Datatilsynet

OSLO KOMMUNE UTDANNINGSETATEN
Postboks 6127 Etterstad
0602 OSLO

Deres referanse	Vår referanse	Dato
AR279591351	18/02579-3/KBK	29.04.2019

Varsel om vedtak - Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN

1. Innledning

Vi viser til melding om brudd på personopplysningssikkerheten (avviksmelding) fra Oslo kommune sendt 7. september 2018.

Saken gjelder sårbarheter i mobilapplikasjonen Skolemelding, en meldings-app utviklet for bruk i Osloskolen. I appen kan foresatte og elever sende meldinger til ansatte i skolen. Det har vært mulig for uvedkommende å logge seg inn som autoriserte brukere og dermed få tilgang til personopplysninger om elever, foresatte og ansatte. Det innebærer potensielt å få tilgang til personopplysninger om Osloskolens mer enn 63 000 grunnskoleelever[1] og alle foresatte og lærere til elevene. Det er også mulig å registrere personopplysninger av særlig kategorier i fritekstfeltet. Datatilsynet har bare vurdert bruddet på personopplysningssikkerheten opp mot grunnskolen. Hvorvidt dette har hatt betydning overfor den videregående skolen og spesialskolene er ikke vurdert i dette varselet.

Ut fra opplysningene i saken, mener Datatilsynet at Oslo kommune har overtrådt reglene om personopplysningssikkerhet i personvernforordningen (Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016) og vi varsler derfor om at vi vurderer å fatte fire ulike vedtak. Det ene vedtaket gjelder ileggelse av overtredelsesgebyr. De tre andre vedtakene gjelder pålegg om å iverksette nærmere tiltak.

2. Varsel om vedtak

2.1 Varsel om pålegg – artikkel 58 nr. 2 bokstav d

Datatilsynet varsler med dette Oslo kommune om at Datatilsynet, med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, vurderer å fatte vedtak om følgende pålegg:

[1] Kilde: https://www.oslo.kommune.no/politikk-og-administrasjon/etater-foretak-og-ombud/utdanningsetaten/arsberetning-2017/?del=3#gref

1) *Oslo kommune må iverksette organisatoriske og tekniske tiltak i appen Skolemelding ved å forhindre muligheten for at det kommuniseres særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav c, jf. artikkel 25 nr. 1 og nr. 2.*

2) *Oslo kommune må iverksette organisatoriske og tekniske tiltak for å sikre vedvarende konfidensialitet og integritet i appen Skolemelding, for å forhindre at uvedkommende får tilgang til personopplysninger om barn, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, jf. artikkel 32 nr. 1, bokstav b*

3) *Oslo kommune må iverksette organisatoriske og tekniske tiltak som sørger for at det finnes 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*

En nærmere begrunnelse for vedtakene om pålegg, se pkt. 5.1

2.2 Varsel om overtredelsesgebyr – artikkel 58 nr. 2 bokstav i
I medhold av personopplysningsloven § 26 andre ledd kan Datatilsynet ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83.

Datatilsynet varsler med dette Oslo kommune om at Datatilsynet, med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, jf. personvernforordningen art. 83, vil vurdere å fatte følgende vedtak om overtredelsesgebyr:

3) *Oslo kommune skal, i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, betale et overtredelsesgebyr på **2.000.000 NOK – to millioner norske kroner** – til statskassen, for ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, og sikring av vedvarende konfidensialitet og integritet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, og personvernforordningen 32 nr. 1. bokstav b og d*

En nærmere begrunnelse for vedtaket om overtredelsesgebyr, se pkt. 5.2

Dette brevet er et forhåndsvarsel om vedtak, jf. forvaltningsloven § 16.

3. De faktiske forholdene og sakens gang

3.1 Gangen i saken
Datatilsynet ble kjent med saken etter at Aftenposten torsdag 6. september 2018 hadde en nyhetsartikkel om alvorlig sikkerhetshull i appen.

Oslo kommune sendte melding om brudd på personopplysningssikkerheten (avviksmelding) til Datatilsynet den 7. september 2018.

Vi mottok en e-post den 10. september 2018 fra en privatperson som har engasjert seg i saken. I e-posten fremkom det flere opplysninger om saken og den viste også til Roy Solbergs blogginnlegg (https://blog.roysolberg.com/2018/09/osloskolen-leak), som har beskrevet sårbarhetene. Roy Solberg er en systemutvikler som ofte påpeker sårbarheter i digitale løsninger.

Med dette som bakteppe sendte Datatilsynet et krav om redegjørelse til Oslo kommune den 4. oktober 2018 og vi mottok svar fra Oslo kommune sendt 26. oktober. I forlengelsen av det har vi hatt dialog per telefon.

Vi ba om mer informasjon per e-post sendt 23. november og mottok svar fra kommunen 26. november.

3.2 Nærmere om de berørte system og funksjonalitet

Skolemelding er en meldings-app for Osloskolens foresatte, elever og ansatte. I appen kan foresatte og elever sende melding til kontaktlærer/faglærer eller andre ansatte på skolen. De kan også svare på meldinger sendt fra skolen. Appen gir også lærere en mulighet til å kommunisere med hverandre.

På Oslo kommunes nettside (https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/digital-skolehverdag/skolemelding/) står det at foresatte kan melde fravær i appen og i Portalen. (Portalen er en skoleplattform for Osloskolen og den enkelte skole har hver sin portal.) Meldingen sendes automatisk til barnets kontaktlærer. Det står videre: *«Bruk ikke appen eller øvrige kommunikasjonskanaler i Skoleplattform Oslo til å sende sensitive personopplysninger, som ditt barns helseopplysninger. Det holder å si at barnet ikke kommer på skolen i dag.».* I Skolemelding meldes fravær ved å klikke på «Ny melding» og knappen «Meld fravær». Det er her et fritekstfelt for å skrive hva fraværet gjelder. Det står ingenting i selve appen om at man ikke skal skrive inn sensitive personopplysninger.

For å autentisere brukere benytter Skolemelding seg av ID-porten for foresatte og FEIDE for ansatte. Dette er veletablerte standardkomponenter for autentisering og dette avviket gjelder ikke disse to tjenestene. Avviket berører hvordan disse komponentene integreres med Skolemelding for håndtering av innlogging.

3.3 Nærmere om de faktiske forholdene i saken

I det følgende vil vi beskrive hvordan vi, basert på sakens dokumenter og informasjon innhentet fra ulike parter, oppfatter de faktiske forholdene i saken.

I meldingen om brudd på personopplysningssikkerheten vi mottok fra Oslo kommune 7. september 2018 står hendelsen beskrevet slik:

> «Autoriserte brukere av skolemeldingsappene som har kunnskap til å dekryptere apper og har riktig type programvare har kunnet tilegne seg tilgang til andre brukeres personopplysninger av typen, navn, e-postadresse og hvilke barn en forelder har, samt meldinger sendt til og fra skolen. Ved å kombinere fødselsnummer, client secret og systempassord var det mulig å få tilgang til personopplysningene som er nevnt over.

> Dette i kombinasjon med manglende sikring ved bruk av et konkret api gjorde det mulig å få tilgang til andres meldinger for innloggede brukere.»

Etter å ha blitt kjent med blogginnlegget fra Roy Solberg (se referanse ovenfor), sendte vi et krav om redegjørelse til Oslo kommune 4. oktober 2018. Vi ba kommunen gi en tilbakemelding på om det som er beskrevet i blogginnlegget er riktig og om det er andre opplysninger i saken, som kan gi et helhetsbilde på hvilke sikkerhetsbrudd som har skjedd.

Vi fikk tilsvar fra Oslo kommune sendt 26. oktober 2018 at de hadde drøftet innholdet i avviksmeldingen med CGI Norge AS (CGI). CGI er leverandør av Skolemelding. CGI bekreftet at den opprinnelige beskrivelsen av avviket var noe misvisende. Oslo kommune skriver:

> «Etter videre undersøkelser bekrefter nå CGI at det var mulig å dekryptere koden for skolemeldingsappene og tilegne seg kunnskap om svakheter i autentiseringsprosessen, og gjennom det få tilgang til andre brukeres data ved å omgå pålogging via FEIDE eller ID-porten uten å være en autorisert bruker av løsningen. De presisere samtidig at det forutsetter at man må inneha mye kompetanse og kunnskap om både autentisering og skolemeldingen for å gjøre dette uten først å være pålogget. Som kjent ble avviket også først avdekket av en som hadde tilgang til løsningen.
>
> Ved å utnytte svakheten kunne en altså ved kun å kjenne en ansatt eller elevs brukernavn eller en foresatts personnummer få tilgang til deres personopplysninger av typen navn, e-postadresse og hvilke barn en foresatt har. Videre kunne en da også hente ut en og en melding uavhengig av bruker.
>
> CGI mener derfor at analysene i bloggen i hovedsak er korrekt. CGI har også selv avdekket svakhetene i bloggen i den videre sikkerhetstesting av applikasjonen, der alle feil som kan medføre sikkerhetsavvik er rettet.
>
> Vi har også gjennomført egne sikkerhetstester av løsningen i etterkant og har verifisert at avvikene er utbedret.»

I meldingen vi mottok 7. september stod det under «tiltak» beskrevet at kommunen ville øke hyppigheten på testing av sikkerheten i løsningen. Basert på det og svaret vi mottok 26. oktober, sendte vi en e-post til Oslo kommune 23. november der vi ønsket informasjon om hvordan testing har blitt gjennomført. Vi stilte også spørsmål om det finnes en risikovurdering for denne løsningen, samt om det finnes en DPIA (vurdering av personvernkonsekvenser).

Vi mottok svar fra Oslo kommune 26. november. Her står det beskrevet at leverandøren (CGI) gjennomførte sikkerhetstesting i perioden 16. – 24. august 2018. Leverandøren identifiserte noen sårbarheter og foreslo tiltak for å redusere disse i sin sikkerhetsrapport. Det kommer videre frem at leverandøren ikke hadde informert kommunen om resultatene av sikkerhetstesten, men at de valgte å vente med tiltaket til neste planlagte release. Kommunen oppgir at det er grunnen til at de raskt kunne lukke avviket og gi ut en oppdatering av appen.

De skriver videre at hvis de hadde kjent til sårbarheter tidligere ville de ha stengt løsningen inntil disse var utbedret.

På spørsmål fra Datatilsynet om det finnes DPIA og risikovurdering for løsningen, svarer kommunen at det ikke ble gjennomført en formell DPIA, men at det ble gjennomført en risikovurdering. En av ni identifiserte sårbarheter/trusler ble vurdert som uakseptabel. Sårbarheten var at det registreres sensitive data i løsningen. Det ble foreslått noen tiltak for å håndtere sårbarheten. Det ene var å gi informasjon på skolenes og kommunens nettsider om at det ikke må skrives sensitive opplysninger i fritekstfeltet, som er gjennomført. Det andre var å legge inn informasjon i appen i neste oppdatering, som var planlagt til 13. desember 2018. Et siste tiltak var å lage maler for registrering av ulike typer fravær. Dette tiltaket er planlagt som en del av videreutviklingen av løsningen i 2019. Avslutningsvis skriver kommunen at Utdanningsetaten vil vurdere behovet for fritekstfelt for å melde fravær.

Datatilsynet har ikke bedt om eller fått tilsendt risikovurdering utover det som er beskrevet over. Vi har heller ikke bedt om eller fått tilsendt rapport fra sikkerhetstestingen.

3.4 Sårbarhetene i systemet

Slik vi forstår det kan ikke sårbarhetene utnyttes ved vanlig bruk av appen Skolemelding, men ved at man bruker et verktøy slik som en web proxy for å kunne se og manipulere trafikk av data som kommuniseres gjennom systemet. Slike verktøy er lett tilgjengelig for nedlasting fra internett. Det krever en viss teknisk kompetanse for å kunne bruke dem, men det er også lett tilgjengelig informasjon på internett om hvordan man kan bruke dem.

3.4.1 Autentiseringsproblemer

Vi beskriver her prosessen for en foresatt-bruker av Skolemelding.

Når en bruker av appen for foresatte skal logge inn, blir brukeren som forventet tatt gjennom innloggingsprosessen i ID-porten. Det er etter dette at problemer oppstod. Det var en feil i logikken til autentiseringsserveren (kalt midporten), som brukes av systemet. Innloggingsløsningen ga kun ut fødselsnummer (som er foresattes bruker ID) som et tilgangstoken[2] etter innlogging. Det var derfor her mulig å lage sitt eget tilgangstoken uten å gå via innloggingsløsningen så lenge det ble benyttet et fødselsnummer som er registrert som en foresatt.

Fødselsnummer er bygget opp på en veldefinert måte og er begrenset til 11 millioner. Dette gjør det lett for en angriper å generere alle mulige fødselsnummer, for så å prøve de ut mot løsningen. Utvalget av fødselsnummer man trenger å teste kan også reduseres basert på eksempelvis fødselsår når man vet at man skal prøve ut fødselsnummer som kan tilhøre foresatte til barn i grunnskolen. Basert på en ytterligere svakhet i systemet er det ikke nødvendig å ha mer enn en gyldig bruker for å få tilgang til andres meldinger.

3.4.2 Manglende skille mellom brukere gjør at man kan få tilgang til andres meldinger

[2] Et tilgangstoken inneholder sikkerhetsinformasjon for en innloggingssesjon og identifiserer blant annet brukeren og dens rettigheter.

Når en bruker er autentisert kan vedkommende lese meldinger som ligger lagret på serveren. Dette gjøres i bakgrunnen av appen ved å spesifisere blant annet en ID for ønsket melding. ID-en er et sekvensielt generert heltall som fungerer som en unik identifikator for meldingen. Systemet mangler en verifikasjon på hvem en melding (ID) tilhører når den hentes ut. Dette fører til at en autentisert bruker kan hente ut hvilken som helst melding i systemet ved å spesifisere en gyldig meldings-ID, uavhengig av hvem den tilhører. Gjetting av gyldige ID-er vil ikke være vanskelig siden de som tidligere nevnt består av sekvensielle heltall.

3.4.3 Mulighet for høsting av opplysninger og knytte person til meldinger

Det er også mulighet til å hente ut informasjon om brukeren man er innlogget som og elevene som er tilknyttet denne brukeren. Dette inkluderer fullt navn, brukernavn, e-post, fødselsnummer og telefonnummer. Dette gjøres ved å kjøre et kall til serveren, som returnerer LDAP[3] data. Dette resulterer i at selv om noen i utgangspunktet tester med tilfeldige fødselsnummer så vil de videre ha mulighet til å knytte fødselsnummeret til person og familie på en lett måte.

4 Regelverket på området

4.1 Reglene i personvernforordningen

Personvernforordningen regulerer alle sider av behandling av personopplysninger. Personvernforordningen artikkel 5 omhandler det som må sies å være kjernen i personvernretten, og artikkelen er helt sentral for tolkningen av forordningens øvrige bestemmelser. Overtredelse av prinsippene i art. 5 kan i seg selv føre til ileggelse av sanksjoner, og det følger av art. 83 nr. 5 at overtredelser av art. 5 er blant de lovovertredelsene som kan resultere i de høyeste overtredelsesgebyrene, dvs. 20 000 000 euro (p.t. ca. 195 millioner NOK) for behandlingsansvarlige eller databehandlere som ikke er å regne som foretak.

Som det fremgår av bestemmelsen, gjelder art. 5 nr. 1 bokstav c dataminimering og prinsippet om at personopplysninger skal være relevante og begrenset til det som er nødvendig for formålene. Art. 5 nr 1 bokstav f gjelder personopplysningssikkerhet og prinsippet om plikt til å sikre nødvendig integritet og konfidensialitet. Art. 5 nr. 2 knesetter *ansvarsprinsippet*, som fastslår at det er den behandlingsansvarlige som har ansvaret for å overholde personvernprinsippene i art. 5 nr. 1.

Prinsippet i art. 5 nr. 1 bokstav c om dataminimering er særlig nevnt i artikkel 25 om krav til innebygd personvern og personvern som standardinnstilling.

Prinsippet i art. 5 nr. 1 bokstav f om integritet og konfidensialitet er nærmere beskrevet og utfylles av mer konkrete bestemmelser i personvernforordningen kapittel IV, se f.eks. artikkel 24 om iverksetting av nødvendige egnede tekniske og organisatoriske tiltak, artikkel 25 om krav til innebygd personvern og personvern som standardinnstilling, og artikkel 32 om personopplysningssikkerheten.

[3] Lightweight Directory Access Protocol er en protokoll som brukes til oppslag i en katalogtjeneste på en server

4.2. 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 personopplysningsloven (2018) § 26 annet ledd er det bestemt at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83, jf. artikkel 83 nr. 7.

I forarbeidene til ny personopplysningslov (Prop. 56 LS (2017-2018)) viser departementet til at

> «Datatilsynet i flere saker har ilagt administrative gebyrer mot offentlige organer, og departementet kan ikke se noen grunn til å ikke videreføre en slik adgang for Datatilsynet. Departementet viser også til at høringsinstansene generelt har vært positive til at overtredelsesgebyr skal kunne ilegges mot offentlige myndigheter.»

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 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.[4]

5 Datatilsynets vurdering av avvikene og begrunnelse for varsel om vedtak

5.1 Varsel om pålegg om iverksetting av tiltak

Oslo kommune er behandlingsansvarlig for de behandlingene som er omtalt i saken.

Datatilsynet mener at det foreligger brudd på bestemmelsen i personvernforordningen artikkel 25 nr. 1 og nr 2, som stiller krav til den behandlingsansvarlige om at det gjennomføres egnede tekniske og organisatoriske tiltak for å ivareta personvernprinsippene, slik som

[4] 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

dataminimering, og at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål, som behandles.

Datatilsynet vurderer å fatte vedtak om følgende pålegg:

4) *Oslo kommune må iverksette organisatoriske og tekniske tiltak i appen Skolemelding ved å forhindre muligheten for at det kommuniseres særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav c, jf. artikkel 25 nr. 1 og nr. 2.*

5) *Oslo kommune må iverksette organisatoriske og tekniske tiltak for å sikre vedvarende konfidensialitet og integritet i appen Skolemelding, for å forhindre at uvedkommende får tilgang til personopplysninger om barn, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, jf. artikkel 32 nr. 1, bokstav b*

6) *Oslo kommune må iverksette organisatoriske og tekniske tiltak som sørger for at det finnes 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*

Datatilsynet vurderer at pålegg 1) er nødvendig for å unngå at særlige kategorier av personopplysninger om barn kommuniseres i appen. Oslo kommune skriver på sin nettside at Skolemelding ikke skal benyttes til sensitive opplysninger. En av bruksområdene som trekkes frem er melding om sykefravær. Melding om fravær gjøres i et fritekstfelt i appen. Det finnes ingen advarsel eller informasjon i selve appen om at man ikke skal skrive inn sensitive personopplysninger i meldinger. Basert på dette fremstår det som sannsynlig at det vil legges sensitive opplysninger inn i løsningen, og vi kan med stor sannsynlighet anta at man ikke har tatt utgangspunkt i innebygd personvern (jf. forordningen artikkel 25) når man har laget løsningen.

Datatilsynet vurderer at pålegg 2) er nødvendig for å sikre at uvedkommende ikke får tilgang til å se meldinger om barn, se og endre personopplysninger om barn, foresatte eller ansatte, og sende meldinger om andre personer. Oslo kommune er ikke kjent med at andre enn den som har varslet om sikkerhetshullet har benyttet seg av dette. Det henvises ikke til noen konkrete tiltak som logg-gjennomgang eller andre tiltak som har blitt gjennomført for å verifisere eller avkrefte eventuell utnyttelse av sikkerhetshullene i løsningen. Oslo kommune svarer i e-post 26. november 2018 at sikkerhetshullet ble lukket samme dag som hendelsen inntraff.

Datatilsynet vurderer at pålegg 3) er nødvendig for at Oslo kommune selv skal ta ansvar for sikkerhetstesting og ha en tettere oppfølging av leverandøren for å unngå at kjente sikkerhetshull slipper gjennom sikkerhetstesting ved utvikling og oppdatering av appen. Oslo kommune skrev i den opprinnelige avviksmeldingen at hyppigheten av sikkerhetstesting skulle økes. Det indikerer at det har vært utført sikkerhetstesting av løsningen tidligere.

5.2 Varsel om 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 menneskerettskonvensjonen) artikkel 6, og i samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556 med videre henvisninger.

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.

Meldingen om brudd på personopplysningssikkerheten har avdekket forhold som utgjør mulige brudd på personvernforordningen artikkel 25 nr. 1 og 2, og artikkel 32 nr. 1:

- Lansering av en nyutviklet app hvor et av bruksområdene er at foresatte skal sende meldinger om sine barn eller gi beskjed om fravær ved bruk av fritekstfelt, gjør det lett å kommunisere særlige kategorier av personopplysninger om barn, uten at det er tekniske tiltak for å begrense hva som kommuniseres og uten at det informeres om det i appen, er i strid med personvernforordningen artikkel 25 nr. 1 og nr. 2.
- Manglende sikkerhet rundt innlogging til appen, som gjorde det mulig å få tilgang til å se og endre personopplysninger til mer en 63 000 barn, er i strid med personvernforordningen artikkel 32 nr. 1, bokstav b). I tillegg vil det omfatte opplysninger om foresatte og lærere.
- Mangelfull sikkerhetstesting før lansering av appen, og at appen ble lansert med sikkerhetshull som er godt kjent i sikkerhetsmiljøer verden over, er i strid med personvernforordningen artikkel 32 nr. 1, bokstav d)
- Lansering av en skolemeldingsapp med en uakseptabel sårbarhet som Oslo kommune ikke hadde gjennomført egnede tiltak for å lukke, og mangelfull kontroll med leverandøren, CGI, om resultatene av sikkerhetstesten, er et brudd på ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2, jf. artikkel 5 nr. 1 bokstav f)

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:

- ***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, jf. artikkel 83 nr. 2 bokstav a***

Omfanget

Bruddet på personopplysningssikkerheten er et resultat av manglende tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet og integritet, jf. forordningen artikkel 32. Vi viser også til personvernforordningens fortalepunkt 83.

Overtredelsen omfatter over 63.000 barn i grunnskolen i Oslo kommune. Overtredelsen omfatter barn, som i mindre grad har forutsetninger for å ivareta sine rettigheter og friheter. At bruk av appen skolemelding er en frivillig sak endrer ikke bildet av alvorlighetsgraden i bruddene.

Datatilsynet viser i denne forbindelse til at særlig barn har krav på høy beskyttelsesgrad når det behandles opplysninger om dem, se personvernforordningens fortalepunkt 38 hvor det heter:

> *«Barns personopplysninger fortjener et særlig vern, ettersom barn kan være mindre bevisste på aktuelle risikoer, konsekvenser og garantier, samt på de rettigheter de har når det gjelder behandling av personopplysninger.»*

Uvedkommende har fått tilgang til personopplysninger om mange barn gjennom appen skolemelding. Vi viser her til personvernforordningens fortalepunkt 38, hvor det påpekes at barns personopplysninger skal gis et særlig vern. At barns rettigheter og friheter har vært utsatt gjør overtredelsen ekstra alvorlig, og Datatilsynet har lagt vekt på dette som en skjerpende omstendighet.

Manglende innebygd personvern

I fraværsdelen av appen skolemelding skal det meldes om fravær. På kommunens nettsider er det informert om at det ikke må skrives sensitive opplysninger i fritekstfeltet. Noen slik informasjon er ikke lagt inn i fraværsdelen av appen skolemelding, noe Datatilsynet vil mene kunne vært med på å begrense muligheten for at det kommuniseres særlige kategorier av personopplysninger. Dette tiltaket alene vil imidlertid ikke gi et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet og integritet. I tillegg må man teknisk hindre muligheten for å kunne legge inn særlig kategorier av personopplysninger.

Den omstendighet at uvedkommende har hatt mulighet til å få tilgang til andres personopplysninger har også medført en mulighet til å manipulere personopplysningene til disse.

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

Testing

Det er skjerpende at Oslo kommune ikke har hatt nødvendig kontroll med testing som er gjort av leverandør. En innsikt i testresultatene kunne ha medført at kommunen på et tidligere tidspunkt kunne ha gjennomført tiltak for å lukke sikkerhetshullene, før skolemeldingsappen

ble tilgjengeliggjort for nedlasting. Det foreligger en plikt etter internkontroll-reglementet til å sikre og påvise at behandlingen utføres i samsvar med forordningen artikkel 24.

Vi viser her til ansvarsprinsippet i artikkel 5 nr. 2, jf. artikkel 5 nr. 1 bokstav f, idet det hviler en særskilt plikt på den behandlingsansvarlige til å overholde prinsippene i artikkel 5.

- ***Hvorvidt overtredelsen ble begått forsettlig eller uaktsomt, jf. artikkel 83 nr. 2 bokstav b***

Datatilsynet finner det sterkt kritikkverdig at kunnskap om hva som har skjedd ved bruddet på personopplysningssikkerheten, og sårbarheten i skolemeldingsappen har tilkommet Datatilsynet gjennom initiativ fra privatpersoner. Oslo kommune innrømmer da også at avviksmeldingene var misvisende. Dernest finner Datatilsynet det uheldig at saken er omtalt i media før avviksmelding er sendt Datatilsynet.

Vi vurderer det som hevet over tvil at Oslo kommune har hatt kunnskap om nødvendigheten for etablering av organisatoriske og tekniske tiltak i appen. Ved ikke å ta de nødvendige skrittene, har kommunen handlet uaktsomt. Feilene som er funnet i Skolemelding er av en sånn art at de har vært på OWASP[5] topp 10 listen i mange år. OWASP topp 10 er et anerkjent dokument for bevisstgjøring omkring sikkerhet i webapplikasjoner og blir ofte referert til blant folk i sikkerhetsmiljøet og på sikkerhetskonferanser. Det er en enighet blant sikkerhetseksperter verden over om hva som er de mest kritiske sikkerhetsrisikoer i webapplikasjoner. Datatilsynet har vist til OWASP flere steder i sin veileder om programvareutvikling med innebygd personvern[6]. Feilene i Skolemelding er beskrevet i A2, A3 og A5 i OWASP topp 10 fra 2013. Gitt sikkerhetshullene som er funnet i løsningen, fremstår en eventuell testing som har vært gjort som meget mangelfull.
Dette må betegnes som uaktsomt.

- ***Eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd, jf. artikkel 83 nr. 2 bokstav c***

Sikkerhetshullet ble lukket samme dag som kommunen oppdaget det. Det er viktig at kommunen gjorde disse tiltakene, men har ikke hatt nevneverdig betydning for de varslede pålegg.

- ***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, jf. artikkel 83 nr. 2 bokstav d***

Personvernforordningen har innført en langt høyere grad av ansvarlighet for den behandlingsansvarlige, jf. ansvarsprinsippet i artikkel 5. Oslo kommune har ikke gjennomført tekniske eller organisatoriske tiltak, som lever opp til prinsippene om innebygd personvern, jf. artikkel 25. Datatilsynet finner heller ikke at Oslo kommune har sikret et tilstrekkelig sikkerhetsnivå, jf. artikkel 32. Det kan derfor konstateres at Oslo kommune har utvist uaktsomhet i forhold til akseptabelt beskyttelsesnivå.

---

[5] Open Web Application Security Project – https://www.owasp.org
[6] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/

- ***Graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den, jf. artikkel 83 nr. 2 bokstav f***

Oslo kommune har meldt inn overtredelsen og har vært i dialog med Datatilsynet under sakens gang, uten at det har vært med på å redusere de mulige negative virkningene av overtredelsen.

- ***Kategoriene av personopplysninger som er berørt av overtredelsen, jf. artikkel 83 nr. 2 bokstav g***

Vi kan konstatere at særlige kategorier av personopplysninger, slik dette er definert i personvernforordningen artikkel 9, har vært eksponert for uvedkommende. Da overtredelsen omfatter barn i grunnskolen viser vi til personvernforordningens fortalepunkt 75, hvor det påpekes at det skal tas særlig hensyn til risikoen knyttet til barns personopplysninger, om behandlingen omfatter en stor mengde personopplysninger og berører et stort antall registrerte.

Opplysninger som har vært tilgjengelig er fraværsopplysninger som i et fritekstfelt kan resultere i at opplysninger om fraværsgrunn oppgis. Dessuten vil det i skolemeldingsappen kunne være registrert opplysninger som krever konfidensialitet, som for eksempel opplysninger om mobbing.

- ***På hvilken måte tilsynsmyndigheten fikk kunnskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen, jf. artikkel 83 nr. 2 bokstav h***

Datatilsynet ble først kjent med det aktuelle forholdet gjennom oppslag i media. Datatilsynet ble varslet om bruddet på personopplysningssikkerheten fra Oslo kommune 7. september 2018. Det er uheldig at Datatilsynet først får kunnskap om avviket etter at saken har vært omtalt i media.

- ***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, jf. artikkel 83 nr. 2 bokstav k***

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

Datatilsynet legger særlig vekt på at det ikke var etablert tilstrekkelige organisatoriske og tekniske tiltak i appen skolemelding. Datatilsynet vurderer dette som alvorlig. Brukerne av kommunens tjenester har en klar og beskyttelsesverdig interesse mot mangelfulle sikkerhetstiltak hvor konfidensialitet og integritet er påkrevd. Dette kan få alvorlige konsekvenser for den enkelte både fordi omgivelsene får 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.

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

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

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 knyttet til 63.000 barn i grunnskolen. 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, den mangelfulle testing, 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 slik som barn, 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 **2.000.000 NOK** anses som riktig.

7 Avsluttende merknader

Vi gjør oppmerksom på at dette brevet kun er et *forhåndsvarsel* om vedtak, jf. forvaltningsloven § 16.

Vi oppfordrer Oslo kommune til å gi sitt syn på varselet, både når det gjelder vårt varsel om ileggelse av overtredelsesgebyr og vårt varsel om pålegg om iverksetting av tiltak. Frist for merknader settes til **1. juni 2019**.

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

Dersom dere har spørsmål kan dere kontakte Knut Kaspersen på telefon 22 39 69 07.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Kaspersen
fagdirektør

Kopi til: OSLO KOMMUNE UTDANNINGSETATEN, Rohan Fininger, Postboks 6127 Etterstad, 0602 OSLO