DRAMMEN KOMMUNE

Spørsmål 122 (2021) fra Herman Ekle Lund (V): Deling av innbyggernes persondata med tredjepart

Til:	Rådmannen	Dato:	27.05.2021
Fra:	Herman Ekle Lund (V)	Saksnr:	21/00070-122
		Deres ref:	

Vi har mottatt henvendelser fra våkne og bekymrede foreldre fra en av drammensskolene, som i korte trekk er bekymret for at skolen og kommunen deler unødvendig og identifiserende informasjon om skoleelever, til mange leverandører av digitale læringsmidler.

Noe liknende var tema for et politikerspørsmål tilbake i januar 2020, som oppfølging av den såkalte "Vigilo-skandalen" i Bergen kommune. Rådmannen svarte da følgende: https://www.drammen.kommune.no/globalassets/politikk-og-samfunn/dokumenter/sporsmal-og-svar/spm-12-m-svar.pdf

Gjennom dette svaret virket det som Drammen kommune er oppmerksomme på denne problematikken og at man har utviklet gode rutiner for å hindre at persondata deles uten samtykke.

I lys av dette er det leit å nå høre om nye bekymringer, knyttet til andre applikasjoner i skolen. De nevnte foreldrenes bekymring går på deling av informasjon mellom Feide og andre apper/programmer i skolen.

I dette tilfelle er matematikk-appen Kikora eksempel (en av mange digitale læringsapper). Påloggingstjenesten Feide gir Kikora identifiserende elevinformasjon, slik at hvert enkelt barns prestasjon, arbeidsstil, og evnenivå, blir analysert og lagret sammen med barnets identitet. Dette er sensitive opplysninger for hver enkelt person. Det er imidlertid unødvendig for funksjonen i Kikora å dele barnas identitet. Lærer trenger å vite hvem eleven er, men Kikora trenger ikke å gjøre dette. Praksis strider mot begrensningsprinsipper i datalagringsdirektivet, og det kan ikke avtales å dele mer enn nødvendig.

Hver kommune har en databehandleravtale med Kikora, der Kikora oppgir at de kan dele data med underleverandører. Kikora AS er en kommersiell aktør med mange eiere, som kan bli oppkjøpt. Det virker unødvendig riskabelt å la de koble sensitive data om barns prestasjon, med identitet.

Politisk sekretariat
Organisasjonsnummer
921234554

Postadresse
Postboks 7500
3008 DRAMMEN

Besøksadresse

Telefon +4732040000
kommunepost@drammen.kommune.no

I Kikora appen er det barnet selv, som ved første pålogging samtykket til at Kikora kan innhente identifiserende informasjon fra Feide. Uten å bekrefte fikk barnet i eksemplet ikke bruke appen. Barn har verken kognitive forutsetninger eller juridisk myndighet til å foreta slike valg.

Det er ingen hemmelighet at kjøp og salg av persondata (av stadig flere kritiske røster kjent som "overvåkningsøkonomien") utgjør et av verdens største og mest lukrative markeder i dag. Vi mener derfor Drammen, og andre kommuner, må ha ytterste aktsomhet i møte med leverandører som fisker etter persondata fra våre innbyggere – særlig når nasjonal lovgivning og felles europeiske direktiv uttrykker svært tydelig at persondata ikke skal deles med mindre personen – fortrinnsvis en myndig person – har gitt aktivt samtykke til dette, og at det skal kunne brukes systematisk i kommersiell sammenheng.

Det kan hende at dette er storm i et vannglass, men vi ser uansett på dette med stor bekymring og ønsker å bruke føre-var-prinsippet her. Derfor ber vi om at rådmannen besvarer følgende spørsmål snarlig:

- Hvilke vurderinger har rådmannen gjort av hva som er nødvendig behandling av personopplysninger knyttet til elever – på generelt grunnlag, ikke spesifikt til dette tilfellet?
- Hvilke vurderinger har rådmannen gjort for å sikre at opplysninger om barn ikke kommer på avveie eller på annen måte misbrukes av tilbydere av eksempelvis apper som brukes i skolen?
- Hvilke rettslige grunnlag bygger behandling av skoleelevers personopplysninger i Drammen kommune på? Hvilke tiltak vil rådmannen gjøre for å følge opp sikring av de spesifikke tilfellene knyttet til Feide og Kikora som beskrevet over?
- Kan rådmannen, på generelt grunnlag, garantere for at innbyggeres persondata ikke deles med tredjeparter som kommunen samarbeider med, uten at innbyggerne (herunder myndige innbyggere, eventuelt foresatte på vegne av ikke-myndige barn) har gitt aktivt samtykke til dette?

Svar

1) Hvilke vurderinger har rådmannen gjort av hva som er nødvendig behandling av personopplysninger knyttet til elever – på generelt grunnlag, ikke spesifikt til dette tilfellet?

Alle programmer som er i bruk i skolene i Drammen kommune skal ha ROS-analyse for hvilke data som behandles. Drammen kommune benytter både ROS (risiko og sårbarhetsanalyse), DPIA (en vurdering av personvernkonsekvenser med større kompleksitet) og teknisk løsningsbeskrivelser med kvalitetsdokumenter. Dataminimering er et eget tema i alle disse analysene. Drammen kommune inngår databehandleravtaler med leverandørene. Databehandleravtaler er juridisk bindende for leverandørene, og skal sikre at informasjon ikke kan videreformidles til andre formål enn det som er avtalt.

Drammen kommune har oversikt over alle apper og programmer som benyttes i skolene, og det er foretatt en betydelig innstramming med tanke på antall apper og programmer som skolene har til rådighet. Rådmannen har administrasjonsstyring på hvilke apper som benyttes i klasser og skoler, og det er ikke opp til skolene selv å bestemme dette. Denne avgrensning er for at kommunen til enhver tid skal vite hvilke apper som er i porteføljen til kommunen, og sikre at appene er vurdert.

Når det gjelder pedagogisk programvare har alle skoler meldt inn til administrativ skoleeier hva de benytter, i tillegg til sentralt innkjøpte læremidler. Nye systemer må gjennom porteføljeprosessen.

Drammen kommune samarbeider med flere andre nærliggende eller sammenlignbare kommuner både i etablerte nettverk og andre uformelle faglige nettverk. KS har opprettet et eget rådgivningsprosjekt som heter SkoleSec; SkoleSec - KS. Erfaringer viser at kommuner står i mange like problemstillinger, og kommunene utvikler seg sammen i dette store og krevende feltet.

Tjenestene samarbeider tett med personvernombudet i kommunen, både i forhold til rådgiving og faglige vurderinger. Administrativ skoleeier jobber kontinuerlig med å oppdatere både databehandleravtaler, ros-analyser og interne rutinebeskrivelser. Dette er et stort og ressurskrevende arbeid.

2) Hvilke vurderinger har rådmannen gjort for å sikre at opplysninger om barn ikke kommer på avveie eller på annen måte misbrukes av tilbydere av eksempelvis apper som brukes i skolen?

Rådmannen har gjort følgende vurderinger:

- ROS, DPIA og tekniske løsningsbeskrivelser er kvalitetsdokumenter der informasjonssikkerhet er vurderingstema.
- Kommunen har kontroll på porteføljen av hva som brukes av skolene.
- Kommunen har en sentral styring av apper på elevens iPad.
- Leverandører med sine underleverandører er rettslig bundet ved Databehandleravtaler.
- Rådmannen har utarbeidet interne rutinebeskrivelser for å minimere restrisiko ved bruk av digitale verktøy.
- Rådmannen ber om bekreftelse på sletting fra leverandører når digitale programmer tas ut av porteføljen.
- Persondata slettes når elever flytter ut av kommunen eller slutter i grunnskolen.

3) Hvilke rettslige grunnlag bygger behandling av skoleelevers personopplysninger i Drammen kommune på? Hvilke tiltak vil rådmannen gjøre for å følge opp sikring av de spesifikke tilfellene knyttet til Feide og Kikora som beskrevet over?

Opplæringsloven §§1-3 og 1-4, samt forskrift til opplæringsloven kapittel 3 regulerer skolens plikt til tilpasset opplæring og vurdering. Opplæringsloven §2-3 gir retning for innhold og vurdering i grunnskolen, der LK20 er skolens sentrale styringsdokument.

Feide er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning. Drammen kommune bruker Feide-innlogging for ansatte og elever. Det rettslige grunnlaget for behandling av personopplysninger for skoleelever er hjemlet i opplæringsloven, men i tillegg samtykker elevene selv ved første gangs pålogging av systemer i Feide. Samtykke brukes i liten grad innenfor offentlig sektor - nasjonal særlov eller myndighets utøvelse (allmenn interesse), jf. personvernforordningen art. 6 nr. 1 bokstav c og e.

Eleven kan sammen med foresatte logge seg på innsynsløsningen til Feide. Når en sluttbruker logger på en tjeneste i Feide får han eller hun en liste over hvilke personopplysninger som blir sendt til tjenesten. Sluttbrukere kan når som helst gå til innsyn.feide.no og få full oversikt over hvilke tjenester som mottar hvilke data. Rådmannen vil sikre at skolene gjør denne tjenesten kjent for foresatte.

En av de viktigste fordelene med Feide er at sluttbrukernes personvern styrkes. Dette fordi Feide gir kontroll på dataflyten. Feide gjør det mulig for sluttbrukere og vertsorganisasjoner å holde oversikt over hvilke tjenester som mottar hvilke data, på tross av en stadig økende mengde digitale tjenester.

Ved kommunesammenslåingen ble det inngått avtale med Kikora, og det ble gjort ROS-vurdering ut fra Databehandleravtalen. Kikora er rettslig bundet av sin Databehandleravtale. I juridisk forstand er ikke elevarbeid personsensitive opplysninger, men personopplysninger med interesse som bør minimeres.

Drammen kommune har i forbindelse med dette svaret sendt en forespørsel til Kikora for å kvalitetssikre detaljer rundt lagring, sletting og deling av personopplysninger i løsningen. Dersom Kikora ikke svarer opp henvendelsen fra kommunen på en tilfredsstillende måte vil kommunen gjennomføre en ny ROS-analyse og vurdere tiltak.

4) Kan rådmannen, på generelt grunnlag, garantere for at innbyggeres persondata ikke deles med tredjeparter som kommunen samarbeider med, uten at innbyggerne (herunder myndige innbyggere, eventuelt foresatte på vegne av ikke-myndige barn) har gitt aktivt samtykke til dette?

Generelle tiltak for informasjonssikkerhet og personvern i Drammen kommune:

1. Porteføljestyring med kvalitetskontroll og ressursallokering samt godkjenning før drift (ROS, DBA, DPIA)
2. Opprettelse av Informasjonssikkerhetsråd som skal sikre en velfungerende informasjonssikkerhetsadministrasjon med forankring i utvidet ledergruppe
3. Eget personvernombud – rådføres i prosesser og saker
4. Opplæring og bevisstgjøring av ansatte på området (e-læringsmoduler og fokusområder for internkontroll i 2021 er bl.a. personvern)
5. Kontrollutvalget bestilte i 2020 en revisjon på personvern – endelig rapport fremlagt i kommunestyret 4. mai 2021

Mer inngående til det siste spørsmålet

16. juli 2020 avsa EU-domstolen en prinsipielt viktig dom om overføring av personopplysninger mellom EU/EØS og USA, også kalt Schrems II-dommen. Dommen har potensielt store konsekvenser for alle virksomheter som i dag benytter seg av sky-tjenester, og særlig fordi nesten alle leverandører et sted i verdikjeden benytter seg amerikanske selskaper. Selve sky-lagringen i dag ligger ofte hos de fire store: Microsoft Azure, Amazon Web Service, Google Cloud Platform eller IBM Cloud.

Bruk av skytjenester innebære ofte at noen av personopplysningene overføres til land utenfor EU/EØS, såkalte tredjeland. Dommen konkluderer med at Privacy Shield som overføringsgrunnlag mellom virksomheter i EU/EØS og USA er ugyldig. Årsaken er bekymringen for at personvernet til de registrerte ikke kan ivaretas på lik linje i USA som i EU/EØS, grunnet amerikanske myndigheter tilgang til personopplysninger i forbindelse med enkelte overvåkningsprogrammer. Av samme grunn vil det være vanskelig å benytte andre overføringsgrunnlag, som EU-kommisjonens standarsbestemmelser, da kravene til beskyttelsesnivå som stilles i dommen i praksis vil være vanskelig å oppfylle.

Dersom kommunen skal overføre opplysninger til en leverandør som skal behandle personopplysninger på vegne av kommunen, inngås det i dag en databehandleravtale. Dersom opplysningene skal overføres

til tredjeland, skal det i tillegg etablere et gyldig overføringsgrunnlag. Frem til nå har slike overføringsgrunnlag bestått av Privacy Shield (en sertifiseringsordning der mottakeren av opplysningene sertifiseres i henhold til EU-US Privacy Shield rammeverket) eller ved bruk av EU-kommisjonens standardbestemmelser («Standard Contractual Clauses»). Overføringer av personopplysninger til USA basert på Privacy Shield er nå å anse som ulovlig. Det påpekes at EU-kommisjonene er i ferd med å ferdigstille de nye standardkontraktene som skal være mer presise enn de gamle, og vil kunne fungere som et lovlig overføringsgrunnlag.

Drammen kommune har startet arbeidet med å skaffe seg en oversikt over alle kommunens databehandlere med henblikk på om det skjer overføring av data til tredjeland, samt hvilke overføringsmekanismer som benyttes der slik overføring skjer. Dette er et stort arbeid som i praksis startet opp rett før årsskiftet 2021. På grunn av pandemien har det vært vanskelig å øke intensiteten og fremdriften i dette arbeidet. Det forventes at dette arbeidet kan strekke seg inn i 2022.