Datatilsynet

ASKER KOMMUNE
Katrineåsveien 20
3440 RØYKEN

| Deres referanse | Vår referanse | Dato |
|---|---|---|
| 20/11347-143 | 20/01516-8 | 15.03.2021 |

## Vedtak om overtredelsesgebyr - Asker kommune - Melding om avvik

### 1. Innledning

Vi viser til innsendt melding av 20. mai 2020 om brudd på personopplysningssikkerheten, oppfølgende brev av 22. mai 2020, hvor Asker kommune tilkjennegir at de ser alvorlig på hendelsen, og at de i den forbindelse ønsker at Datatilsynet gjennomfører et stedlig tilsyn, samt kommunens tilsvar av 18. desember 2020.

For ordens skyld gjør Datatilsynet oppmerksom på at stedlig tilsyn ikke er aktuelt på nåværende tidspunkt. Dette skyldes den generelle situasjonen knyttet til den eksisterende pandemien i landet.

*Asker kommune pålegges i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83, å betale et overtredelsesgebyr til statskassen på **1 000 000** – én million – kroner*

- *for å ha publisert personopplysninger på kommunens hjemmeside uten behandlingsgrunnlag jf. personvernforordningen artikkel 6 jf. artikkel 5, og*
- *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 ikke å ha tilfredsstillende rutiner for håndtering av postlistene på internett, jf. personvernforordningen artikkel 24 jf. personopplysningsloven § 26 første ledd.*

Bakgrunnen og begrunnelsen for vedtaket følger under.

### 2. Saksforholdet

Datatilsynet mottok 20. mai 2020 en melding om brudd på personopplysningssikkerheten fra Asker kommune. Kommunen har på sin hjemmeside publisert taushetsbelagte personopplysninger. I tillegg har kommunen publisert 127 fødselsnummer (alle elleve siffer) på hjemmesiden.

Utgangspunktet for hendelsen var at kommunen ble varslet 19. mai 2020 av en privatperson om at dokumenttitler fra kommunens postlister inneholdt 127 navn og fødselsnummer i til sammen 170 journalposter. Opplysningene som var tilgjengelige var, i tillegg til navn og fødselsnummer, tittel på dokumentet. Flere av sakene gjelder barn, og omfatter forhold fra 2009 til 2014. I enkelte tilfeller har dette medført at også taushetsbelagte opplysninger er blitt offentliggjort, f.eks. i forbindelse med vedtak om PPT, spesialundervisning og boligtilskudd. Selve dokumentet har ikke vært offentlig tilgjengelig. Dokumenttitlene på de omtalte sakene ble umiddelbart fjernet fra kommunens nettsider.

Kommunen har også gjort undersøkelser for å se om det er flere tilfeller av urettmessig publisering av personopplysninger i postlistene enn hva som fremkommer av varselet. Kommunen opplyser at det er gjort enkelte funn, men at kommunen vil fortsette med videre undersøkelser.

I tillegg omfatter avviket 43 dokumenttitler om 33 ansatte fra 2018 - 2019. Bruddet på personopplysningssikkerheten har oppstått som resultat av at rutiner ikke har blitt fulgt. Postlistene korrekturleses av to personer hver dag. Likevel har kommunen ikke oppdaget avvikene. Kommunen opplyser at den ikke har hatt rutiner for å ta stikkprøver i gamle postlister.

## 3 Lovovertredelsen

Avvikene gjelder brudd på personopplysningsregelverkets krav om konfidensialitet. Personopplysninger som skulle vært skjermet er blitt gjort tilgjengelig for uvedkommende på kommunens hjemmeside. Personopplysningene som omfattes av bruddet er fødselsnummer og tittel på dokumentet. I dokumenttittelen synliggjøres det at flere av sakene omfatter barn. I enkelte tilfeller har dette medført at også taushetsbelagte personopplysninger er blitt offentliggjort, f.eks. i forbindelse med vedtak om PPT, spesialundervisning og boligtilskudd, samt andre opplysninger av konfidensiell karakter.

Dette utgjør 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 postlistene publiseres på kommunens hjemmeside er det tydelig at det ikke er etablert et slikt sikkerhetsnivå. At hendelsen ikke oppdages av kommunen, men av en privatperson tyder også på mangelfulle rutiner for å oppdage slike hendelser.

Hendelsen omfatter personopplysninger som er taushetsbelagt etter forvaltningsloven § 13 nr. 1. Etter offentlegforskrifta § 7 er det ikke tillatt å publisere fødselsnummer og taushetsbelagte personopplysninger på internett. Konsekvensen for de berørte kan ha blitt at postlisten er blitt 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.

Personopplysninger som fremkommer av postlistene, 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 et egnet behandlingsgrunnlag etter personvernforordningen artikkel 6 for å kunne publisere slike opplysninger.

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

I tillegg vil praksisen kunne være et brudd på artikkel 24, da etablerte rutiner for håndtering av postlistene er mangelfulle.

**4 Hvilket regelverk skal anvendes**

Den nye personopplysningsloven (personopplysningsloven 2018), som i § 1 inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20. juli 2018. Loven opphevet samtidig lov 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven 2000) og reglene i forskrift 15.12.2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften 2000). På grunn av sakens hendelsesforløp, er det nødvendig å ta stilling til om saken skal vurderes etter personopplysningsloven 2018 eller personopplysningsloven 2000.

Vi har kommet til at personopplysningsloven av 2018 må anvendes i saken. Dermed kommer også bestemmelsene i personvernforordningen til anvendelse, jf. lovens § 1. Dette gjelder alle sakens sider, også de som gjelder ileggelse av overtredelsesgebyr, jf. også personopplysningsloven § 26 andre ledd og § 33.

Denne saken gjelder brudd på regelverket som har oppstått på et tidspunkt forut for ikrafttredelsen av personopplysningsloven 2018. Regelverksbruddene har imidlertid vært kontinuerlige og har vedvart i tid, og ble oppdaget den 19. mai 2020, altså etter ikrafttredelsestidspunktet til den nye personopplysningsloven. De aktuelle hendelsene har med andre ord strukket seg over en lengre periode, fra 2004 til 2020. På tidspunktet før 20. juli 2018 gjaldt personopplysningsloven 2000 og personopplysningsforskriften 2000. Forskriften §§ 2-6, 2-11, 2-13 og 2-14 regulerte slike forhold som saken omhandler.

De aktuelle forholdene som er til vurdering, har altså oppstått før ikrafttredelsen av personopplysningsloven 2018, men de har vedvart og vært kontinuerlige en tid etter at den nye personopplysningsloven lov trådte i kraft den 20. juli.

Personopplysningsloven 2018 § 33 første ledd nedfeller en særskilt overgangsregel om overtredelsesgebyr som lyder som følger:

> «*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*.»

Når det treffes vedtak om overtredelsesgebyr skal altså spørsmål om lovvalg vurderes ut fra hva som må regnes som *handlingstidspunktet*. Datatilsynets vurdering er at handlingstidspunktet i denne saken er utstrakt i tid – den eller de lovstridige handlingene har oppstått før den 20. juli, men det har dreid seg om, og vil fortsette å dreie seg om, et konstant og kontinuerlig regelverksbrudd helt til den behandlingsansvarlige sørger for å bringe behandlingsaktivitetene i samsvar med regelverkets krav.

Ettersom den behandlingsansvarlige ikke har foretatt seg noe for å sørge for å bringe de ulovlige behandlingsaktivitetene til opphør og i samsvar med regelverkets krav før i august i år, må handlingstidspunktet i § 33 anses å være etter ikrafttredelsestidspunktet til den nye personopplysningsloven. Det følger dermed av personopplysningsloven § 33 at denne saken skal vurderes etter personopplysningsloven 2018. Dette er for øvrig også i samsvar med EMK art 7, som viser til hhv. «handlingstidspunktet» og «den tid da [handlingen] ble begått».

Vi viser også til forarbeidene til personopplysningsloven 2018 (Prop. 56 LS (2017-2018) side 196), hvor departementet blant annet uttaler følgende om spørsmål 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 ikke gjelder overtredelsesgebyr og som oversendt nemnda før ny lov, men som behandles etter ny lov. Se for eksempel PVN-2018-005 og PVN-2018-006.

På denne bakgrunn vurderer vi det som klart at saker som gjelder løpende eller vedvarende brudd på reglene må vurderes etter personopplysningsloven 2018 og personvernforordningen.

## 5 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).

For foretak er skyldvurderingen særegen. I forvaltningsloven § 46 (1) 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».

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 personopplysninger om minst 120 personer, og omfatter 170 dokumenter i perioden 2004 – 2020.

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll på opplysninger om seg selv, og hvorvidt andre har sett opplysninger om vedkommende. Det føres ikke logg på hvem som er inne og ser eller laster ned personopplysninger fra kommunens postliste. Postlistene inneholdt personopplysninger av konfidensiell karakter. Noen av personopplysningene er underlagt taushetsplikt, bl.a. gjelder dette vedtak om PPT, spesialundervisning og boligtilskudd.

Datatilsynet ser alvorlig på at kommunen ikke har hatt rutiner som kunne ha bidratt til at bruddet ble oppdaget. Videre anser vi det også som meget alvorlig at lovbruddet har foregått over 16 år.

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

Datatilsynet finner det kritikkverdig at kommunen har publisert opplysninger om innbyggere i kommunen hvor konfidensialitet er påkrevd. Til tross for rutiner har bruddet skjedd på grunn av menneskelig svikt. Dessuten har man hatt utilstrekkelige rutiner for å avdekke de forhold som er nevnt i avviksmeldingen, noe kommunen selv innrømmer.

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.

Hendelsen er alvorlig, og må betegnes som grovt uaktsomt.

*c)* ***eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd***

Kommunen opplyser at de vil ta kontakt med de berørte så snart som mulig.

*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***

Behandlingsansvarlig er ansvarlig for manglende organisatoriske og tekniske tiltak som er egnet for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

*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***

Det kan konstateres at særlige kategorier av opplysninger har vært publisert på kommunens hjemmeside, bl.a. vedtak om PPT, spesialundervisning og boligtilskudd. Selve dokumentene det refereres til er imidlertid ikke blitt offentliggjort.

*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 20. mai 2020.

*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 Asker 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 Asker kommune har hatt økonomiske fordeler, eller unngått direkte eller indirekte tap som et resultat av overtredelsen. Det kan heller ikke anføres noe i formildende retning.

## 6 Samlet vurdering

Vi viser til innsendt melding av 20. mai 2020 om brudd på personopplysningssikkerheten. Datatilsynet ser positivt på at Asker 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.

Etter Datatilsynets vurdering, er saken imidlertid prinsipielt viktig. Asker kommune burde 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.

Kommunen har blant annet ikke hatt rutiner for å ta stikkprøver i gamle postlister, noe kommunen opplyser i avviksmeldingen. Dette er også en konsekvens av at bruddet på personopplysningssikkerheten ble oppdaget av en privatperson.

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

## 7 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 de 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 en behandling av personopplysninger hvor konfidensialitet er påkrevd, og at dette har skjedd over en periode på 16 år. 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.

Vi viser til de allmennpreventive hensynene og signalvirkningen av et overtredelsesgebyr i denne saken, som vi mener er betydelige. Det er svært viktig at alle offentlige instanser som behandler innbyggernes personopplysninger og opplysninger om sårbare personer er seg sitt ansvar bevisst og at slike hendelser ikke inntreffer.

Etter en totalvurdering av saken, og da særlig sett hen til overtredelsens varighet og alvorlighet 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 **1.000 000 NOK** anses som riktig.

## 8 Klageadgang

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

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

*Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer*