Datatilsynet

LILLESTRØM KOMMUNE
SENTRALADMINISTRASJON
Postboks 313
2001 LILLESTRØM

Deres referanse	Vår referanse	Dato
	21/03177-5	02.02.2022

Vedtak om overtredelsesgebyr - Lillestrøm kommune Sentraladministrasjonen

1. Innledning

Vi viser til innsendt melding av 29. september 2021 om brudd på personopplysningssikkerheten, samt oppfølgende melding av 1. oktober 2021, varsel om vedtak om overtredelsesgebyr av 12. november 2021 og deres tilsvar av 3. desember 2021.

Datatilsynet ser at Lillestrøm kommune har flere av rutinene på plass, men kan ikke se at det er laget rutiner for etterkontroll, dvs. at man ikke har rutiner for kontroll av dokumenter som allerede er lagt ut på kommunens hjemmeside. Denne type rutiner er viktig for å sikre at personvernregelverket etterleves og for å oppdage avvik. På grunn av opplysninger i deres tilsvar finner Datatilsynet grunn til å nedjustere skyldkravet fra grovt uaktsomt til uaktsomt. Dette får betydning for overtredelsesgebyrets størrelse, som etter vår nye vurdering settes til 300 000 kroner.

Ut fra opplysningene i saken, mener Datatilsynet at Lillestrøm kommune har overtrådt reglene om personopplysningssikkerhet i personvernforordningen:

> *Lillestrøm kommune pålegges i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, å betale et overtredelsesgebyr til statskassen på* ***300 000 – tre hundre tusen – kroner***
>
> - *for ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet til å oppnå vedvarende konfidensialitet i behandlingssystemene og tjenestene jf. personvernforordningen artikkel 32 nr. 1 bokstav b), jf. artikkel 5, og*
> - *for å ha publisert personopplysninger på kommunens hjemmeside uten behandlingsgrunnlag, jf. personvernforordningen artikkel 6, jf. artikkel 5.*

Bakgrunnen og begrunnelsen for det varslede vedtaket følger under.

2. Saksforholdet

Datatilsynet mottok 29. september 2021 en melding om brudd på personopplysningssikkerheten fra Lillestrøm kommune. Kommunen har publisert et dokument på offentlig journal hvor 10 av 21 vedlegg inneholdt personopplysninger av særlige kategorier, jf. artikkel 9 nr. 1. Kommunen glemte å merke de 10 aktuelle vedleggene unntatt offentlighet slik de skulle. Heller ikke saksbehandler oppdaget dette. Dokumentet har vært gjennom ytterligere to manuelle kvalitetskontroller i dokumentasjonssenteret uten at feilen ble oppdaget.

Kommunen ble gjort oppmerksom på at dokumentet med vedlegg var tilgjengeliggjort på kommunens hjemmeside fra 27. september til 28. september av en journalist i lokalavisen Romerikes Blad. Undersøkelser viste at fire ulike IP-adresser (deriblant Romerikes Blad) har aksessert dokumentet. Dokumentene ble fjernet fra postlisten og unntatt offentlighet umiddelbart etter at hendelsen ble oppdaget. Deretter ble de berørte varslet.

3. Lovovertredelsen

Avvikene gjelder brudd på konfidensialitet, jf personvernforordningen artikkel 32. Personopplysninger som skulle vært skjermet er blitt gjort tilgjengelig for uvedkommende på internett, bl.a. av en journalist i lokalavisen Romerikes Blad. Dette gjelder opplysninger om

- Navn og fødselsdato på elev
- Navn og adresse til foresatte
- Skolens beskrivelse og vurderinger av elevens oppførsel og utfordringer
- Foreldrenes beskrivelse av eleven
- Elevens egen beskrivelse av hvordan han/hun har det hjemme og på skolen
- Elevens resultat på tester og kartlegginger
- Andre offentlige instansers vurderinger av eleven
- Eventuelle diagnoser. Eksempelvis dysleksi eller ADHD, som eleven har
- Konkret vurdering av hvor mye spesialundervisning elevene har behov for, og hvordan den bør gjennomføres for å ha effekt

Hendelsen vil innebære brudd på personvernforordningen artikkel 32 nr. 1 bokstav b, som krever at det etableres et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet. Når et dokument med vedlegg om en elev publiseres på kommunens hjemmeside er det tydelig at det ikke er etablert et slikt sikkerhetsnivå, eventuelt at det ikke fungerer etter hensikten. At hendelsen ikke oppdages av kommunen, men av en tredjepart, her Romerikes Blad, tyder også på mangelfulle rutiner på dette området.

Hendelsen omfatter personopplysninger som er taushetsbelagt etter forvaltningsloven § 13 nr. 1. Etter offentlegforskrifta § 7 er det ikke tillatt å publisere taushetsbelagte personopplysninger på internett. Dokumentet ble tilgjengeliggjort på kommunens hjemmeside (internett). Konsekvensen for eleven er at dokumentet kan ha blitt sett eller lastet ned av uvedkommende, som kan spre disse videre.

Offentleglova § 10 tredje ledd og offentlegforskrifta § 7 første ledd slår fast at virksomheter som er omfattet av loven kan publisere dokumenter for allmenheten på internett. Det er opp til

den enkelte virksomhet å bestemme om dette skal skje. Offentlegforskrifta § 7 andre ledd regulerer hvilke personopplysninger som ikke kan publiseres på internett. Blant annet vil dette gjelde personopplysninger som er underlagt taushetsplikt, fødselsnummer og særlige kategorier av opplysninger som følger av personvernforordningen artikkel 9 og 10.

Dokumentet med vedlegg, som ble lagt ut på kommunens hjemmeside, var underlagt taushetsplikt. Hvis det publiseres personopplysninger på internett som ikke er tillatt etter offentlighetsloven, vil personvernforordningen komme til anvendelse. Dette innebærer at kommunen må ha behandlingsgrunnlag etter personvernforordningen artikkel 6 for å kunne publisere slike opplysninger.

Når personopplysninger ved lov ikke er tillatt publisert på internett vil ingen av de øvrige vilkårene for å etablere et gyldig behandlingsgrunnlag etter personvernforordningen være oppfylt.

4. Vurdering av personvernforordningens regler om overtredelsesgebyr

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

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

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

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

Det følger av ordlyden i straffeloven § 27 og av forarbeidene til bestemmelsen at det gjelder et objektivt straffansvar for foretak. Høyesterett har lagt til grunn at objektivt ansvar for foretaksstraff ikke er forenlig med straffebegrepet i Den europeiske menneskerettskonvensjon artikkel 6 nr. 2 og artikkel 7, slik det nå er fastlagt i Den europeiske menneskerettsdomstols storkammerdom 28. juni 2018 G.I.E.M. S.r.l. med flere mot Italia. For å eliminere motstriden med EMK må foretaksstraff kunne ilegges ved ordinær uaktsomhet.

I brev av 2. juni 2021 har Kommunal- og moderniseringsdepartementet oversendt Justis- og beredskapsdepartementets orientering av 12. mai 2021 om betydningen av denne høyesterettsdommen for administrative sanksjoner. Justis- og beredskapsdepartementet uttaler følgende:

> «I påvente av utredningen om foretaksstraff og eventuelle forslag til lovendringer, anbefaler vi at departementene orienterer sine underliggende etater om Høyesteretts avgjørelse, og at denne inntil videre legges til grunn også ved ileggelse av overtredelsesgebyr overfor foretak. Dette innebærer at det ved ileggelse av overtredelsesgebyr overfor foretak stilles krav om at den som har opptrådt på vegne av foretaket har utvist alminnelig uaktsomhet.»

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

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

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

Bruddet på personopplysningssikkerheten omfatter 10 av vedleggene i et dokument. Dette gjelder opplysninger om eleven som nevnt i pkt. 3.

Når kommunen aktivt har besluttet at postlister og dokumenter i fulltekst skal publiseres på kommunens hjemmeside er det en viss fare for uønskete hendelser, f.eks. ved at opplysninger som det ikke er tillatt å publisere likevel blir det. For å få et sikkerhetsnivå som evner å sikre vedvarende konfidensialitet må kommunen gjennomføre egnede tekniske og organisatoriske tiltak. Dette har kommunen ikke gjort.

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll over opplysninger om seg selv, og hvorvidt andre har fått tilgang til opplysninger om vedkommende. Dokumentet inneholdt personopplysninger av personlig karakter som etter forvaltningsloven § 13 nr. 1 er underlagt taushetsplikt.

Bruddet på personopplysningssikkerheten ble oppdaget av en ekstern part. Det tyder på mangelfull rutine, i forbindelse med etterkontroll, for å fange opp slike brudd.

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

Bruddet på personopplysningssikkerheten har medført at konfidensielle opplysninger er publisert på internett. En slik hendelse kan få store personvernkonsekvenser for den berørte,

ved at opplysningene kan bli kjent for tredjeparter. At saken beror på menneskelig svikt endrer ikke på kommunens ansvar. Ved å publisere fulltekstdokumenter på internett har kommunen etablert en rutine som krever et ekstra høyt sikkerhetsnivå.

Angjeldende sak indikerer at opplæring/ansvarliggjøring ikke har hatt den ønskede virkning, og at man da må vurdere andre tiltak for å sikre seg mot slike brudd på personopplysningssikkerheten.

Datatilsynet er kommet til at Lillestrøm kommune ved sentraladministrasjonens øverste leder har opptrådt uaktsomt, jf. HR-2021-797-A, jf. personvernforordningen artikkel 5 nr. 2.

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.

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***

Noen organisatoriske tiltak var etablert. Datatilsynet kan imidlertid ikke konstatere at tiltak for etterkontroll var omfattet av disse.

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***

Dette er ikke relevant i saken.

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

Dette gjelder opplysninger om eleven som nevnt under pkt. 3.

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

Datatilsynet fikk kunnskap om dette gjennom innmeldt brudd på personopplysningssikkerheten 29. september 2021.

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***

Det har ikke tidligere vært gjennomført tiltak overfor Lillestrøm kommune med hensyn til samme saksgjenstand.

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

Brudd på atferdsnormer har ikke vært tema i avviket.

k) ***enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen***

Datatilsynet har ikke konstatert at Lillestrøm kommune har hatt økonomiske fordeler, eller unngått direkte eller indirekte tap som et resultat av overtredelsen. Det kan heller ikke anføres andre forhold i formildende retning.

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

5. Samlet vurdering

Datatilsynet ser positivt på at Lillestrøm kommune raskt tok grep da den usikre lagringen ble oppdaget samt meldte fra om avviket til Datatilsynet. Kommunen har også iverksatt tiltak som skal forhindre lignende lovbrudd i fremtiden. Det er imidlertid alvorlig at konfidensielle personopplysninger er publisert på kommunens hjemmeside. Det er kommunens ansvar å påse at slike hendelser ikke skjer.

Etter Datatilsynets vurdering, er saken imidlertid prinsipielt viktig. Lillestrøm kommune burde ha vært rustet til å ivareta kravene til personopplysningssikkerhet ved publisering av postlister på deres hjemmeside. I dette henseende kan et vedtak om overtredelsesgebyr gi en viktig signaleffekt.

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

6. Gebyrets størrelse

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

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

Departementet skriver videre at det har notert seg bekymringen som enkelte offentlige høringsinstanser har uttrykt, men departementet legger til grunn at det innenfor reglene i

forordningen artikkel 83, som også angir de momenter det skal legges vekt på ved utmålingen av administrative gebyrer, ligger rom for et betydelig skjønn med hensyn til størrelsen på gebyret. Departementet uttaler at «[b]eløpsgrensene i forordningen artikkel 83 angir maksimalgrenser for utmåling av administrative gebyrer, mens det ikke er fastsatt noen minimumsgrenser.»

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

Vi har særlig sett hen til at bruddet på personopplysningssikkerheten er knyttet til et dokument hvor konfidensialitet er påkrevd. Publisering vil kunne medføre store personvernkonsekvenser for den berørte. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale instanser følger de regler som er gitt, og særlig de som gir enkeltindivider rettigheter som er ment å være en beskyttelse mot utlevering av denne typen opplysninger.

Signalvirkningen av denne saken og de allmennpreventive hensyn, mener vi er tydelige. Det er viktig at slike hendelser ikke inntreffer, og at alle offentlige instanser som behandler innbyggernes personopplysninger og opplysninger om sårbare personer, må være seg sitt ansvar bevisst.

Etter en totalvurdering av saken, og da særlig sett hen til alvorligheten i overtredelsen og lovverkets krav om at ileggelsen av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende, har vi kommet til at et overtredelsesgebyr på **300 000 NOK** anses som riktig.

7. Klage

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer