

Overordnet vurdering av personvern i iPad-universet

Versjon 1.0, sist oppdatert 27.01.23

Dette dokumentet er en overordnet beskrivelse av personvern i iPad-universet, og vil kun ta for seg det som er spesifikt for appene som brukes på iPad. Dokumentet er et supplement til "Overordnet beskrivelse av personvern i digitale læremidler", og kan brukes som et grunnlag når man skal gjøre risikovurderinger og personvernkonsekvensvurderinger (DPIA) av tjenester/apper i Osloskolen.

Viktig presiseringer:

- når det refereres til "apper", gjelder det *kun* de appene som er tilgjengelige i og lastes ned på iPad gjennom Apple School Manager.
- Appene som brukes på iPad finnes også ofte i Web-versjon, hvor det i stor grad er grensesnittet som er ulikt. I denne vurderingen er det kun app-versjonen som er hensyntatt.
- Det er kun bruken av appen ifm. undervisning/skole som vurderes. Bruken utenfor dette faller utenfor Osloskolens behandlingsansvar.

Innhold

Innledning.....	2
Apple, Apple School Manager og personvern.....	3
Gratis apper og reklame.....	4
Lightspeed.....	4
1. En systematisk beskrivelse bruk av apper.....	6
Livssyklus.....	6
Behandlingens art.....	6
Behandlingens omfang.....	7
Behandlingens formål.....	8
Konfidensialitet.....	8
Integritet.....	8
Erfaringer.....	8
Ulike datasett og formål.....	8
Kilder, mottakere, informasjonssikkerhet og ansvarsforhold.....	8
2. Nødvendighet og proporsjonalitet.....	8
Sentral infrastruktur.....	8
Dataminimering.....	9
Riktighet.....	9

Lagringsbegrensninger	9
De registrertes rettigheter	9
De registrertes friheter	9
Bruken av apper representerer ingen begrensninger i forhold til Den europeiske menneskerettskonvensjonen.....	9
3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene.....	9
Risiko: manglende reelle medbestemmelser	9
Risiko: Manglende reell åpenhet.....	10
Risiko: manglende forutsigbarhet ved behandlingen.....	10
4. Ledelsens validering av overordnet vurdering av personvernkonsekvenser i apper	10
Sammenstilling og presentasjon av funn	10
Råd og anbefalinger fra personvernombud (personvernforordningen artikkel 35 nr. 2).....	11
Synspunkter fra de registrerte eller deres representanter (personvernforordningen artikkel 35 nr. 9). ..	11
Ledelsens gjennomgang, beslutning og godkjenning	11
Versjonshistorikk.....	11

Innledning

Nettbrettene som brukes i Osloskolen er iPad fra Apple, og når en skole ønsker å ta i bruk en ny app, ber lærer IKT-ansvarlig ved skolen om å kjøpe/laste ned appen via Apple School Manager. Appen gjøres så tilgjengelig for klassen/faggruppen som skal bruke den basert på informasjon hentet fra det skoleadministrative systemet IST Everyday (grunnskole), Visma InSchool (videregående skole) eller SITS (voksenopplæring). Både skolen og Utdanningsetaten kan sette policyer (tekniske innstillinger) i appen for å regulere hva slags funksjonalitet som skal være gjeldende for den enkelte app via Lightspeed. For å være sikker på at man ivaretar elevene og lærernes personvern, er det nødvendig å gjennomføre personverngodkjenning av appene som skal brukes i skolene – før de tas i bruk. Skolene har tidligere hatt et sentralt ansvar for å godkjenne appene de ønsker å bruke, men dette er flyttet til sentral administrasjon (Utdanningsetaten) for å effektivisere arbeidet og unngå at alle skolene må gjøre samme vurderinger. Det er et stort omfang med apper, og det tar derfor noe tid å få oppdatert alle apper i henhold til ny rutine. Hvordan dette skal gjøres er beskrevet i avsnitt om livssyklus for app i "*Overordnet vurdering av personvern i digitale læremidler*". Både Apple, Apple School Manager og Lightspeed er beskrevet i dette dokumentet.

Fokuset i denne beskrivelsen av iPad-universet er å gi et overordnet bilde av hvordan dagens situasjon er, med fokus på hvilke risikoer som er knyttet til bruk av apper på iPad. Dette vil inkludere personvern i Apple-universet, og hvordan iPad og apper administreres i Osloskolen. Denne vurderingen kan brukes som et grunnlag til mini-DPIAer og risikovurderinger som skal gjennomføres av de ulike appene.

Apple, Apple School Manager og personvern

Apple School Manager er portalen til Apple for utdanningsinstitusjoner, hvor skolene kan velge å kjøpe betalte versjoner og laste ned gratisversjoner av apper for enkeltbrukere og større grupper (klasser/trinn). Appene tilgjengelig i Apple School Manager er enten utviklet av Apple eller ulike utviklere, heretter referert til som "leverandører". Omfanget av apper tilgjengelig i Apple School Manager er tilsvarende App Store (for privatbrukere), og i mars 2016 var det over 1 millioner apper designet spesielt for iPad. Leverandørene av apper kan være alt fra enkeltindivider til store globale selskaper. Leverandørene velger selv hvilke priser appene skal ha.

Alle apper må følge Apple sine retningslinjer, som legger vekt på at produktene skal være designet til å begrense innsamling og bruk av data, og at behandlingen skal være mest mulig åpen og kontrollert. Apple legger vekt på at alle appene som distribueres via Apple School Manager skal ha de høyeste kravene til personvern, sikkerhet og innhold. Her er det viktig å poengtere at disse kravene er ulike mellom land, og det er dermed ingen garanti for at de er vurdert ut fra samme krav som vi har i Norge (Personvernforordningen ift. personvern). Generelt gjøres dette på to måter:

1. Apple har tilgjengeliggjort en rekke [verktøy](#) som leverandørene kan bruke i utviklingen av nye apper, og
2. Apple sjekker apper for skadelig programvare, og avviser/fjerner apper med kritikkverdig, skadelig, utrygt eller ulovlig innhold.

Apple har utviklet en funksjonalitet i iPadOS 15 som lar brukerne kontrollere og overvåke hvordan apper bruker deres data i større grad enn tidligere. Denne funksjonaliteten kalles Personvernrapport, og det er vurdert i Utdanningsetaten at dette en funksjonalitet som ikke skal brukes i Osloskolen, verken ifm. vurdering av apper eller for å kontrollere hvor leverandører sender data. Loggingen omfatter kun IP-adresser og ikke innhold som sendes. Vurderingen er i hovedsak basert på at det ikke er ønskelig eller hensiktsmessig å hente ut denne type informasjon fra den enkelte elevs iPad, i tillegg til at det etter vår vurdering er i en gråsoner ift. overvåkning. Per nå er det en funksjonalitet som ikke styres sentralt fra, og dersom funksjonaliteten skruses på er dette utenfor Osloskolens behandlingsansvar, og noe elev/foresatt selv er ansvarlig for.

Med iPadOS15 er det også en funksjonalitet som gjør at appen ber om brukerens tillatelse når man tar den i bruk, her skal brukeren svare "be om ikke bli sporet".

Appene i Apple-universet er [klassifisert](#) i ulike aldersgrupper (4+, 9+, 12+, 17+, PG) og kategori (utdanning, barn, spill, etc.) basert på hva slags innhold appen inneholder. Aldersgrensene er i stor grad anbefalt, men i noen tilfeller gjelder juridiske føringer i forhold til personvern som setter grense ved 13 år. Dersom det samles inn informasjon om barn under 13 år, skriver leverandør at det krever samtykke fra foresatte. Disse aldersgrensene avviker i noen tilfeller fra Pan European Game Information's (PEGI) definisjon av aldersgrenser, og det er disse retningslinjene Osloskolen har valgt å følge da de er tilpasset norske forhold. Osloskolen skal ikke bruke samtykke som behandlingsgrunnlag, og bruken av appene vil være hjemlet i personvernforordningen artikkel 6 og/eller 9, samt opplæringsloven §2-3, §3-4 eller §9 A. Behandlingsgrunnlag er ytterligere beskrevet i "*Overordnet vurdering av personvern i digitale*

læremidler". Apple skriver på sine egne hjemmesider at de overvåker kategoriene, og sikrer at apper som publiserer er i henhold til selskapets retningslinjer.

Apple opprettholder [sertifiseringer](#) i samsvar med ISO 27001- og 27018-standardene for Apple School Manager.

Man kan lese mer om Apple og personvern på nettsidene til Apple, [Apple og personvern i deres privacy policy](#), og om [Apple School Manager](#).

Gratis apper og reklame

Ved bruk av apper er de største utfordringene knyttet til leverandører, dette står beskrevet i "*Overordnet vurdering av personvern i digitale læremidler*".

Det som er litt spesielt for bruk av apper, er at en del av disse er gratis mot at brukerne utsettes for reklame og leverandøren samler inn en del aktivitetsdata om brukeren. Det vil si at man ikke trenger å betale for å bruke dem, men man aksepterer at leverandør samler inn en del aktivitetsdata. Dette er apper man bør unngå å bruke, da det er vanskeligere å regulere hva leverandøren samler inn og gjør med denne type data. I tillegg utsettes brukeren ofte for reklame, noe man skal unngå ihht Opplæringsloven §9-6. Skal gratis apper godkjennes til bruk, skal det være under to forutsetninger:

- Leverandør gir tilstrekkelig garanti og informasjon om hvordan de bruker dataen.
- Utdanningsetaten har ekstra krav i vurderings- og godkjeningsprosessen. Dette inkluderer blant annet at det undersøkes hva slags forretningsmodell leverandøren har, samt hva og hvordan de deler informasjon med underleverandører. Videre skal det etableres gode retningslinjer for bruken av appen i Osloskolen. Dette inkluderer informasjon om hva slags informasjon skal/ikke skal legges inn i tjenesten, rutiner for sletting av informasjon, etc.

Lightspeed

Lightspeed er Osloskolens Mobile Device Management-løsning (MDM), som gjør det mulig å administrere iPadene som brukes. Det er dette som gjør at man kan bruke apper i den grad man kan idag, da man kan regulere bruken både sentralt fra skoleeier og på den enkelte skole. Dette ved at man kan blokkere apper som ikke skal brukes, tildele og trekke tilbake lisenser, identifisere brukte og ubrukte lisenser, og sette policyer for bruk av apper. Dette kan for eksempel være å justere hva slags funksjonalitet som skal være tilgjengelig (bruk av kamera, deling via AirDrop, etc).

På denne måten kan man regulere og ha kontroll over hvordan man bruker nettbrett og apper, samt i noen grad hva slags tilgang appen skal ha til informasjonen som samles inn i appen og på nettbrettet.

IKT-ansvarlige er administrator for Lightspeed ved sin skole, og kan enkelt rulle ut apper automatisk gjennom Lightspeed etter den er kjøpt/lastet ned i Apple School Manager. I Lightspeed kan IKT-ansvarlig forenkle oppsetts prosessen for brukerne, konfigurere enhetsinnstillinger og distribuere apper til de rette gruppene. Dette ved at skoleadministrativt

system (IST Everyday) er koblet til Lightspeed, og man kan tildele roller, ansvar og tilgang til appene basert på informasjon om klasse, faggruppe, lærer, etc.



Det er viktig å merke seg at selv om Lightspeed gir god oversikt og muligheter til å regulere bruken, er det ikke dermed sagt at personvernet automatisk ivaretas. Dette da det ikke er alt man kan regulere, og noe av funksjonaliteten vil være standard og ikke mulig å skru av fra leverandør/underleverandørs side. Det er derfor viktig at det gjøres gode vurderinger av appene som skal brukes på skole, både lokalt på den enkelte skole og sentralt i administrasjonen. Dette for å sikre at man opererer i henhold til regelverk og sikrer at tilstrekkelige avtaler er på plass, parallelt med at man sørger for organisatoriske tiltak internt i Osloskolen, som opplæring/bevisstgjøring av lærere og elever i god skikk og bruk.

I løpet av høsten 2021 kommer det en ny versjon av Lightspeed (14.5) som gjør det mulig å se hva slags informasjon brukerne deler med de ulike appene. Dette vil også gjøre det enklere å fjerne apper man ser medfører en risiko for brukerne Osloskolen ikke kan akseptere. Det vurderes også om appkjøp skal gjøres sentralt via skoleeier, fremfor hos hver enkelt skole. Dette vil gjøre det enklere å ha overordnet kontroll over apper, begrense unødvendig kjøp, samt effektivisering av prosessen med å godkjenne nye apper ift. personvern. Dette vil redusere risikoen for at skoler laster ned og tar i bruk apper uten at personvernet er vurdert tilstrekkelig.

Det er utarbeidet grunnkurs for IKT-ansvarlige i bruk av Lightspeed, som inkluderer forslag til årsplan for å rydde og oppdatere for å sikre at grupper og lisenser er riktig ved skolestart, nyttår og skoleslutt.

Datatilsynet har utarbeidet en [liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA](#) i henhold til personvernforordningen artikkel 35-4 og artikkel 57-1 bokstav k. Apper som evaluerer læring, mestring eller trivsel faller inn under et av punktene i denne listen:

- Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager. Dette inkluderer alle utdanningsnivåer, fra barne- og ungdomsskole, videregående skoler og høyere utdanning. (Sårbare registrerte og systematisk monitorering.)

Å evaluere elevenes læring, mestring og trivsel er en plikt som reguleres i opplæringsloven med forskrift. Hjemmelsgrunnet blir belyst i "Overordnet vurdering av personvern i digitale læremidler", under avsnitt om "nødvendighet og proporsjonalitet".

Datatilsynet har også laget en liste over når det ikke kreves vurdering av personvernkonsekvenser. Dette punktet i listen er bakgrunnen for at det utarbeides en overordnet beskrivelse av iPad-universet, og denne beskrivelsen kan ligge til grunn i vurderingene som gjøres av de ulike appene som evaluerer læring, mestring eller trivsel:

- Dersom behandlingens art, omfang, sammenheng og formål er veldig lik en behandling det allerede er gjennomført en vurdering av personvernkonsekvenser for. I slike situasjoner kan resultatet fra den foreliggende vurderingen for lignende behandlinger brukes.

Begrunnelsen for dette er at appene har mye til felles:

- Tilgjengelig via samme plattform (Apple School Manager)
- Apple hevder å ha et strengt regime på at appene som ligger tilgjengelig der har vært gjennom en vurdering av Apple ift. personvern, informasjonssikkerhet, etc.
- Man kan sette en del policyer i Lightspeed til hva man kan tillate i Appene, og man kan styre både fra sentralt (Utdanningsetaten) og fra skoleledelsen på hver enkelt skole.

Det vil være nødvendig å gjøre en vurdering av hver enkelt app for å vurdere behov for å gjennomføre DPIA.

For å sikre kvalitet og innhold ihht. lovkrav (personvernforordningen artikkel 35-7) i denne vurderingen, ligger Datatilsynets sjekkliste for vurdering av personvernkonsekvenser (DPIA) som grunnlag. Strukturen videre er:

1. En systematisk beskrivelse av behandlingen.
2. Nødvendighet og proporsjonalitet.
3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene.
4. Ledelsens validering av DPIA

1. En systematisk beskrivelse bruk av apper

Livssyklus

Proessen å vurdere apper til iPad er lik for de andre universene, og beskrevet i «Overordnet vurdering av personvern i digitale læremidler».

Behandlingens art

Personopplysninger om elever og ansatte som bruker en app, kan bli tilgjengelig på disse måtene – dette kan omtales som aktivitetsdata:

- **Brukergenerert innhold hos Osloskolen:** hvilke oppgaver eleven har jobbet med og resultatet av det, informasjon om eleven, hvor ofte og hvor lenge eleven har brukt appen, identifikatorer som IP-adresse.
- **Brukergenerert data hos app-leverandør:** eventuell innloggingsinformasjon, bruksmønster, informasjon brukeren legger inn (om seg selv eller andre). Dette kan være aktivitetsdata (hva en elev har gjort i appen av oppgaver og resultater fra disse), eller vurderingsdata (hvordan en lærer har vurdert elevarbeider eller score på oppgaver med automatisk retting). Beskrivelse av denne type behandling skal dokumenteres i databehandleravtale/SCC.
- **Brukergenerert data hos Apple (via iPad):** personopplysninger fra kontoen, kjøp og nedlastningene til brukerne, for å
 - Kunne levere innholdet brukeren kjøper og laster ned.
 - Skreddersy/tilpasse funksjoner og tilpasse anbefalinger til apper, man kan velge å fjerne tillatelsen til bruk av disse dataene.
 - Få informasjon om hvordan brukerne bruker enheten.

Utfordringen med bruk av apper er at de fleste har ulike leverandører. Annet enn at man laster ned app fra samme sted, bruker samme bruker for å opprette konto (skoleplattformbruker) og at man kan sette noen policyer via Lightspeed, er det ikke noen større likheter i appene.

Behandlingens omfang

Hvilke apper skolen ønsker å ta i bruk bestemmes av den enkelte skole. Elevene har ikke mulighet til å laste ned apper fritt selv, og brukeren deres på iPad er koblet opp mot skoleplattformbruker eller administrert Apple-ID.

Når elever bruker disse ressursene, legger de igjen aktivitetsdata, Aktivitetsdata fra elevers bruk blir samlet inn og behandlet av de ulike leverandørene. Dataene eies av eleven selv, men forvaltes av skoleeier og reguleres av databehandleravtalen mellom den enkelte leverandør og skoleeier.

Omfanget av det som lagres om den enkelte elev er avhengig av omfanget av bruk. Det er ulikt fra skole til skole i hvor stor grad de benytter seg av digitale læremidler til undervisningen og hvor mye tid hver enkelt elev bruker i hver enkelt app. Jo større del av undervisningen skolen velger å gjennomføre på i det digitale rom, jo større del av elevenes aktiviteter blir digitale. For eleven selv vil bruken av digitale læremidler ligne på den analoge parallellen: Skriveboka husker hva du skrev i forrige skrive økt slik at du i neste økt kan fortsette der du slapp. Eleven er også vant med lærers vurderingsplikt og at lærer vil hente fram tidligere besvarelser som er utført innenfor en vurderingsperiode slik at dette inngår i det totale vurderingsgrunnlag. Dette danner de generelle rammene for lagringstid.

Aktivitetsdata skal i skolesammenheng ikke omfatte private opplysninger av typen adresse, opplysninger om økonomi, bekjentskapskrets, eller liknende. Denne informasjonen samles kun inn dersom brukeren selv har lagt inn denne informasjonen eller logger på fra privat brukerkonto, og det skal unngås. Det er også tilfeller hvor leverandøren logger lokasjonsdata fra brukeren (basert på hvor enheten er), men dette kan man som oftest skru av funksjonalitet for.

Aktivitetsdata av særskilte kategorier av personopplysninger, som for eksempel opplysninger om helse, rase og religion (personvernforordningens artikkel 9) skal begrenses.

Behandlingens formål

Formålet med behandlingen (bruk av digitale læremidler) er beskrevet i «*Overordnet vurdering av personvern i digitale læremidler*», da formålet er felles for alle universene.

Konfidensialitet

Som et resultat av økt fokus på personvern og informasjonssikkerhet, ser man også at leverandørene har et fokus på dette og at konfidensialitet skal ivaretas. Dette er ofte beskrevet i personvernerklæringene til leverandørene, og skal adresseres i DBA/SCC, ROS og eventuelt mini-DPIA.

Integritet

Vurdering av elevarbeid får konsekvenser både for elevens videre valgmuligheter og motivasjon. Det er derfor avgjørende at personopplysninger om elever og deres aktivitet er korrekte. Leverandørene har som regel oppgitt i personvernerklæringen hva brukeren må gjøre for å få innsyn i informasjonen de behandler om brukeren. Dette skal også være regulert i databehandleravtale/SCC.

Erfaringer

Utfordringen knyttet til bruk av apper er at mange av leverandørene er utenfor EU/EØS, og dermed har andre reguleringer og krav. Man ser at det er stort fokus på personvern generelt, men i vurderingsprosessen av apper er det viktig å undersøke hva slags informasjon leverandør behandler, hvor informasjonen lagres, om de har andre reguleringer man vet er i strid med det Osloskolen må forholde seg til, og hvilke underleverandører som eventuelt brukes.

Ulike datasett og formål

Appene i universet deler i utgangspunktet ikke data på tvers, da skal dette i henhold til Apples nyeste operativsystem bes om samtykke til. Hva slags informasjon som behandles og formål med behandlingen for hver enkelt app er ytterligere beskrevet i produktspesifikke nettsider på Osloskolens hjemmesider.

Kilder, mottakere, informasjonssikkerhet og ansvarsforhold

Alle problemstillinger i dette avsnittet er ivaretatt i databehandleravtale/SCC i apper som er godkjent.

2. Nødvendighet og proporsjonalitet

Beskrivelse av personvernprinsippene, rettslig grunnlag, læringsplaner og sentrale føringer står nærmere beskrevet i "*Overordnet vurdering av personvern i digitale læremidler*".

Sentral infrastruktur

Hver enkelt app har egen infrastruktur, og den sentrale infrastrukturen vil i dette tilfellet være knyttet til mulighetene man har til regulering/kontroll rundt bruk av apper gjennom Lightspeed. Dette ved at det settes policyer både sentralt fra skoleeier og ved den enkelte skole. IKT-

ansvarlige har tilgang til begrunnelse for valgte policyer, samt forutsetninger for hvilke valg som kan gjøres på skolenivå.

Dataminimering

Dataminimering ivaretas ved at hver enkelt iPad-app skal gjennomgå en egen godkjenningsprosess (se avsnittet «Livssyklus»). I denne prosessen må man kartlegge og begrunne hvorfor appen skal ha tilgang til informasjonen den har. Godkjenningsprosessen skal sikre at det kun åpnes for data som er nødvendig i forhold til formålet som er definert.

Riktighet

Se avsnittet *integritet* under "*Hvilken sammenheng behandlingen utføres i («kontekst»)»*."

Lagringsbegrensninger

Lagringsbegrensninger avtales i databehandleravtale/SCC mellom skoleeier og leverandør. Fagets varighet er utgangspunktet for vurdering av hvor lenge aktivitetsdata kan lagres hos leverandøren. Når det er snakk om bruk av apper, er det viktig å være oppmerksom på hvor leverandør lagrer informasjonen, samt hvilke underleverandører de bruker og hvor disse lagrer personopplysninger. Dette er ytterligere beskrevet i overordnet vurdering. I henhold til personvernforordningens artikkel 17, er det også viktig å være oppmerksom på hvilke sletterutiner leverandøren har, og når personopplysningene i appen skal slettes.

De registrertes rettigheter

De registrerte har rett til rettferdig og gjennomsiktig behandling, jf. personvernforordningen artikkel 12, 13 og 14. Bruken av apper i Oslo skolen skal ikke være basert på samtykke som behandlingsgrunnlag. Se avsnittet *Rettslig grunnlag* under *Personvernprinsippene i Overordnet vurdering av personvern i digitale læremidler*.

Data som registreres i digitale løsninger er initiert av at lærer i mer eller mindre grad bestemmer hva eleven skal arbeide med. Noen undervisningsopplegg har høy grad av lærerstyring, mens annen elevaktivitet kan være mer åpen og styrt av elevens egne valg og prioriteringer. Dersom en elev opplever at lærer legger opp til digitale læringsaktiviteter som eleven eller foresatte har innsigelser på, er dette en sak mellom lærer og elev på tilsvarende måte som for analoge læringsaktiviteter.

De registrertes friheter

Bruken av apper representerer ingen begrensninger i forhold til Den europeiske menneskerettskonvensjonen.

3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene.

Den generelle beskrivelsen av dette er beskrevet i "*Overordnet vurdering av personvern i digitale læremidler*". I det følgende er det dokumentert konkret for iPad-universet.

Risiko: manglende reelle medbestemmelser

Viser til tilsvarende avsnitt i overordnet dokument.

Risiko: Manglende reell åpenhet

En av de større utfordringene med bruk av apper er at det er vanskelig for brukerne å få innsikt og forstå hva slags aktivitetsdata som behandles, og hvorfor det behandles. Konsekvensen av dette kan være at eleven legger igjen digitale spor uten å være klar over dette, og at vedkommende ville agert annerledes dersom man var klar over situasjonen.

Det er derfor viktig at man i vurdering av den enkelte app får oversikt over hva slags informasjon som behandles, så man kun godkjenner apper hvor man har behandlingsgrunnlag for det – og at man i beskrivelse av tjenesten på nettsidene til Oslo skolen tydeliggjør hva slags aktivitetsdata som behandles om den enkelte.

Risiko: manglende forutsigbarhet ved behandlingen

De fleste apper utvikles i dag med fokus på personvern, og legger til rette for forutsigbarhet ved behandlingen. I en del apper, spesielt de utviklet mot utdanningssektoren, vil det være mulig å styre tilganger og innsyn i informasjon, og i disse tilfellene er det viktig at Oslo skolen har gode rutiner for å sikre at det kun er de med tjenstlig behov som får innsyn.

Utfordringen rundt personvern i apper vil i stor grad være rundt de appene som ikke er utviklet med utdanning som formål, da det ikke nødvendigvis er like tilrettelagt for tilgangsstyring, innsyn i aktivitetsdata for behandlingsansvarlig og at mange av de er gratis. Det er derfor viktig å gjøre gode vurderinger av om apper, for å sikre at leverandør ivaretar personvern tilstrekkelig.

4. Ledelsens validering av overordnet vurdering av personvernkonsekvenser i apper

Sammenstilling og presentasjon av funn

iPad-universet er i konstant endring, både i form av omfang av apper og kontinuerlige oppdateringer fra Apple og ulike leverandører. De største utfordringene knyttet til bruk av apper i Oslo skolen handler primært om kompleksiteten i antallet apper skolene ønsker å bruke, og at leverandørene i en del tilfeller er lokalisert utenfor EU/EØS, som kan føre til overføring av personopplysninger til tredjestater. Markedet begynner å ta innover seg de strenge personvernreguleringene innenfor EU/EØS og stadig flere land følger trenden med å oppdatere personvernregelverk, men det tar tid og det vil være nasjonale ulikheter mellom lovene. Arbeidet med å vurdere den enkelte app er også så stor, at Oslo skolen bør fortsette å engasjere seg i nasjonale tiltak for å dele og trekke på andres erfaringer og kompetanse.

Man kan ikke si noe samlet sett om iPad-universet ivaretar brukernes personvern tilstrekkelig, som en følge av kompleksiteten med leverandører. For å sikre at Oslo skolen ivaretar brukernes personvern ved bruk av iPad, er det derfor viktig å ha gode prosesser for personvern godkjenning og forvaltning av den enkelte app. Her er det spesielt viktig å vurdere behov for gjennomføring av DPIA, samt risikovurderinger som fokuserer på bruken av appen og leverandørforhold (lagring og eierskap av personopplysningene). Lightspeed gjør det mulig for Oslo skolen å regulere hva slags apper som kan tas i bruk på iPad, men det er viktig å huske at det muliggjør regulering av funksjonalitet og om man kan bruke appen eller ikke, men ikke hva slags aktivitetsdata som lagres hos leverandør og hvordan den enkelte bruker den.

Det er viktig at man har etablert en god prosess for forvaltning av appene, både i form av revidering av risikovurderinger og DPIA, og rutiner for sletting av både app og elevdata. Dette da det er mange leverandører som ikke har gode rutiner for automatisk sletting av personopplysninger i appen.

Utdanningsetaten har ansvar for å gjøre vurderinger av appene som Oslo skolen ønsker å ta i bruk, og beskrive hvilke som er godkjent for bruk og ikke. Det er innenfor denne rammen skolen kan velge hva de ønsker å bruke. Per i dag er det en policy og tillitsbasert rutine, og behov for ytterligere tiltak vurderes.

Råd og anbefalinger fra personvernombud (personvernforordningen artikkel 35 nr. 2)

Dette dokumentet ble sendt til personvernombudet i Oslo kommune november 2021, og gått gjennom 17.01.22. I etterkant av møtet ble det innarbeidet tilbakemeldinger fra personvernombud før dokumentene ble sendt på høring til de registrerte og deres representanter. Personvernombudets kommentar kan leses i "*Overordnet vurdering av personvern i digitale læremidler*". Det er ikke gitt spesifikke kommentarer på de enkelte universene. Personvernombud deltok også i høringsmøte med de registrertes representanter 04.05.22.

Synspunkter fra de registrerte eller deres representanter (personvernforordningen artikkel 35 nr. 9).

"Overordnet vurdering av personvern iPad-univers" oversendes til Foreldreutvalget for grunnopplæringen (FUG), Elevorganisasjonen (EO) og Utdanningsforbundet med invitasjon til å gi skriftlig tilbakemelding. Dette ble gjort sammen med de andre vurderingene som er gjort, og denne prosessen sammen med innspill fra de registrertes representanter er ytterligere beskrevet i "*Overordnet vurdering av personvern i digitale læremidler versjon 1.0*".

Ledelsens gjennomgang, beslutning og godkjenning

Denne overordnede vurderingen av iPad-universet ift. personvernkonsekvenser, inkludert rutine for personverngodkjenning, blir lagt til godkjent på ledernivå i Utdanningsadministrasjonen etter at innspillene fra Personvernombudet, FUG, EO og Utdanningsforbundet er implementert.

Versjonshistorikk

Versjon	Dato	Forfatter
0.8 utkast sendt til personvernombud for innspill	November 2021	Brian Jørgensen og Kaja Felix Sønslie (innleid konsulent)
0.9 – etter innspill fra personvernombud, sendes på høring til de registrerte	19.01.2022	Brian Jørgensen og Kaja Felix Sønslie (innleid konsulent)
0.91 klargjøring for språkvask	08.09.2022	Brian Jørgensen (UDE), Heli Kristiina Kananen og Kaja Felix Sønslie (innleide konsulenter)

1.0 Til ledergodkjenning	27.01.2023	Brian Jørgensen og Heidi Skjebstad
--------------------------	------------	------------------------------------