eksterne nedlastninger innenfor avviksperioden, men vi mener det likevel er vanskelig å vite omfanget av spredningen av personopplysningene. Avviket representerer like fullt et lovbrudd, og bruddet har fremdeles gjort de registrerte ute av stand til å ha kontroll over sine egne personopplysninger.

Når det gjelder offentliggjøring av fødselsnummer og kontonummer, kan konsekvensene være store i form av identitetstyveri og/eller svindelforsøk.

b) Hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Vi viser til vår vurdering under punkt 4.2, der vi konkluderer med at overtredelsen betegnes som simpelt 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. Det har også blitt informert om hendelsen i lokale medier, og kommunen har publisert tiltaksrapport på sine nettsider med informasjon om avviket og iverksatte tiltak.

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

Årsaken til avvikene beskrives delvis som systemsvakhet, der databehandler muligens har vært en medvirkende årsak til lovbruddet.

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

Det kan ikke konstateres tidligere relevante overtredelser.

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

Grue kommune meldte raskt inn avviket etter det ble oppdaget og har sendt inn tilstrekkelig informasjon til tilsynsmyndigheten.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Avviket omfatter personopplysninger om elever som har vært involvert i 9A-vedtak om skolemiljø, mobbing etc. Det er også referater fra møter mellom foreldre og skole som har inneholdt sensitive opplysninger om elever. Helseopplysninger er definert som særlige kategorier av personopplysninger etter personvernforordningen artikkel 9 og er som et utgangspunkt forbudt å behandle. Dette innebærer at vi anser avviket som alvorlig.

I tillegg er det avdekket avvik i åtte tilfeller der fødselsnummer i søknadsdokumenter er gjort offentlig tilgjengelig. Fødselsnummer er ikke ansett å være en særlig kategori av personopplysninger, men er ifølge personopplysningsloven § 12 underlagt særlige krav for behandling.

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

Grue kommune sendte selv inn avviksmelding innenfor den lovpålagte fristen.

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 i denne saken.

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

Ikke relevant i denne 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»

Ikke relevant i denne saken.

Datatilsynets oppsummering og konklusjon

Datatilsynet ser positivt på at Grue kommune raskt meldte inn avviket til Datatilsynet samt informerte de berørte registrerte om avvikene. Kommunen satte i gang et omfattende kontrollarbeid og iverksatte tiltak for å forhindre liknende hendelser i fremtiden.

Vi ser imidlertid alvorlig på at det er publisert konfidensielle og taushetsbelagte opplysninger på internett. Det er tale om særlige kategorier av personopplysninger som omhandler 14 elever og deres foreldre. I tillegg ble det offentliggjort fødselsnummer og/eller kontonummer til syv registrerte samt informasjon om en person i en straffesak. Kommunen har undersøkt logg over eksterne nedlastninger innenfor avviksperioden og mener det samlet sett er et

begrenset antall personer som har fått tilgang til opplysningene på postjournalen. Dette er en formildende faktor, med begrenset betydning, siden vi mener det likevel ikke er mulig å vite det eksakte omfanget av spredningen av personopplysningene, og lovbruddet like fullt har vært til stede. Bruddet på personopplysningssikkerheten har gjort et betydelig antall registrerte ute av stand til å ha kontroll over sine personopplysninger.

Basert på en samlet vurdering, mener vi at avviket er av en så alvorlig karakter at det er nødvendig å ilegge Grue kommune et overtredelsesgebyr.

4.4 Gebyrets størrelse

I vurderingen av 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. artikkel 83 nr. 1.

Grue kommune har sendt kommentarer til varselet om vedtak angående utmålingen av overtredelsesgebyret. Kommunen mener Datatilsynet i større grad må ta hensyn til formildende omstendigheter, informasjon om skadeomfanget samt kommunens økonomi og størrelse. Vi vil vurdere kommunens anførsler fortløpende nedenfor.

Først og fremst har vi vektlagt at bruddet knytter seg til personopplysninger som er taushetsbelagte og til dels særlige kategorier av personopplysninger. Publisering av slike personopplysninger kan ha store konsekvenser for de berørte registrerte. Videre ser vi alvorlig på at det var mange berørte registrerte og at enkelte av opplysningene har vært tilgjengelige for uvedkommende siden 2020.

4.4.1 Formildende faktorer

Personvernforordningen artikkel 83 nr. 2 bokstav k legger til grunn at det skal tas hensyn til enhver formildende faktor ved utmåling av gebyrets størrelse. I vårt varsel tok vi hensyn til at Grue kommune raskt sørget for skjerming av personopplysningene som var offentlig tilgjengelige. Kommunen har også informert de registrerte i personlig brev, i tillegg til å ha informert offentligheten i lokalavisa og på kommunens nettsider. Kommunen satte i gang et omfattende kontrollarbeid for å avdekke ytterligere avvik etter at det første avviket ble oppdaget. På bakgrunn av dette utarbeidet kommunen en tiltaksrapport som ble gjort tilgjengelig for offentligheten.

Kommunen har gjort Datatilsynet oppmerksom på at det allerede er brukt store ressurser på å begrense skadevirkningene og for å forhindre gjentakelse i fremtiden. Datatilsynet har vektlagt dette i nedjusteringen av gebyret, se også vår vurdering av kommunens økonomi nedenfor.

4.4.2 Kommunens grad av skyld

Datatilsynet har vurdert at kommunens ledelse har utvist simpel uaktsomhet, jf. vår vurdering under punkt 4.2. Grue kommune argumenterer for at de allerede før avviket hadde etablert et

system for informasjonssikkerhet, rutiner for postmottak og postjournal med internkontroll, samt gjennomføring av relevant opplæring for saksbehandlere. Årsakene til avvikene beskrives som saksbehandleres manglende kunnskap og bevissthet om arkivsystemet, samt en systemsvakhet.

Vi understreker at det er Grue kommunes ansvar å gi sine ansatte tilstrekkelig opplæring samt velge et arkivsystem som kan oppfylle de lovpålagte pliktene kommunen har på en hensiktsmessig måte. Vi mener vi i tilstrekkelig grad tok hensyn til kommunens lave skyldgrad i vårt varsel om vedtak.

4.4.3 Skadeomfanget

I forbindelse med avvikshåndteringen, undersøkte kommunen logg over eksterne nedlastninger i løpet av avviksperioden. Kommunen argumenterer for at det samlet sett er et begrenset antall personer som har fått tilgang til opplysningene på postjournalen og at dette må ha betydning for utmåling av gebyret.

Datatilsynet ser positivt på at kommunen har en fungerende loggkontroll og at kommunen har oversendt informasjon om eksterne nedlastninger til tilsynet. Vi mener likevel at det er vanskelig å vite i hvilket omfang personopplysningene har blitt spredd, og vi fastholder vår vurdering om at bruddene har gjort den registrerte ute av stand til å ha kontroll over sine egne personopplysninger.

Kommunen har videre argumentert for at kommunens størrelse må hensyntas i utmåling av beløpet. Datatilsynet vurderer at et innbyggertall på ca. 4 500 personer[2] vil begrense det potensielle skadeomfanget og risikoen for spredning av personopplysningene. Vi mener dette taler for en nedjustering av det varslede beløpet.

4.4.4 Kommunens størrelse og økonomiske situasjon

Det følger av personvernforordningen artikkel 83 nr. 5 at det ved utmåling av gebyr skal ses hen til virksomhetens omsetning. Overført til en kommune, har Personvernnemnda i sak PVN-2023-09 uttalt at det er «relevant å se hen til kommunens økonomi og antallet innbyggere».

Grue kommune informerer om at de er en liten kommune med dårlig økonomi og at et overtredelsesgebyr på 400 000 kroner vil bidra til å gjøre en allerede svært krevende økonomisk situasjon enda vanskeligere.

Datatilsynet ser positivt på at kommunen har tatt avviket på alvor og brukt ressurser på å iverksette omfattende kontrollarbeid og forbedring av rutiner.

Vi mener at hensynet til kommunens størrelse og økonomiske situasjon taler for en nedjustering av det varslede overtredelsesgebyret. Vi bemerker at en reduksjon av

[2] Grue – kommune i Innlandet – Store norske leksikon (snl.no)

overtredelsesgebyret fremdeles må være virkningsfullt overfor kommunen og virke avskrekkende i hvert enkelt tilfelle, jf. artikkel 83 nr.1.

I avvikssak med referanse 20/01984, ble Askim kommune (nå Indre Østfold kommune) ilagt et overtredelsesgebyr på 200 000 kroner for å ha publisert en elevmappe på offentlig postjournal. Elevmappen inneholdt personopplysninger som var underlagt taushetsplikt. Askim kommune hadde i 2019 et innbyggertall på 15 865, ifølge Store Norske leksikon.[3] Avvikssaken i Grue kommune vurderer vi som mer alvorlig, da kommunen publiserte dokumenter tilknyttet skolemiljø som berører 14 elever og deres foresatte. I tillegg ble det oppdaget åtte ytterligere avvik der personnummer eller kontonummer var blitt offentliggjort på internett.

Etter en samlet vurdering har Datatilsynet kommet til at det er rimelig å nedjustere overtredelsesgebyret til 250 000 NOK.

5. 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.

Dersom dere har spørsmål, kan dere kontakte oss på e-post postkasse@datatilsynet.no.

Med vennlig hilsen

Camilla Nervik
seksjonssjef

Kristin Skolt
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

[3] Askim – tidligere kommune – Store norske leksikon (snl.no)