Datatilsynet

OSLO KOMMUNE UTDANNINGSETATEN
Postboks 6127 Etterstad
0602 OSLO

Deres referanse	Vår referanse	Dato
18/34319 - 21	18/02579-13/KBK	11.10.2019

Vedtak om overtredelsesgebyr

Vi viser til melding om brudd på personopplysningssikkerheten (avviksmelding) fra Oslo kommune sendt 7. september 2018, varsel om vedtak av 29. april 2019 og Oslo kommunes svar av 21. juni 2019.

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).

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, jf. personvernforordningen art. 83, fatter Datatilsynet følgende vedtak om overtredelsesgebyr:

> *Oslo kommune pålegges, i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, å betale et overtredelsesgebyr på **1.200.000 NOK – en million to hundre tusen norske kroner** – til statskassen for overtredelser av plikter som følger personvernforordningen.*
>
> *Gebyret ilegges som følge av at Oslo kommune ikke har 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*

Bakgrunnen og begrunnelsen for vedtaket følger under.

1. Saksforholdet

1.1. Beskrivelse av saken

Saken gjelder sårbarheter i mobilapplikasjonen Skolemelding. Dette er en applikasjon som kan lastes ned på mobiltelefonen, og som er utviklet for bruk i Osloskolen. I applikasjonen kan foresatte og elever kommunisere med ansatte i skolen. Kommunikasjonen er skriftlig, og kan sammenlignes med SMS eller e-post.

Det har vært mulig for uvedkommende å logge seg inn som autoriserte brukere og dermed få tilgang til personopplysninger om elever. Mer enn 63 000 grunnskoleelever[1] i Osloskolene er omfattet.

I tillegg er det mulig å registrere særlige kategorier av personopplysninger i fritekstfeltet, for eksempel om barnas helse. Dette kan ha medført risiko for at uvedkommende har kunnet se opplysninger av inngripende karakter.

1.2. Saksgangen

Datatilsynet ble kjent med saken etter at Aftenposten torsdag 6. september 2018 hadde en nyhetsartikkel om alvorlige sikkerhetshull i applikasjonen.

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

Datatilsynet mottok også en henvendelse fra en privatperson i sakens anledning. Datatilsynet sendte deretter et krav om redegjørelse til Oslo kommune den 4. oktober 2018, og vi mottok svar fra Oslo kommune sendt 26. oktober. Vi har også hatt dialog med kommunen per telefon.

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

I brev av 29. april 2019 varslet Datatilsynet vedtak om tre pålegg om iverksettelse av tiltak som ble ansett nødvendige for å lukke de aktuelle avvikene fra krav i personvernregelverket. Vi varslet også at vi ville vurdere å fatte vedtak om overtredelsesgebyr som følge av bruddet på behandlingsansvarliges plikter etter personvernregelverket.

Oslo kommune besvarte varselet rettidig i brev av 21. juni 2019.

I svaret fra Oslo kommune redegjøres det nærmere for systemet Skolemelding, samt om CGIs forpliktelser (kommunens leverandør) og hendelsesforløpet før og etter sikkerhetshendelsen. Datatilsynet legger denne redegjørelse til grunn som en del av sakens faktiske forhold. Datatilsynet har vurdert Oslo kommunes forslag til tiltak i sakens anledning, og finner at avvikene nå er lukket. De varslede vedtakene om pålegg anses derfor bortfalt.

Datatilsynet vil i det følgende kun vurdere vedtak om overtredelsesgebyr.

1.3. Nærmere om systemet og funksjonalitet i Skolemelding

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

---

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

På Oslo kommunes nettside (https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/digital-skolehverdag/skolemelding/) står det at foresatte kan melde fravær i applikasjonen 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 applikasjonen 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 avviket i saken gjelder ikke disse to tjenestene.

Avviket berører hvordan disse komponentene integreres med Skolemelding for håndtering av innlogging.

1.4. Oslo kommunes beskrivelse av avvikene

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.»

Avviket ble nærmere beskrevet i brev fra Oslo kommune datert 26. oktober 2018:

> «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.»

Datatilsynet sendte flere forespørsler om redegjørelser knyttet til blant annet hvordan testing av løsningen var blitt gjennomført, om det var gjennomført risikovurderinger og personvernkonsekvensvurderinger (DPIA).

Oslo kommune har i sine svar 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 kom 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 oppga at det var grunnen til at de raskt kunne lukke avviket og gi ut en oppdatering av applikasjonen. De opplyste videre at hvis de hadde kjent til sårbarheter tidligere ville de ha stengt løsningen inntil disse var utbedret.

På spørsmål fra Datatilsynet om det var gjennomført DPIA og risikovurdering for løsningen, svarte 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 applikasjonen 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. Utdanningsetaten ville også 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.

1.5. Sårbarhetene i systemet

I vårt varsel om vedtak ble sårbarhetene i systemet beskrevet på følgende måte:

Slik vi forstår det kan ikke sårbarhetene utnyttes ved vanlig bruk av applikasjonen 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.

1.5.1. Autentiseringsproblemer

Når en bruker av applikasjonen 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.

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

Når en bruker er autentisert kan vedkommende lese meldinger som ligger lagret på serveren. Dette gjøres i bakgrunnen av applikasjonen 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.

1.5.3. 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.

2. Oslo kommunes tilbakemeldinger

Oslo kommune har i brev av 21. juni 2019 ikke bestridt Datatilsynets fremstilling av de faktiske forholdene som går frem av vårt varsel om vedtak av 29. april 2019.

Vi legger i det følgende til grunn at vår fremstilling av avvikets karakter og omfang gir en korrekt beskrivelse.

---

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

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

Kommunen har i sitt tilsvar beskrevet hvordan avvikene er lukket, og hvilke tiltak som er satt inn for å hindre at lignende avvik skjer igjen. Vi legger til grunn at disse tiltakene er tilfredsstillende, og anser avvikene som lukket.

Oslo kommune har kommet med innvendinger mot størrelsen på det varslede overtredelsesgebyret. Disse omtales nedenfor under vår vurdering av om overtredelsesgebyr skal ilegges.

3. Rettslig grunnlag for vurderingen

3.1. Om 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.

Som det fremgår av bestemmelsen, gjelder art. 5 nr. 1 bokstav f personopplysningssikkerhet og prinsippet om plikt til å sikre nødvendig integritet og konfidensialitet.

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 32 om personopplysningssikkerheten.

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.

3.2. 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 personopplysnings-loven (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 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.[4]

4. Datatilsynets vurderinger og begrunnelse for vedtak

4.1. Vurdering av om lovbrudd har funnet sted

Behandlingen av melding om brudd på personopplysningssikkerheten avdekket følgende forhold som utgjør brudd på personvernforordningen artikkel 32 nr. 1:

1. Manglende sikkerhet rundt innlogging til applikasjonen, 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.
2. Mangelfull sikkerhetstesting før lansering av applikasjonen, og at den ble lansert med sikkerhetshull som er godt kjent i sikkerhetsmiljøer verden over, er i strid med personvernforordningen artikkel 32 nr. 1, bokstav d)
3. Lansering av en skolemeldingsapplikasjon 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)

Oslo kommune har ikke bestridt Datatilsynets vurderinger av om og i hvilken grad det har skjedd avvik fra personvernforordningens krav til behandling av personopplysninger.

4.2. Datatilsynets vurdering av vilkårene for ileggelse av overtredelsesgebyr

4.2.1. Generelt om vurderingen

Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Overtredelsesgebyr kan ilegges for avvik som har funnet sted, også for tilfeller hvor avvikene er lukket på vedtakstidspunktet for overtredelsesgebyret.

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.

---

[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

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 gjennomgår i det følgende de relevante vilkårene i personvernforordningen artikkel 83 nr. 2:

4.2.2. Artikkel 83 nr. 2 bokstav 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 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. Alle har ikke tatt skolemeldingsapplikasjonen i bruk, men potensialet er likevel 63.000. Overtredelsen omfatter barn, som i mindre grad har forutsetninger for å ivareta sine rettigheter og friheter. At bruk av applikasjonen 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.»*

At barns rettigheter og friheter har vært utsatt gjør overtredelsen ekstra alvorlig, og Datatilsynet har lagt vekt på dette som en skjerpende omstendighet.

I fraværsdelen av applikasjonen skal det meldes om fravær. På kommunens nettsider er det informert om at det ikke må skrives sensitive opplysninger i fritekstfeltet. Tilsvarende informasjon er ikke lagt inn i fraværsdelen av applikasjonen, noe Datatilsynet vil mene kunne vært med på å begrense muligheten for at det kommuniseres særlige kategorier av personopplysninger.

De fleste som bruker applikasjonen Skolemelding går ikke inn via kommunens hjemmesider, men via applikasjonen, og vil således ikke få denne informasjonen. Dette vil imidlertid ikke ha avgjørende betydning for avvikets alvorlighetsgrad.

Den omstendighet at uvedkommende har hatt mulighet til å få tilgang til andres personopplysninger ha medført en mulighet til å manipulere personopplysningene i applikasjonen.

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 i applikasjonen.

4.2.3. Artikkel 83 nr. 2 bokstav b: vurdering av grad av skyld

I følge forvaltningsloven § 46 kan det ilegges administrativ sanksjon overfor et foretak selv om ingen enkeltperson har utvist skyld. Med det menes at Oslo kommune har et objektivt skyldansvar. Med foretak menes selskap, samvirkeforetak, forening eller annen sammenslutning, enkeltpersonforetak, stiftelse, bo eller offentlig virksomhet.

Vi vurderer det som hevet over tvil at Oslo kommune har hatt kunnskap om nødvendigheten for etablering av organisatoriske og tekniske tiltak i applikasjonen. Ved ikke å ta de nødvendige skrittene, har kommunen handlet uaktsomt.

Datatilsynet finner at det er en klar sannsynlighetsovervekt for at Oslo kommune har overtrådt art. 5 og artikkel 32 i personvernforordningen.

4.2.4. Artikkel 83 nr. 2 bokstav c: tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd

Sikkerhetshullet ble lukket samme dag som kommunen oppdaget det. Det er viktig at kommunen gjorde disse tiltakene, og vil være en signaleffekt overfor andre. Datatilsynet mener dette skal virke formildende i vurderingen av overtredelsesgebyret.

4.2.5. Artikkel 83 nr. 2 bokstav d: 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

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.

---

[5] Open Web Application Security Project – https://www.owasp.org

[6] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/

Det kan derfor konstateres at Oslo kommune har utvist uaktsomhet i forhold til akseptabelt beskyttelsesnivå.

4.2.6. Artikkel 83 nr. 2 bokstav f: samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den

Det har ikke vært noe samarbeid med Datatilsynet for å bøte på overtredelsen. Oslo kommune har på eget initiativ gjort nødvendige tiltak for å lukke bruddene på personopplysningssikkerheten.

4.2.7. DetteArtikkel 83 nr. 2 bokstav g: kategorier av personopplysninger som er berørt av overtredelsen

Ettersom 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.

Vi kan konstatere at særlige kategorier av personopplysninger, slik dette er definert i personvernforordningen artikkel 9, har vært eksponert for uvedkommende.

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

4.2.8. Artikkel 83 nr. 2 bokstav h: måten tilsynsmyndigheten fikk kunnskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen

Datatilsynet ble først kjent med det aktuelle forholdet gjennom oppslag i media. Vi 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.

Datatilsynet finner det sterkt kritikkverdig at kunnskap om hva som har skjedd ved bruddet på personopplysningssikkerheten, og sårbarheten i skolemeldingsapplikasjonen har tilkommet oss gjennom initiativ fra privatpersoner. Oslo kommune innrømmer da også at avviksmeldingene var misvisende. Dette vil ha betydning i vår vurdering om overtredelsesgebyr skal ilegges.

4.2.9. Artikkel 83 nr. 2 bokstav k: andre 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 funnet 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 applikasjonen Skolemelding. Datatilsynet vurderer dette som alvorlig, og er en av årsakene til at overtredelsesgebyr er ilagt. Brukerne av kommunens tjenester har en klar og beskyttelsesverdig interesse mot mangelfulle sikkerhetstiltak hvor konfidensialitet og integritet er påkrevd.

Mangelfull sikkerhet 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.

I formildende retning kan det påpekes at Oslo kommune reagerte med en gang de fikk kunnskap om sikkerhetshullene.

4.2.10. Oppsummering og konklusjon

Etter en helhetsvurdering av avvikets omfang, karakter og alvorlighetsgrad, har Datatilsynet kommet til at det er korrekt å opprettholde vårt varslede vedtak om overtredelsesgebyr.

Vi har lagt særlig vekt på at det er barns personvern som er rammet av avviket.

4.3. Utmåling av overtredelsesgebyret 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»,

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 vekt. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken, samtidig som gebyrets størrelse må stå i et rimelig forhold til overtredelsen og virksomheten, jf. art. 83 nr. 1.

Vi har særlig sett hen til at bruddet på personopplysningssikkerheten er knyttet til et betydelig antall barn i grunnskolen. Videre har vi lagt vekt 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 av denne typen opplysninger.

Ileggelse av overtredelsesgebyr i denne saken vil ha en viktig signaleffekt. Datatilsynet ønsker å tydelig kommunisere at slike hendelser vurderes som alvorlige 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. Vi har lagt vekt på de allmennpreventive virkningene et vedtak om overtredelsesgebyr antas å ha.

I vårt varslede vedtak anga vi at gebyrets størrelse ville bli satt til 2.000.000 NOK.

Oslo kommune besvarte vårt varsel med innsigelser til størrelsen på gebyret. Den anførte *«at det er tilstrekkelig å pålegge leverandøren forpliktelser om rapportering av avvik, i tillegg til det er etablert rutiner for kontinuerlig oppfølging av leverandøren. Vi har ansett denne praksisen som tilfredsstillende, da den har fungert godt over flere år gjennom at avvik har blitt oppdaget og ryddet opp i. Det er også innrømmet av leverandøren at mangelfull oppfølging av avtalen skyldes menneskelig svikt. UDE mener at forannevnte må anses som formildende omstendigheter. Vi har uansett ønsket å forbedre vår kontroll hva angår sikkerhetstester, og har derfor innført tiltak om felles gjennomgang av alle resultater fra sikkerhetstesting med leverandør, jf. ovenfor».*

Oslo kommune påpeker at de ikke kunne melde avvik til Datatilsynet da de ikke hadde kunnskap om forholdene. At Oslo kommune ikke hadde kunnskap om testresultatene kommer, slik Datatilsynet ser det, som et resultat av manglende prosjektstyring mellom kommunen og deres leverandør.

Datatilsynet gjør oppmerksom på at Oslo kommune er ansvarlig for de alvorlige brudd som har skjedd ved ikke å innføre organisatoriske og tekniske tiltak som er egnet til å sikre vedvarende konfidensialitet og integritet i applikasjonen Skolemelding. At Oslo kommune var i den tro at applikasjonen var sikkerhetstestet før den ble produksjonsatt, og mente det var tilstrekkelig å pålegge leverandøren forpliktelser om rapportering av avvik er en kalkulert risiko, som ikke kan virke formildende på hendelsen.

Oslo kommune påpeker endelig at leverandøren har en betydelig del av ansvaret for hendelsen. Datatilsynet er ikke uenig i dette, men dette fritar likevel ikke kommunen fra ansvaret.

Endelig påpeker kommunen at det bare kan konstateres at to personer er berørt av bruddet på personopplysningssikkerheten. Dette tillegger Datatilsynet liten betydning da potensialet var langt større.

Datatilsynet har kommet til at det varslede overtredelsesgebyret må nedjusteres noe. Vi har i vurderingen lagt vekt på at Oslo kommune har iverksatt skadebegrensende tiltak så raskt kommunen fikk kunnskap om bruddet på informasjonssikkerheten, og vist vilje til å ordne opp i hendelsen.

Etter en totalvurdering av saken har vi kommet til at et overtredelsesgebyr på **1.200.000 NOK** anses som riktig.

5. Vedtak om overtredelsesgebyr

5.1. Vedtak om overtredelsesgebyr

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, jf. personvernforordningen art. 83, fatter Datatilsynet følgende vedtak om overtredelsesgebyr:

> *Oslo kommune pålegges, i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, å betale et overtredelsesgebyr på* ***1.200.000 NOK – en million to hundre tusen norske kroner*** *– til statskassen for overtredelser av plikter som følger personvernforordningen.*
>
> *Gebyret ilegges som følge av at Oslo kommune ikke har 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.*

5.2. Inndrivelse av overtredelsesgebyret

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.

5.3. 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.

5.4. 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