Datatilsynet

ÅLESUND KOMMUNE
Postboks 1521
6025 ÅLESUND

Deres referanse	Vår referanse	Dato
	20/02147-6 KBK/-	15.03.2021

Vedtak om overtredelsesgebyr ved bruk av treningsappen Strava – Ålesund kommune

1. Innledning

Vi viser til innsendt melding av 5. mai 2020 om brudd på personopplysningssikkerheten ved bruk av treningsappen Strava, samt oppfølgende redegjørelse av 30. juni 2020. Vi viser også til redegjørelse av 2. juli 2020 fra personvernombudet i Interkommunalt arkiv Møre og Romsdal IKS. Samt til svar på varsel om overtredelsesgebyr av 16. desember 2021.

Ut fra opplysningene i saken, mener Datatilsynet at Ålesund kommune har overtrådt reglene om personopplysningssikkerhet i personvernforordningen (Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016).

Ålesund kommune pålegges i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83 nr. 7, å betale et overtredelsesgebyr til statskassen på ***50 000 – femti 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, integritet og robusthet i behandlingssystemene og -tjenestene, jf. personvernforordningen artikkel 32 nr. 1 bokstav b), jf. artikkel 5, og*
- *for ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning, jf. personvernforordningen artikkel 24 nr. 1 jf. personopplysningsloven § 26 første ledd, og*
- *for ikke å ha vurdert hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet, jf. personvernforordningen artikkel 35*

Bakgrunnen og begrunnelsen for vedtaket følger under.

2. Saksforholdet

Datatilsynet mottok 5. mai 2020 en melding om brudd på personopplysningssikkerheten fra Ålesund kommune. Kommunen opplyser at dette gjelder Kolvikbakken ungdomsskule og Vatne ungdomsskule.

Lærere ved disse skolene påla elevene å laste ned treningsappen Strava til bruk i gymtimer. Det ble opprettet åpen gruppe pr. klasse med navn på elever. Elevene fikk oppdrag, f.eks. å sykle en bestemt strekning. Lærerne brukte sporing ved hjelp av appen til å sjekke at alle elevene hadde fullført oppgaven. Skolen og skoleledelsen ble informert om bruddet på personopplysningssikkerheten 5. mai 2020.

Bruken av Strava oppstod i en situasjon der lærerne måtte strekke seg svært langt for å gjennomføre forsvarlig undervisning i en pandemisituasjon. Kommunen ser likevel ikke dette som unnskyldende for manglende systematisk kontroll med applikasjoner i skolen

3. Lovovertredelsen

3.1 Behandlingsansvaret

Strava er en treningsapp som loggfører trening og lar brukerne analysere og sammenligne sine data med egne eller andres treningslogger. Strava Inc. lagrer opplysningene som appen genererer. Disse opplysningene vil være å regne som personopplysninger, som Strava Inc. i utgangspunktet er behandlingsansvarlig for. Behandlingsansvarlig er den som «alene eller sammen med andre bestemmer formålet med og midlene for behandlingen», jf. personvernforordningen artikkel 4 nr. 7.

Lærere ved to skoler i Ålesund kommune har pålagt elevene å laste ned Strava. Nedlasting av appen har vært obligatorisk. Dette vedkjenner kommunen seg i meldingen av 5. mai 2020. Dessuten har kommunen brukt appens sporingsfunksjon til å sjekke at alle elevene har fullført oppgaven sin. Bruken av denne sporingsfunksjonen regnes som en behandling av personopplysninger om hver enkelt elev. I forbindelse med denne behandlingen har vi lagt til grunn at det er kommunen, ved skolen, som er den behandlingsansvarlige. Det er skolen som har bestemt formålet med denne behandlingen, ved at skolen ønsket å kontrollere at elevene gjennomførte de oppgavene som de var pålagt. Personopplysningene ligger i appen i den private telefonen til elevene. Det er også skolen som har bestemt midlene for behandlingen, ved at skolen har valgt å ta i bruk treningsappen Strava for å realisere det nevnte formålet. Lærerne og de to skolene må her identifiseres med kommunen. Ved å pålegge bruk av treningsappen Strava på den enkelte elevs private mobiltelefon for å behandle personopplysninger om elevenes gjennomføring av treningsøvelser, har Ålesund kommune oppfylt vilkårene i personvernforordningen artikkel 4 nr. 7, og blir å regne som behandlingsansvarlig for denne behandlingen av personopplysninger.

Det følger av det som er sagt over at Ålesund kommune bl.a. har ansvaret for at treningsappen Strava, og den behandlingen av personopplysninger som appen muliggjør, er risikovurdert, jf. artikkel 32, at kommunen har egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, jf. artikkel 24, og for vurdering av personvernkonsekvensene etter artikkel 35.

3.2 Mangelfulle rutiner

Kommunen opplyser at det ikke er etablert noen rutine for anskaffelse av apper. Dette har vært påpekt fra informasjonssikringsansvarlig uten at slike rutiner er blitt etablert. Disse rutinene skal synliggjøre at personopplysningene behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte, at de samles inn for spesifikke, uttrykkelig angitte og berettigede formål, at de er adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for og at de behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene. Manglende rutiner har medført at det har oppstått en stor risiko for elevenes rettigheter og friheter. Ved ikke å ha etablert rutiner for tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning, er dette et brudd på artikkel 24 nr. 1.

3.3 Mangelfull sikkerhet ved behandlingen

Treningsappen Strava har blitt tatt i bruk uten at det er gjennomført en risikovurdering. Ved ikke å ha gjennomført en risikovurdering har kommunen ikke tatt hensyn til sannsynlighets- og alvorlighetsgrad for risiko for fysiske personers rettigheter og friheter. Dette vil være et brudd på personvernforordningen artikkel 32 nr. 1 bokstav b, som krever at det etableres et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet, integritet og robusthet i behandlingssystemene og -tjenestene.

3.4 Mangelfull vurdering av personvernkonsekvensene

Ålesund kommune har ikke gjennomført en vurdering av personvernkonsekvensene etter personvernforordningen artikkel 35. Manglende vurdering blir da å anse som et brudd på personvernforordningen artikkel 35. Det vises her til Datatilsynets hjemmeside med en liste over hvilke behandlingsaktiviteter som alltid utløser krav om at det gjennomføres en DPIA, se *https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/*

Datatilsynet anser at bruk av treningsappen Strava vil medføre behandlingsaktiviteter som krever at det gjennomføres en DPIA. Bruk av treningsappen medfører bl.a. at det behandles lokasjonsdata om elevene. Dessuten kan det være behandlet særlige kategorier av personopplysninger, så fremt elevene selv har opplyst om dette i appen. Bruk av treningsappen vil også medføre behandling av personopplysninger ved å systematisk monitorere effektivitet og ferdigheter. Hensikten med treningsappen har vært å se om elevene har gjennomført øvelsene. Man kan imidlertid også måle ferdighetene opp mot andre.

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 (EMK) 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 skolens pålegg til elevene til å laste ned treningsappen Strava uten at det er gjennomført en risikovurdering eller vurdering av personvernkonsekvensene ved å ta i bruk denne.

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll på opplysninger om seg selv, og hvorvidt andre har sett opplysninger om vedkommende. Ved å

se på valgte ruter, særlig start- og sluttpunkt, vil man også kunne utlede hvor eleven bor. Dette er særlig problematisk om noen har hemmelig adresse.

Datatilsynet ser alvorlig på at det fra kommunens side ikke har vært kontroll på hvilke apper som kan lastes ned og tas i bruk i regi av skolen.

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

Bruddet på personopplysningssikkerheten har medført at den registrerte har mistet kontroll på opplysninger om seg selv ved at valget av Strava ikke var frivillig. En slik hendelse kan få store personvernkonsekvenser for den berørte, ved at opplysningene kan bli kjent for tredjeparter. Saken indikerer rutinesvikt i kommunen. Det kan konstateres at det ikke er noen rutine i kommunen over hvilke apper som skal tas i bruk i regi av skolen. Det er således heller ikke tydelige rutiner i forbindelse med nedlasting av apper, bl.a. at disse skal risikovurderes før de tas i bruk.

Hendelsen er alvorlig, og fraværet av rutiner må betegnes som grovt uaktsomt.

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***

Det kan konstateres at ansvaret for bruddet på personopplysningssikkerhet påligger Ålesund kommune. Det vises her til pkt. 3.

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 ved bruk av treningsappen Strava, og inneholder opplysninger om navn, klassetrinn og lokasjonen. Kommunen opplyser i meldingen at en del opplysninger (f.eks. helse) krever samtykke før de blir lagret.

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 5. 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 Ålesund 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 ser positivt på at Ålesund kommune raskt tok grep da bruddet på personopplysningssikkerheten ble oppdaget samt meldte fra om avviket til Datatilsynet. Kommunen har også iverksatt tiltak som skal forhindre lignende lovbrudd i fremtiden.

Datatilsynet har ikke konstatert at Ålesund kommune har hatt økonomiske fordeler, eller unngått direkte eller indirekte tap som et resultat av overtredelsen.

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

5. Samlet vurdering

Det er imidlertid alvorlig at kommunen pålegger elever å laste ned treningsappen Strava til elevens private mobil, uten at appen har vært risikovurdert, og ikke har vurdert personvernkonsekvensene ved bruk av appen.

Etter Datatilsynets vurdering, er saken prinsipielt viktig. Ålesund kommune burde vært rustet til å ivareta kravene til personopplysningssikkerhet ved bruk av apper. I dette henseende kan et vedtak om overtredelsesgebyr gi en viktig signaleffekt.

Etter en samlet vurdering, hvor Datatilsynet også har tatt hensyn til situasjonen kommunen befant seg i, har Datatilsynet kommet til at Ålesund 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 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 et resultat av at kommunen ikke har hatt kontroll på nedlasting apper, og som et resultat av dette ikke har gjennomført egnede tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale instanser følger de regler som er gitt.

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 **50 000 NOK** anses som riktig.

7. Avsluttende merknader

Vi oppfordrer Ålesund kommune til å gi sitt syn på varselet, både når det gjelder vårt varsel om ileggelse av overtredelsesgebyr. Frist for merknader settes til 16. oktober 2020.

Datatilsynet vil ta endelig stilling i saken først etter at svarfristen er utløpt.

8. Inndrivelse av overtredelsesgebyr
Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig, jf. personopplysningsloven (2018) § 27. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

9. 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.

10. Innsyn og offentlighet
Dere har rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18. Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige, jf. offentlighetsloven § 3, men understreker samtidig at sikkerhetsdokumentasjon som hovedregel er unntatt offentlighet, jf. offentlighetsloven § 13 og forvaltningsloven § 13 første ledd nr. 2.

Dersom dere har spørsmål, kan dere ta kontakt med saksbehandler Knut B. Kaspersen..

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer