Datatilsynet

RÆLINGEN KOMMUNE
Postboks 100
2025 FJERDINGBY

Deres referanse	Vår referanse	Dato
	20/02191-1 KBK/-	02.07.2020

Vedtak om overtredelsesgebyr - Rælingen kommune

1. Innledning

Vi viser til melding om brudd på personopplysningssikkerheten fra Rælingen kommune sendt 8. mai 2019, varsel om overtredelsesgebyr av 26. februar 2020 og kommunens tilbakemelding av 29. april 2020.

Saken gjelder applikasjonen Showbie, som her er brukt til å kommunisere helserelaterte personopplysninger mellom skole og hjem, ved FINE-gruppa på Marikollen ungdomsskole. Avviket gjelder personopplysninger som omfatter særlige kategorier av personopplysninger.

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

> *I medhold av personopplysningsloven § 26 andre ledd, jf. forordningen artikkel 83, pålegger vi Rælingen kommune å betale et overtredelsesgebyr til statskassen på 500 000 – fem hundre tusen – kroner for å ikke ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, ved manglende sikring av vedvarende konfidensialitet og integritet, jf. forordningen artikkel 32 nr. 1. bokstav b og d, artikkel 24 og artikkel 35, jf. artikkel 5.*

Bakgrunnen og begrunnelsen for vedtaket følger under.

2. Datatilsynets vurdering av kommunens tilbakemelding

I tilbakemeldingen av 29. april 2020 erkjenner kommunen de faktiske forhold i saken som danner grunnlaget for Datatilsynets konklusjon om ileggelse av overtredelsesgebyr, samtidig som de påpeker at gebyret er uforholdsmessig høyt, gitt de konkrete omstendigheter som gjør seg gjeldende i saken.

I det følgende vil Datatilsynet gjennomgå kommunens merknader til gebyrets størrelse.

Kommunen påpeker at *«det er ingen opplysninger i saken som tyder*

på at noen av barna/elevene rent faktisk har vært utsatt for hverken materiell eller ikke-materiell skade, men Datatilsynet har ikke trukket dette momentet tydelig frem i sin vurdering». Datatilsynet er enig i at dette ikke fremkommer tydelig i vedtakets begrunnelse, men ønsker å påpeke at dette fremgår implisitt av pkt. 6.2 bokstav a) siste ledd. Dernest har Datatilsynet lagt vekt på at bruddet på personopplysningssikkerheten har høy risiko for de berørtes rettigheter og friheter. I denne utgjør selve sikkerhetsbruddet en risiko, uavhengig av om risikoen manifesterer seg i en mer konkret form for skade for de berørte eller ikke.

Kommunen påpeker videre at Datatilsynet ikke i tilstrekkelig grad har lagt vekt på at de aktuelle personopplysningene ble fjernet fra appen to dager etter at de faktiske forhold ble oppdaget. Etter vår vurdering kan ikke dette argumentet tillegges videre vekt, fordi det er den behandlingsansvarliges plikt å sørge for at reglene i personopplysningsloven og personvernforordningen overholdes til enhver tid, men vi tar synspunktet til etterretning.

Videre påpeker kommunen at den gjennomgående har benyttet benevnelsen *«elever ved tilrettelagt avdeling»*, og mener at dette er den korrekte karakteristikken å benytte også i tilsynets saksdokumenter. Datatilsynet har merket seg dette og vil etterkomme kommunens ønske.

Endelig påpeker kommunen at denne saken har visse likhetspunkter med saken mot Årdal kommune (PVN-2016-14), hvor det endelige overtredelsesgebyret ble satt til 50 000 kroner. Datatilsynet gjør oppmerksom på at vedtaket mot Årdal kommune var gjort etter gammel personopplysningslov og EU-direktiv 95/46. Kravene og størrelsene til overtredelsesgebyr er betydelig skjerpet etter ny personopplysningslov og personvernforordning, se artikkel 83 nr. 4 og 5. Etter gammel personopplysningslov kunne det gis overtredelsesgebyr maksimert til 10 ganger grunnbeløpet i folketrygden.

På bakgrunn av dette, har Datatilsynet funnet at det er grunnlag for å justere det varslede overtredelsesgebyret ned til 500 00 kroner.

3. Brudd på personvernforordningen

Meldingen om brudd på personopplysningssikkerheten har avdekket forhold som utgjør følgende mulige brudd på personvernforordningen:

- Mangelfull sikkerhet ved innlogging til Showbie, som gjør det mulig å få tilgang til personopplysninger om andre elever i FINE-gruppen, er i strid med personvernforordningen artikkel 32, se særlig nr. 1, bokstav b). Det har vært behandlet særlige kategorier personopplysninger (helseopplysninger) om elever ved tilrettelagt avdeling i applikasjonen, uten at Rælingen kommune har gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå.
- Mangelfull sikkerhetstesting før Showbie ble tatt i bruk i kommunen, og at applikasjonen ble tatt i bruk med et sikkerhetsnivå som ikke er egnet med hensyn til risikoen, er i strid med personvernforordningen artikkel 32 nr. 1 bokstav d)
- Det er ikke gjennomført en vurdering av personvernkonsekvenser, jf. artikkel 35
- Å ta i bruk en applikasjon med et utilstrekkelig sikkerhetsnivå er et brudd på ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2, jf. artikkel 5 nr. 1

bokstav f)

4. Sakens faktiske forhold

Sakens faktiske forhold er basert på meldingen om brudd på personopplysningssikkerheten, og redegjørelsene fra Personvernombudet i Rælingen kommune, Kommunens redegjørelse av 5. juni 2019, samt e-post av 13. september 2019. I brev av 9. mai 2019 ba Datatilsynet om en nærmere redegjørelse i saken. Slik redegjørelse ble sendt Datatilsynet 31. mai 2019 og 5. juni 2019 med rapport fra sikkerhetsansvarlig datert 13. mai 2019. 13. september 2019 bekreftet Rælingen kommune i en e-post at Marikollen ungdomsskole og FINE-gruppa startet med applikasjonen Showbie fra januar 2018. FINE står for Forum for INkluderte Elever, og er en avdeling som gir tilbud om tilrettelagt undervisning for elever med spesielle behov fra 1. – 10. trinn. Showbie er en applikasjon som er utviklet av Microsoft.

Det innmeldte bruddet på personopplysningssikkerheten gjelder mangelfull sikkerhet i Showbie.

Ifølge Statlig pedagogisk tjeneste er Showbie *«en digital læringsplattform som kan forenkle kommunikasjonen mellom lærer og elev, og lette samarbeidet mellom skole og hjem. Showbie tillater læreren å distribuere oppgaver på en enkel måte, og elevene kan levere inn svar og få disse tilbake med en vurdering. Vurderinger kan gis med skrevet tekst, eventuelt i form av video eller audiovisuelt.»*

Ved FINE-gruppa har Showbie fungert som en meldingsbok. FINE-gruppa er en tilrettelagt avdeling ved Marikollen ungdomsskole, og omfatter barn på forskjellig alderstrinn med ulike grader av utviklingshemminger med innslag av forskjellige tilleggsdiagnoser, som for eksempel epilepsi.

26 lærere og 15 elever inkl. foresatte ved FINE-gruppa har tilgang til Showbie. Pålogging gjøres gjennom kode eller fingeravtrykk. Det er ingen ytterligere pålogging til Showbie. Foresatte har ikke egen foreldretilgang. De logger seg på med elevens kode på vedkommendes iPad. Kode på iPad er eneste sikring.

Personvernombudet i Rælingen kommune mottok avviksmelding 28. februar på bakgrunn av en presentasjon som ble vist på enhetsledersamling. Ett av bildene var en skjermdump fra Showbie, som viste en elev på FINE-gruppen, der navnet var sladdet. På venstre side i applikasjonen var det kategorier som het «helse» og «medisiner». Det viste seg at det ikke lå personopplysninger i disse mappene. Mappene var tilrettelagt i samarbeid med RIKT AS for bruk. RIKT AS er et firma som tilbyr opplæring på forskjellige digitale plattformer til primært utdanningssektoren.

Kommunen opplyser i meldingen om bruddet på personopplysningssikkerheten at det ble funnet helseopplysninger under dagsplaner, samt i chat med foresatte (som så ut til å være med eleven). Skolen kommuniserer med foresatte om hvordan dagen har vært, f.eks. om eleven har vært på do, hatt anfall eller fått medisiner. Foresatte kan opptre på vegne av elev, og det er elevens navn som vises, uansett hvem som er pålogget og svarer. Ansatte bruker Showbie på trådløst nett på arbeidsplassen, mens foresatte bruker usikret trådløst nett,

eventuelt mobilnett hjemme. Det finnes ingen rutiner for bruk av Showbie. Rælingen kommune opplyser i brev av 5. juni 2019 at det ikke har vært gjennomført noen vurdering av personvernkonsekvensene før applikasjonen ble tatt i bruk. Kommunen opplyser at det heller ikke har vært gjennomført noen risikovurdering av Showbie før den ble tatt i bruk.

I rapport om bruddet på personopplysningssikkerheten av 13. mai 2019, opplyste sikkerhetsansvarlig at det var en rekke krav som ikke var oppfylt ved behandling av helseopplysninger. Sikkerhetsansvarlig påpekte bl.a. at to-faktor autentisering ved pålogging, og bruk av sikkerhetsnivå 4 i forhold til kommunikasjon med bank-ID, ID-porten e.l., samt kontroll på nettverk, manglet.

En konsekvens av at behandlingen av personopplysningene ikke har tilstrekkelig sikkerhet, er risiko for at uvedkommende får kunnskap om opplysninger som er taushetsbelagte eller er regnet som særskilte kategorier av personopplysninger.

5. Rettslig grunnlag for vurderingen

5.1 Om personvernprinsippene

Personvernforordningen artikkel 5 er sentral for tolkningen av forordningens øvrige bestemmelser. Overtredelse av prinsippene i art. 5 kan i seg selv føre til ileggelse av sanksjoner.

Som det fremgår av bestemmelsen, gjelder art. 5 nr. 1 bokstav f) personopplysningssikkerhet og prinsippet om plikt til å sikre nødvendig integritet og konfidensialitet. Dette er nærmere beskrevet og utfylles av mer konkrete bestemmelser i personvernforordningen kapittel IV, se f.eks. artikkel 32 om personopplysningssikkerheten.

Art. 5 nr. 2 fastslår, gjennom ansvarsprinsippet, at det er den behandlingsansvarlige som har ansvaret for å overholde personvernprinsippene i art. 5 nr. 1.

5.2 Om informasjonssikkerhet

Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32 nr. 1:

> «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 (…)».

Plikten til å gjennomføre egnede tekniske og organisatoriske tiltak fremgår tilsvarende av personvernforordningen artikkel 24, som regulerer den behandlingsansvarliges ansvar særskilt.

5.3 Om vurdering av personvernkonsekvensene

Personvernforordningen artikkel 35 regulerer når den behandlingsansvarlige skal foreta en vurdering av personvernkonsekvensene. Her følger et utdrag av bestemmelsen.

> *«1. Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.*
>
> *2. Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en vurdering av personvernkonsekvenser.*
>
> *3. En vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:*
>
> *a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,*
>
> *b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller*
>
> *c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område.»*

Det vises også til Datatilsynets hjemmesider med veiledning om når DPIA skal gjennomføres www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

5.4 Særlig om ileggelse av overtredelsesgebyr – artikkel 58 nr. 2 bokstav i

Personvernforordningen overlater til medlemsstatene å fastsette om overtredelsesgebyr skal kunne ilegges offentlige myndigheter og organer, jf. artikkel 83 nr. 7. I personopplysnings-loven § 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.

I personvernforordningen artikkel 83 fremgår vilkårene for ileggelse av gebyr. Bestemmelsen inneholder bl.a. en oversikt over hvilke momenter det skal tas hensyn til når det vurderes både hvorvidt overtredelsesgebyr skal ilegges, og hvilke momenter som skal vurderes i forbindelse med utmålingen av gebyrets størrelse. Artikkelen angir også gebyrenes størrelsesorden, og det fremgår av art. 83 nr. 4 og nr. 5 at maksimumssatsene avhenger av hvilke bestemmelser i personvernforordningen som er overtrådt.

Bestemmelsen gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men den legger føringer for skjønnsutøvelsen ved å trekke frem momenter som skal ha særlig vekt. Av artikkelens første ledd går det frem at overtredelsesgebyret i hvert enkelt tilfelle skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende.

Vi viser også til Personvernrådets retningslinjer vedrørende anvendelse og fastsettelse av overtredelsesgebyr i overensstemmelse med forordningen (EU) 2016/679 (WP 253), hvor Personvernrådet redegjør for de generelle kriteriene i art. 83 nr. 1, og momentene i art. 83 nr. 2.[1]

6. Datatilsynets vurdering og begrunnelse
Rælingen kommune opplyser at det ble funnet helseopplysninger under dagsplaner, samt i chat med foresatte, men at det ikke kan konstateres at personopplysninger er kommet uvedkommende i hende.

Rælingen kommune opplyser videre at Showbie ikke var tilrettelagt for behandling av særlige kategorier at personopplysninger, og at det derfor ikke har vært gjennomført noen risikovurdering eller gjennomgang av personvernkonsekvensene av denne behandlingen. Sikkerhetsansvarlig i kommunen har også konstatert at applikasjonen Showbie ikke har et tilstrekkelig sikkerhetsnivå, jf. forordningen artikkel 5 nr. 1 bokstav f), for å kunne behandle særlig kategorier av personopplysninger.

Datatilsynet finner det nødvendig å påpeke at det etablerte sikkerhetsnivået ikke er i samsvar med personvernforordningen artikkel 32 nr. 1 bokstav b), og at kommunen må iverksette tiltak for å skape et tilstrekkelig sikkerhetsnivå.

Rælingen kommune har ikke tydelig kommunisert at Showbie ikke skal benyttes til behandling av særlige kategorier av personopplysninger. Det finnes ingen advarsel eller informasjon i selve applikasjonen om at man ikke skal skrive inn særlige kategorier av personopplysninger. Tilretteleggingen av mappene «helse» og «medisiner» var gjort i samarbeid mellom FINE-gruppen og RIKT AS. En vurdering av personvernkonsekvensene, jf. artikkel 35, ville ha tydeliggjort dette.

Rælingen kommune er ikke kjent med at uvedkommende har benyttet seg av denne svakheten til å få tilgang til personopplysninger, men på grunn av at sikkerheten ikke er tilstrekkelig, har uvedkommende både i og utenfor FINE-gruppa hatt mulighet til å få tilgang på personopplysninger i Showbie.

6.2 Datatilsynets vurdering – overtredelsesgebyr
Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Internrettslig er overtredelsesgebyr ikke å anse som en straff, men en administrativ sanksjon. Det må imidlertid antas at overtredelsesgebyr er å anse som straff etter EMK (Den europeiske menneskeretts-konvensjonen) artikkel 6, og i samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556 med videre henvisninger.

[1] Opprinnelig utarbeidet av Artikkel 29-gruppen, men adoptert av Personvernrådet, se Personvernrådets «Endorsement 1/2018», pkt. 16. Dokumentene er tilgjengelige på https://edpb.europa.eu

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.

Det vises 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 første ledd 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».

Som nevnt over gir artikkel 83 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, idet det ses hen til at ileggelse av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende.

Vi har særlig lagt vekt på følgende momenter i vår vurdering:

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 er et resultat av manglende tekniske og organisatoriske tiltak som skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet og integritet, jf. forordningen artikkel 32.

Særlige kategorier av personopplysninger som kommunen har behandlet i Showbie er helseopplysninger om bl.a. dagsform, anfall (epilepsi), samt eventuelle tilleggsdiagnoser, medisiner og medisinering.

Overtredelsen omfatter 15 elever ved Marikollen ungdomsskole i Rælingen kommune. I tillegg vil 26 lærere være omfattet. Dette gjelder en tilrettelagt avdeling med barn med fysisk eller psykisk funksjonshemming. I en e-post til rektor ved Marikollen ungdomsskole 13. mars 2019 ba daværende sikkerhetsansvarlig om at rektor forklarte hva bruksområdet for Showbie er ved FINE-gruppen. Bakgrunnen for forespørselen var at det ut fra sikkerhetsansvarliges kjennskap på dette tidspunktet kunne se ut som om bruksområdet tilsvarte «*et elektronisk*

pasientjournal system» som kan eller vil inneholde sensitiv informasjon. I sitt tilsvar påpekte rektor følgende: *«Har poengtert flere ganger hva som kan og ikke kan ligge på Showbie for Fine. Laila har instruks om å gjennomgå mapper og sikre at det ikke legges sensitive opplysninger der.»* Det fritar ikke for ansvar om ledelsen har påpekt hvordan Showbie skal brukes, når dette ikke er fulgt opp med nødvendige tiltak.

Det er heller ikke gjennomført noen vurdering av personvernkonsekvensene (DPIA). Da behandling av særlige kategorier av personopplysninger vil kunne medføre en høy risiko for fysiske personers rettigheter og friheter, må Rælingen kommune foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. Vi viser her til personvernforordningens fortalepunkt 38, hvor det påpekes at barns personopplysninger skal gis et særlig vern. At rettighetene og frihetene til barn ved tilrettelagt avdeling har vært utsatt, må vektlegges i skjerpende retning i vurderingen av om det skal ilegges overtredelsesgebyr.

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

I saksdokumentene, blant annet i en e-post fra rektor til sikkerhetsansvarlig er det tydelig at FINE-gruppen har tatt Showbie i bruk på en måte som ikke har vært forutsetningene for bruken. At rektor har gitt instrukser til navngitte personer i FINE-gruppen om at sensitive opplysninger ikke skal legges der, fritar ikke for manglende oppfølging. Risikoen for at dette kunne skje var stor; og da det heller ikke er etablert gode rutiner eller gjennomført noen vurdering av personvernkonsekvensene etter personvernforordningen artikkel 35 eller risikovurdering er dette en systemsvikt av alvorlig karakter. Datatilsynet vil også påpeke at behandling av elever ved tilrettelagt avdeling i Showbie isolert sett vil kreve et tilsvarende sikkerhetsnivå.

Utover rimelig tvil har Rælingen kommune tatt i bruk Showbie uten å iverksette organisatoriske og tekniske tiltak for å sikre vedvarende konfidensialitet og integritet i applikasjonen Showbie, jf. personvernforordningen artikkel 5 nr. 1 bokstav f), jf. artikkel 32 nr. 1 bokstav b), og sørge for en effektiv prosess for regelmessig testing, analysering og vurdering av hvor effektive sikkerhetstiltakene er, jf. personvernforordningen artikkel 5 nr. 1 bokstav f), jf. artikkel 32 nr. 1, bokstav d).

Showbie ble tatt i bruk på Marikollen ungdomsskole tidlig i 2018. I e-post av 13. september 2019 opplyser kommunen følgende:

> *«Marikollen ungdomsskole og FINE-gruppa startet med Showbie fra januar 2018. Foreldrene til barna på FINEgruppa fikk imidlertid ikke opplæring i bruk av appen før i september/begynnelsen av oktober 2018. Avdelingsleder på FINE var litt usikker på konkret tidspunkt. Kommunikasjon mellom foreldre/skole for elevene på FINE kom i gang ila oktober 2018».*

Dette indikerer mangel på bevissthet om hvor viktig det er med nødvendige sikkerhetstiltak. Den manglende bevisstheten må betegnes som uaktsom, og etter vår vurdering dreier det seg om en alvorlig grad av uaktsomhet, som har betydning i vurderingen av om

overtredelsesgebyr skal ilegges.

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

Da bruddet på personopplysningssikkerheten ble avdekket var det tydelig kommunikasjonssvikt om alvorlighetsgraden av bruddet. Dette framgår av redegjørelsen fra personvernombudet. Tiltak kom etter hvert på plass, og personopplysningene ble fjernet fra appen to dager etter at bruddet på personopplysningssikkerheten ble oppdaget.

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***

Personvernforordningen har innført en høyere grad av ansvarlighet for den behandlingsansvarlige, jf. ansvarlighetsprinsippet i artikkel 5 nr. 2. Rælingen kommune har ikke sikret et tilstrekkelig sikkerhetsnivå, jf. artikkel 32. Det kan derfor konstateres at Rælingen kommune ikke har utvist den nødvendige ansvarlighet i forhold til akseptabelt beskyttelsesnivå.

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

Ingen tidligere overtredelser kan konstateres.

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

Det har ikke vært noe samarbeid mellom kommunen og Datatilsynet utover det som følger av personopplysningsloven og personvernforordningens krav, for å bøte på overtredelsen og redusere de mulige konsekvensene av den.

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

Vi kan konstatere at særlige kategorier av personopplysninger, slik dette er definert i personvernforordningen artikkel 9, har vært eksponert i Showbie. Da overtredelsen omfatter barn viser vi til personvernforordningens fortalepunkt 75, hvor det påpekes at det skal tas særlig hensyn til risikoen knyttet til barns personopplysninger.

Personopplysninger som har vært registrert i Showbie er helseopplysninger om dagsform og anfall (epilepsi), samt eventuelle tilleggsdiagnoser, medisiner og medisinering.

Det forhold at bruddet på personopplysningssikkerheten omfatter elever ved tilrettelagt avdeling gjør saken særlig alvorlig, og har vært tillagt stor vekt ved vurderingen av om overtredelsesgebyr skal gis.

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

Datatilsynet ble varslet om avviket fra Rælingen kommune 8. mai 2019.

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 Rælingen kommune med hensyn til samme saksgjenstand.

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

Dette punktet er ikke relevant for 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***

Datatilsynet har ikke konstatert at Rælingen kommune har hatt økonomiske fordeler, eller unngått tap direkte eller indirekte som et resultat av overtredelsen, og det foreligger heller ikke andre skjerpende omstendigheter enn de som er nevnt ovenfor. Vi kan heller ikke se at det foreligger andre formildende faktorer i saken.

7. Oppsummering

I vurderingen av om overtredelsesgebyr skal ilegges, legger Datatilsynet særlig vekt på at overtredelsene betydelig har krenket grunnleggende prinsipper som forordningen verner, jf. forordningen artikkel 5 nr. 1 bokstav f) hvor det heter at «*personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».*

Datatilsynet legger særlig vekt på at det ikke var etablert et akseptabelt sikkerhetsnivå i Showbie. Datatilsynet vurderer dette som alvorlig. Brukerne av kommunens tjenester har en klar og beskyttelsesverdig interesse mot mangelfulle sikkerhetstiltak hvor konfidensialitet er påkrevd. Dette kan få alvorlige konsekvenser for den enkelte både fordi omgivelsene kan få tilgang til informasjon som den registrerte ikke selv har valgt å gjøre kjent, men også fordi tilgjengeligheten gjør det uforutsigbart hvor mange som har skaffet seg informasjonen. Allmennpreventive grunner og hensynet til at reglene skal ha effekt og virke etter sin hensikt, taler da med styrke for at det reageres med et virkemiddel som overtredelsesgebyr.

Slik Datatilsynet ser det er bruddet på personopplysningssikkerhet særlig alvorlig da dette gjelder elever ved tilrettelagt avdeling som har liten eller ingen evne til å ivareta sine rettigheter og friheter.

Datatilsynet kan ikke se at de øvrige momenter som loven fremhever gjør seg gjeldende i nevneverdig grad – verken i skjerpende eller formildende retning.

Konklusjonen er at Datatilsynet er kommet til at overtredelsesgebyr ilegges.

8. Gebyrets størrelse

Når det gjelder gebyrets størrelse, skal de samme momentene tillegges vekt som ved vurderingen av om gebyr skal ilegges. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken. Samtidig må gebyrets størrelse stå i et rimelig forhold til overtredelsen og virksomheten.

Vi har særlig sett hen til at kommunen ikke hadde etablert et akseptabelt sikkerhetsnivå i Showbie, og at den aktuelle behandlingen av personopplysninger gjelder barn ved tilrettelagt avdeling.

Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale instanser følger de regler som er gitt. Vi legger til grunn at signalvirkningen av denne saken, de allmennpreventive hensyn, er betydelige. Det er viktig at slike hendelser ikke inntreffer, og at alle offentlige instanser som behandler innbyggernes personopplysninger og opplysninger om sårbare personer slik som barn, må ta det ansvaret som loven pålegger dem.

Mangelfulle rutiner har ofte som konsekvens at risikoen for feil øker. I denne saken har svake rutiner og manglende etterlevelse av rutinene faktisk hatt en reell konsekvens ved at det er funnet helseopplysninger under dagsplaner, samt i chat med foresatte. Dette tilsier en skjerpet reaksjon.

Kommunen har anført at enkelte omstendigheter etter kommunens syn burde ha vært tillagt vekt i formildende retning. Kommunen har trukket frem at det var kommunen selv som sendte melding om bruddet på personopplysningssikkerheten, at bruddet gjaldt et relativt lavt antall personer, og at de aktuelle opplysningene ble slettet to dager etter at bruddet ble oppdaget.

Vi viser til at plikten til å melde fra til Datatilsynet om brudd på personopplysningssikkerheten er lovpålagt, jf. personvernforordningen art 33, og at denne plikten hviler på den behandlingsansvarlige – i dette tilfellet kommunen. Vi ser ikke at det relativt lave antallet personer bør tillegges vesentlig vekt i formildende retning, men vi understreker at antallet berørte heller er ikke tillagt vekt i skjerpende retning.
Når det gjelder den siste anførselen, om at personopplysningene ble slettet etter to dager, har vi funnet at dette kan tillegges en viss vekt i formildende retning. Vi viser til Personvernrådets retningslinjer om adminsitrative sanksjoner (WP 253), hvor det er uttalt at «timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did", kan tillegges vekt.

Etter dette har vi kommet til at overtredelsesgebyret kan reduseres til **500.000 kroner**.

9. 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.

10. 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.

11. 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.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer