Personvern i digitale læremidler

06.05.2021

Innhold

Om oppdraget

Traq AS har fått i oppdrag av Pålogga AS for å gjennomføre en kartlegging av digitale læremidler i utdanningsmarkedet, med tanke på personvern.

Samlet problemstilling

Tilgjengelig dokumentasjon og standard avtaleverk fra leverandørene som regulerer forholdet mot skolene/utdanningsinstitusjonene har vært gjenstand for undersøkelsene og analysen. Vi har også vurdert personvernerklæringer, brukervilkår og samtykkeerklæringer som regulerer forholdet til sluttbrukerne/elevene/de foresatte, for å forsøke å vurdere hvordan personvernet totalt sett ivaretas.

Opplæringsloven brukes normalt som behandlingsgrunnlag i anvendelsen av disse læremidlene/appene.

Læremidlene tilbyr imidlertid ofte funksjonalitet som kan kreve annet behandlingsgrunnlag enn det som dekkes av opplæringsloven. Det er grenser for hvor både lovhjemmel, samtykke, interesseavveining kan benyttes, men dette er et vanskelig område og sterkt avhengig av den enkelte behandling. For eksempel kan bruk av GPS i visse tilfeller behandles med hjemmel i opplæringsloven, basert på hvilke tiltak som iverksettes.

Våre undersøkelser viser at det er behov for tydelig veiledning og at grenseoppganger for behandlingsgrunnlag må gås opp.

Om sektoren

Utdanningsmarkedet er preget av høy grad av innovasjon. Der de fleste andre sektorene i offentlig sektor over lang tid har hatt mange av de samme leverandørene - har man innen utdanningsmarkedet (Edtech) en flora av aktører, fra store, globale leverandører til mindre leverandører, som leverer produkter av ulike slag. Noen løsninger er fullt ut digitale, mens andre kan være et digitalt læremiddel som følger som et tillegg til en bok.

Innovasjonen og at det kommer tilfang av nye aktører i sektoren er veldig positiv for sektoren og noe andre deler av offentlig sektor kan drømme om. En rik flora av løsninger og nye løsninger er veldig bra i seg selv, men når man får et så bredt spekter av aktører og løsninger, kan det gjøre at det totale aktørbildet blir uoversiktlig.

I kjølvannet av personopplysningslovgivningen (GDPR) er det gitt veldig strenge rammevilkår som krever mye av leverandørene. Den enkelte leverandør må være sin rolle bevisst og ta et selvstendig ansvar for at reglene etterleves. Dokumentasjonskravet og leverandøransvaret er betydelig styrket sammenlignet med tidligere regelverk. Dette handler også om leverandørers modenhet for å kunne absorbere og etterfølge de til enhver tid gjeldende rettsregler.

Utfordringene er sammensatt, både mellom ulike aktører, men også noe mellom opplæringslovgivningen og personvernlovgivningen.

Fra et personvernperspektiv er det slik at hvis leverandørene ikke etterfølger regelverket og tar sitt ansvar, og om innkjøper ikke stiller krav eller er bevisst på sitt ansvar, så vil dette medføre at *elevenes personvern* utfordres løpende.

Datatilsynet publiserte en rapport om personvernet i skole og barnehage i 2014[1]. Utfordringsbildet mht personvern er mye av det samme som i dag, bare at vi har fått en sterkere grad av lovgivning ifm innføring av Personvernforordningen (GDPR) i 2018 og Schrems II i 2020.

Personvernutfordringen i skoler

Personvern handler blant annet om selvbestemmelse. For barn og unge i skole og barnehage, handler det om at foreldre og barn skal ha kontroll med hvordan opplysningene om barna blir brukt. Dette fordrer først og fremst åpenhet fra skolene sin side, med tanke på valg av kommunikasjonsløsninger og lagringsmedier.

Korona og situasjonen med utdanning

Koronasituasjonen mars 2020 gjorde at man fra lærerne og kommunens sin side omstilte seg raskt. Selv om man benyttet edtech-løsninger i ulik grad før korona var det mer som støtte til eksisterende undervisning. Man kan si at digitale hjelpemidler for første gang kom i "front" av undervisningen. Det har vært imponerende arbeid fra alle involverte, men slike prosesser gjør at man bør ta et steg tilbake for å vurdere hensiktsmessige. Vi diskuterer ikke det

---

1 https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvern-i-skole-og-barnehage---samlerapport/

pedagogiske, men vi vurderer det slik at en robust tilnærming fra innkjøpssiden, systematisk vurdering av personvern naturlig nok har blitt oversett i noen av prosessene. Det frigjør ikke ansvaret som ligger til den enkelte leverandør i å levere tjenester med "privacy by design/default/architecture" - i særdeleshet når man leverer produkter og tjenester til og for barn og ungdom. Ser man strengt på det burde dette ha vært innarbeidet ved første kontrakt/kontakt. Vi mener dog at alle parter må bære sin del av ansvaret i dette bildet og har skissert de ulike rollene og ansvarene i figuren under.

Ved at det tas i bruk mange forskjellige kanaler for å kommunisere med foresatte og elever, blir opplysninger om elevene lagt igjen på mange ulike steder, og med ulik grad av sikkerhet. Vi har sett tilfeller hvor skoleeieren ikke har kjennskap til dette og dermed heller ikke har utarbeidet retningslinjer for, eller gitt opplæring i, bruken av dette. Når ingen har vurdert sikkerhetsaspektene ved at opplysninger blir lagret hos en tredjepart, og heller ikke er kjent med at tredjeparten er å anse som en databehandler er sannsynligheten liten for at en databehandleravtale er på plass. En slik avtale er nødvendig for å sikre opplysningene.

Informasjon til foresatte og elever om hvorfor og hvordan opplysningene om elever blir behandlet, er en grunnleggende personvernrettighet. Uten informasjon har foresatte og elever ingen mulighet til å si ifra hvis de mener at skolen ivaretar personvernet på en kritikkverdig måte. Uten informasjon har de heller ingen mulighet til å be om innsyn, retting eller sletting – rettigheter som personvernlovgivningen gir.

Det er store variasjoner i økonomi og tilgjengelige ressurser hos skoleeiere (Kostra, SSB) - man er i veldig stor grad prisgitt hvordan leverandørene følger opp det til enhver tid regelverk.

Utvalg av leverandører

De utvalgte leverandørene er blitt valgt ut av en liste fra Pålogga. Dette er løsninger som har stor utbredelse, stor bruk og som har vært i markedet en periode. Følgende selskap har blitt vurdert:

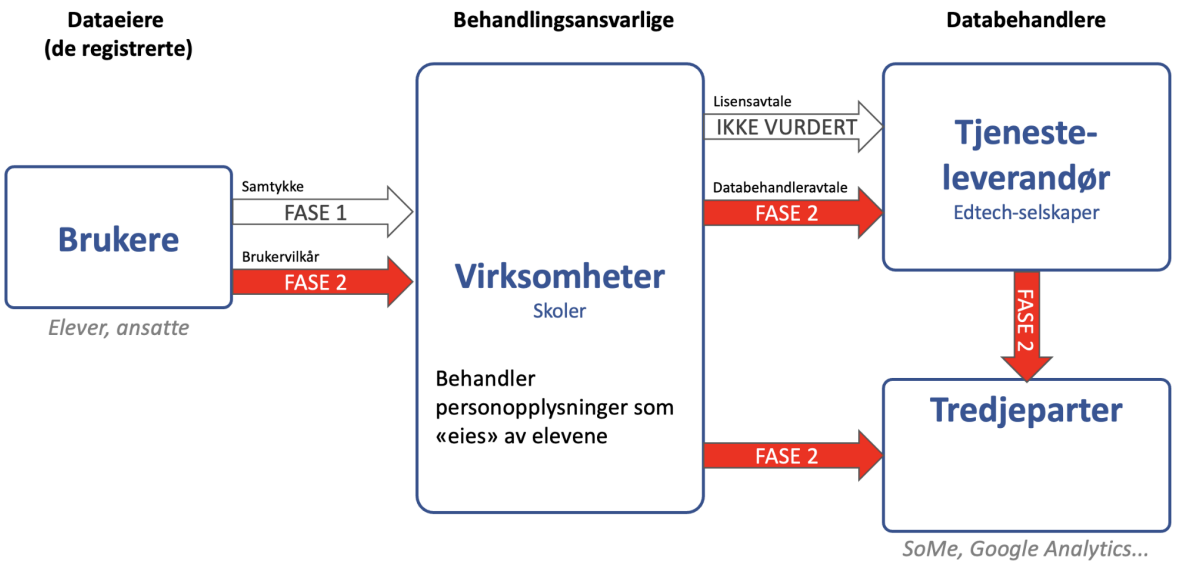
- Book creator
- Creaza
- Into words
- Kahoot
- Kikora
- Learnlab
- Micro:bit
- Microsoft Edu Tech
- Padlet
- Quizlet
- Salaby
- Screencast-o-matic
- Showbie
- Socrative

Fordi formålet med rapporten ikke er å henge ut enkeltleverandører men gi en samlet status over situasjonen med personvern i utdanningssektoren, vil vi videre i rapporten anonymisere selskapene.

Gjennomføring

I perioden fra oktober til desember 2020 gjennomførte Traq en første fase med vurdering av samtykkeerklæringene i utdanningsprodukter fra 15 ulike leverandører. Hovedfokus i første fase var å for å få oversikt over hvilke data som faktisk samles inn og hva sluttbrukeren samtykker til når de bruker disse løsningene. Resultatene ligger i tekst og tabell under.

I løpet av den andre fasen har Traq kontaktet leverandører for å få oversikt over hvilken informasjon som ligger inne i deres standard databehandleravtaler. Disse avtalene gir ideelt sett innsikt i hva som faktisk reguleres.



Undersøkelsen ble gjennomført i perioden fra januar 2021 til mars 2021. Som utgangspunkt sendte vi henvendelser til 16 leverandører (14 nevnt innledningsvis og to plattformer som er vurdert separat og ikke nevnt her) og vi fikk tilbakemelding fra kun fire av de vi har i rapporten her. De andre, 10 leverandører, har ikke respondert. I mangel av tilbakemelding gjennomførte vi undersøkelser basert på tilgjengelige personvernerklæringer og annen informasjon som er offentlig tilgjengelig. Vi har gjennomgått og sortert ut informasjon som kan være relevant. Dette er informasjon samlet i et bakgrunnsdokument/råmateriale for denne rapporten. Dette råmaterialet ble så gjennomgått og slutningene i denne rapporten er en samlet vurdering av dataene som er samlet inn samt en grundig vurdering av hver enkelt leverandør.

Vi opplever, tross den lave responsen på å motta databehandleravtalene, å ha et tilstrekkelig grunnlag for å kunne gi innsikt i problemstillingene og komme med noen forslag til tiltak.

Det er mange juridiske avveininger som kan gjøres basert på disse funnene og prosjektet har hatt dialog med advokatmiljø om disse perspektivene. Vi har ikke gått i detalj på de rettslige problemstillingene, men har ønsket å peke på utfordringene og kompleksiteten - at dette er sammensatte problemstillinger hvor det må løftes på flere områder - samt komme med noen anbefalinger basert på funnene.

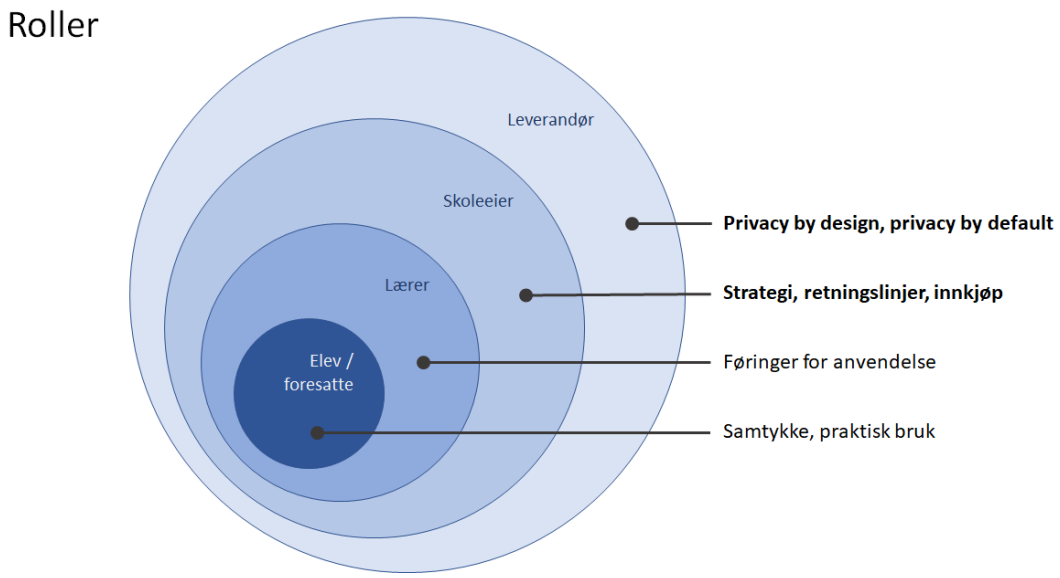
Ansvarsforhold

Det er kunden, her skoleeier / kommuner/ innkjøpere, som er ansvarlig for å sikre at databehandleravtaler etableres ved anskaffelse av digitale læremidler. Det er juridisk sett virksomhetens øverste leder som er ansvarlig, men oppgaven er vanligvis delegert.

Basert på erfaring fra tidligere antar vi at det sjelden gjøres tilpasninger av leverandørenes standard databehandleravtaler. Enkelte kommuner gjør dette, mens de fleste nok aksepterer standardavtaler som kommer fra leverandørene. Dette resulterer ofte i at innkjøper signerer

leverandørens avtaler uten å sikre at de virksomhetsspesifikke behovene innlemmes som del av avtaleverket.

Vi har satt opp en modell for hvilke roller og ansvar de ulike aktørene har:



Leverandøren har ansvar for at grunnlaget for personvern ivaretas i produktene, spesielt med tanke på at de kan ha store brukermasser både nasjonalt og globalt. Selv om det er behandlingsansvarlig som skal sikre at produktene som benyttes er i tråd med personvernprinsippene, så er det vanskelig å se for seg at leverandørsiden ikke har et selvstendig ansvar i dette. Prinsipper om "privacy by design" og "privacy by default" legger konkrete føringer for hvilke egenskaper produkter for dette markedet skal ha[2].

Skoleeier er behandlingsansvarlig, og ansvarlig for å ivareta personvernet til barn i barnehage og skole, ansatte og foresatte etter personvernforordningen (GDPR)[3].

Lærer er ansvarlig for føringer for den praktiske anvendelsen av produktet.

Eleven er sluttbrukeren og den som i praksis benytter sluttbrukerløsningen/produktet.

Foresatte samtykker på vegner av eleven for tjenester/områder i tilfeller hvor det ikke finnes annet rettslig grunnlag.

2 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

3 https://www.udir.no/regelverk-og-tilsyn/personvern-for-barnehage-og-skole/barnehage-og-skoleeiers-ansvar-gdpr/

Hovedfunn

Med en stor flora av leverandører som både er lokale men også globale, er det veldig vanskelig å finne vurderingskriterier som er felles for alle. Formålet/-ene for behandlingen varierer, samt at noen løsninger brukes på flere områder/ i flere fag, mens andre dekker veldig konkrete områder/ fag.

Vi har her tatt ut en del hovedpunkter fra analysen:

- *Det er ofte uklart hvilket behandlingsgrunnlag man bruker, om det er rene samtykkebaserte løsninger eller om behandlingen gjøres for å utføre en lovmessig plikt med grunnlag i opplæringsloven.*
- *Ingen felles struktur på personvernerklæringer. Ulik struktur bidrar til at det er vanskelig å sammenligne, følge opp eller få innsyn i dataene.*
- *Mange av virksomhetene blander samtykker og personvernerklæringer om hverandre.*
- *Som bruker blir man i liten grad informert om endringer i vilkårene.*
- *Man bør nok fra kommunen/ skolen sin side ha prosesser/ vurderinger av konkrete veivalg, f.eks. om en lærer kan aktivere lagring av biometriske opplysninger i Leverandør B sin løsning.*
- *Behov for veiledning i grensegangene mellom foreldre/foresatte, barn og skole/lærer. Hva må man eventuelt ha samtykke til fra foreldre/foresatte? Kan en lærer samtykke til biometri? Det er få løsninger som har tilrettelagt for samtykke fra foresatte, men de fleste av disse plasserer dette ansvaret hos skolen.*
- *Digital profilering av elever; når går grensen og hva kreves? Kommunen/skolen bør gi tydelig informasjon om hvor deres ansvar stopper og foreldrenes ansvar begynner.*
- *Funnene i undersøkelsen avdekker at mange skoler støtter seg for tungt på løsningene, og i mindre grad foretar selvstendige undersøkelser og tiltak. Dette er i stor grad sammenfallende med Datatilsynets årsrapport fra 2020[4].*
- *Mange av problemstillingene som undersøkelsen tar opp vil belyses ved bruk av Datatilsynets veiledere[5].*

Vi ser også at enkelte leverandører (f.eks. Leverandør B) gir mulighet for læreren til å aktivere biometri for klassen/ eleven. Ved bruk av slik funksjonalitet er det ytterligere behov for etablerte rutiner og prosesser hos den behandlingsansvarlige for å sikre personvernet[6].

Foresatte samtykker på vegner av eleven for tjenester/områder hvor det ikke finnes annet rettslig behandlingsgrunnlag. Det er dog noe usikkert på hvordan den enkelte skole/kommune/behandlingsansvarlig gjør dette. Noe veiledning på dette bør nok bli tydeligere da det i enkelte tilfeller kan virke som at læreren samtykker på vegne av elevene.

---

[4] https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsrapport-for-2020/spesielt-om-barn-unge-og-utdanning/

[5] Se f.eks. https://www.udir.no/regelverk-og-tilsyn/personvern-for-barnehage-og-skole/veiledere-fra-dt/ og https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/

[6] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/

Vi opplever i kartleggingen at leverandørene blander personvernerklæringer, samtykker og brukervilkår. En avklaring/ opprydning i dette vil gi rask effekt. Det bør kunne være mulig å standardisere og spisse dette fra innkjøpers side for a) å oppnå mulighet for å sammenligne på tvers av løsninger, b) gjøre det enklere for brukere, og c) enklere kunne gjennomføre ROS-analyser og vurderinger av leverandører og løsninger. Datatilsynet i Danmark har vedtatt en standard databehandleravtale som også kan brukes av norske virksomheter[7].

Våre funn og vurderinger er gitt i kulepunkter, med kursivert skrift, i den løpende teksten under:

- *De aller fleste løsninger har en lang vei å gå på kommunikasjon. Ihht personvernforordningen skal personvern- og samtykkeerklæringer være tilpasset mottaker. I praksis betyr dette at det skal være enkelt og kortfattet, uten lange, juridiske utgreiinger, og det skal ikke gjemmes bort i bruksvilkår eller andre lange dokumenter.*
- *Om rutiner for å melde endringer mtp leverandører er på plass. Det er mange løsninger som ikke varsler ved endringer i vilkår, og kun to løsninger har funksjoner hvor det innhentes nye samtykker ved endringer. Mye tyder på det trengs bedre prosesser og løsninger for å sikre at skolen alltid har et gyldig behandlingsgrunnlag når dette kreves.*
- *Høy grad av usikkerhet om hva som skjer ved tilbaketrekking av samtykket.*
- *Uklarheter rundt hvilke data som deles med hvem, og når, samt hvordan dette kan reguleres fra behandlingsansvarlig sin side.*

Det bør være av alle sin interesse at man får en ryddighet i dette, all den tid de digitale verktøyene må skape og opprettholde tillit. Hvis løsning, rutiner og prosesser svekker tilliten ikke er tilstede er det fare for *digitalt-backlash*[8]. Digitalt-backlash består av økende motstand både mot de globale teknologiselskapene og enda dypere; mot at digital teknologi koloniserer store deler av hverdagen.

- *Det er stor variasjon i modenhet mellom leverandørene.*
- *Majoriteten av de vi undersøker fremhever at personvern er viktig, men synes likevel å ha lav grad av etterlevelse.*
- *Det er stor variasjon i praksis mellom leverandørene.*
- *Ulik lovgivning som er førende bak avtalene. I de løsningene vi har undersøkt gjøres blant annet lovverk fra Irland, Canada og Østerrike gjeldende.*

Leverandørmarkedet er en flora med anslagsvis 500-1000 aktører, hvor noen er store globale aktører og noen er veldig små. I tillegg har man historisk sett også hatt mye utskiftning av aktører. Noen blir oppkjøpt, mens andre klarer seg ikke og forsvinner ut. Det bør tilbys

[7] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet/

[8] https://www.ks.no/contentassets/88fcd4bb46ca40969085566916d8ceba/zynk-endelig-trendrapport-ks.pdf s. 32

opplæring og veiledning til aktører som etablerer seg i markedet, og det bør vurderes om det kan lages en form for "sjekkliste" for de aktørene som ønsker å opptre i dette markedssegmentet.

Det er stor avstand fra å si at "personvern er viktig for oss" til å faktisk gjøre det viktig. Det er ønskelig at leverandørene i større grad fokuserer på å etterleve personvern fremfor å poengtere viktigheten.

I en del tilfeller trekkes utenlandsk lovgivning inn som førende i avtaleverket. Vi har funnet eksempler hvor lovgivning fra Irland, Canada og Østerrike gjøres gjeldende. Som kunde signerer en da på utenlandske avtalevilkår i norske kommuner. Dette tror vi at skolene/ kundene ikke alltid ser rekkevidden av, og oppfordrer til ekstra oppmerksomhet i slike tilfeller.

- *I undersøkelsen har vi fått liten respons når vi har sendt spørsmål til leverandørene, og mange har ikke besvart våre henvendelser i det hele tatt.*
- *Det er lav grad av åpenhet om leverandørenes arbeid med personvern; henvendelser og spørsmål om deres personvernpraksis blir ansett som negativt.*
- *Som sluttbruker er det i noen tilfeller vanskelig å stole på at informasjonen som er gitt i personvern- og samtykkeerklæringer er riktig.*
- *Fra et brukerperspektiv gir ikke løsningene trygghet med tanke på personvern, og/ eller de har mye å gå på å skape trygghet og tillit hos eleven.*

Kvaliteten i personvernprosesser er preget av variasjon, og tilhørende dokumentasjon er noen tilfeller direkte selvmotsigende. Eksempelvis finner vi ulike lister over tredjepartsleverandører hos samme leverandør, noe som medfører usikkerhet rundt håndteringen av personopplysninger.

Å skape tillit til tjenesten er viktig. Personvernundersøkelsen til Datatilsynet for 2020/2021 gir et tydelig bilde av hva som skjer når sluttbrukerne er usikre på om personvernet er ivaretatt i andre type løsninger[9].

Noen globale leverandører, samt Gyldendal, responderte raskt. Forøvrig er det liten eller ingen respons når man sender henvendelser til kontaktpunktet som er gjengitt som kontakt for personvernspørsmål. Det gir inntrykk av at dette er adresser som ikke sjekkes eller har etablerte prosesser for å håndtere slike forespørsler. Enkelte leverandører var kritisk til spørsmål om dette.

- *Etterlevelsen av regelverket rundt utførsel er varierende; personopplysninger føres i stor grad ut av landet, også til tredjestater.*

Det er varierende etterlevelse av regelverket rundt overføring av personopplysninger til tredjestat, jf. domfellelsen i den såkalte Schrems II-saken. Se f.eks. Showbie (navngis som

9 https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/nedkjolingseffekt/

eksempel da dette er åpne data), som Datatilsynet har gitt gebyr til en kommune for, men som de samtidig ikke vurderte med tanke utførsel av personopplysninger til tredjestat[10].

Dette er en global løsning som veldig mange kommuner benytter. Her legge man inn video, bilder, lyd, tekst, tegninger, vurderinger, informasjon om elever.

Det er svært få offentlige anskaffelser som vi kan se på en leverandør som feks Showbie, dermed er det usikkert hvorvidt det har blitt gjennomført en skikkelig vurdering av personvernet. Vi antar at om det hadde blitt gjennomført, så ville en slik type applikasjon blitt vurdert annerledes.

- *Hvordan er dataene lagret? Det bør nok stilles krav til at dataene i løsningen er kryptert.*
- *Mulighet for å stille enhetlige krav til sletterutiner? Det virker som det er veldig varierende på tvers av leverandører.*
- *Kommunen må kunne garantere at personopplysninger slettes når det ikke lenger foreligger behandlingsgrunnlag for behandlingen – for eksempel når brukerkontoen til en elev slettes - det er nok usikkert om det skjer her.*

I vurderingen er det flere tilfeller hvor personopplysninger ikke blir lagret i kryptert form. Vår klare anbefaling er at det stilles krav til at personopplysninger som lagres i løsningen(e) krypteres.

Sletting av personopplysninger bør følge en beste praksis. Enkelte løsninger sletter sannsynligvis ikke dine personopplysninger, og kan ha uryddige prosesser ut mot tredjepartsleverandører, mens andre har tidsbegrenset lagring etter at du har sagt opp brukerforholdet.

Ett av personvernprinsippene gjelder dataminimering; personopplysninger skal slettes innen rimelig tid etter at behandlingen er gjennomført, eller når behandlingsansvarlig ikke lenger har rettslig grunnlag for å beholde dem.

Det er veldig vanskelig å forstå at en leverandør f.eks. skal sitte i 18 måneder med personopplysninger etter at eleven har sluttet å bruke løsningen, eller har bedt leverandøren om å slutte å bruke personopplysningene. Her kan det være rom for å lage en veileder eller stille krav om beste praksis.

Den behandlingsansvarlige må kunne garantere at personopplysninger slettes når det ikke lenger foreligger rettslig behandlingsgrunnlag, for eksempel når brukerkontoen til en elev slettes. Våre undersøkelser gir ikke umiddelbar trygghet for om dette skjer.

- *Leverandørene har varierende syn på sin egen rolle og det tilhørende ansvaret som følger med i forholdet kunde-leverandør.*
- *Generelt kan det se ut som at kompetansen innen personvern er uforholdsmessig lav sett opp mot de personopplysningene som behandles i løsningene som er undersøkt.*

[10] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-gebyr-til-ralingen-kommune/

- *Responsen tyder på at en del av virksomhetene støtter seg på at regelverket ikke har vært håndhevet i særlig grad tidligere, og at tidligere praksis er tilstrekkelig.*

Funn knyttet til behandling og lagring av personopplysninger i digitale læremidler

Konkrete forhold vi har forsøkt å avdekke i denne fasen:

- Hvilke type personopplysninger samles inn (evt. også tekniske data)?
- Hvor lagres dataene (enhet, leverandør, cloud – hvilken cloud? Utenfor EØS?)
- Hvis personopplysninger behandles; hvordan og hvor godt er disse sikret?[11]
- Hvem er leverandør og underleverandører?[12]
- Blir data videreført/ solgt/ benyttet til markedsføring?
- Eventuelt andre data/ betraktninger om personvern og data

Generelle betraktninger for kommune / innkjøper

Det kan være fordelaktig at den enkelte lærer/ skoleeier kan foreta selvstendige pedagogiske vurderinger av Edtech-applikasjoner basert på den enkelte og sine behov, men fragmenterte innkjøp og en "spaghetti-infrastruktur" med et uoversiktlig leverandørbilde kan gå på bekostning av andre vurderinger som for eksempel personvern.

Generelt kan vi si at det må til en opprydding og opplæring i personvernerklæringer, samtykker, databehandler - i tillegg til tydelige rolle- og ansvarsavklaringer, både internt i virksomhetene og mellom aktørene. Det er også noen andre problemstillinger som kan være verdt å ta med videre:

- Kundene/innkjøper synes å ha lite kjennskap til løsningens detaljer rundt personvern før beslutning om innkjøp skjer.
- Det kan virke som at kunder støtter seg på leverandør og vurderinger gjort av andre (skoler etc.).
- Personvern synes å i stor grad være underordnet pedagogiske og bruksmessige egenskaper.
- Man følger sjelden en helhetlig strategi.
- En del av løsningene ses sjelden under regelverket for offentlige anskaffelser og havner dermed utenfor etablerte prosesser og vurderinger.
- Hvordan er personvernombudenes roller i utdanningssektoren vs andre sektorer (f.eks. helsesektoren)?

[11] Her kan det være aktuelt med en form for skala til internt bruk, men innhenting av opplysningene anses som det viktigste

[12] Kan være nyttig for å kategorisere underleverandører, f.eks. vedrørende overføring ut av EØS

Funn knyttet til bruk av samtykker i digitale læremidler

Flere av løsningene kan ikke vurderes tilstrekkelig uten å ha tilgang til avtaleverk mellom leverandører og skoler. Vurdering av løsningenes samtykkehåndtering er derfor basert på personvernerklæringene. For de øvrige løsningene listet under er det opprettet brukerkontoer for å kunne vurdere hva sluttbrukeren må akseptere i prosessen, og når, samt hvor enkelt det er å trekke tilbake samtykker, slette data og slette brukerkonto. For disse løsningene er det gjennomført praktisk test fra sluttbrukerperspektivet, i tillegg til gjennomgang av personvern- og samtykkeerklæring.

Dette dokumentet oppsummerer vurderingene av de ulike læremidlene, hvor resultatet er fordelt i tre ulike kategorier:

> *Godkjent* – her er det stort sett som det skal være, og det er ryddig og god kommunikasjon. Det kan være småting, men generelt høyt nivå.
>
> *Forbedringspotensiale* – Her er det enkelte elementer som ikke er på plass, og det bør meldes til leverandør, slik at de kan utbedre løsningen og oppfylle lovkravene.
>
> *Ikke godkjent* – Her trengs det en større jobb for å kunne godkjenne produktet/ leverandøren. Det anbefales å ikke bruke løsningen før dette er utbedret. Det bør meldes fra til leverandøren slik at de kan utbedre måten samtykker håndteres på.

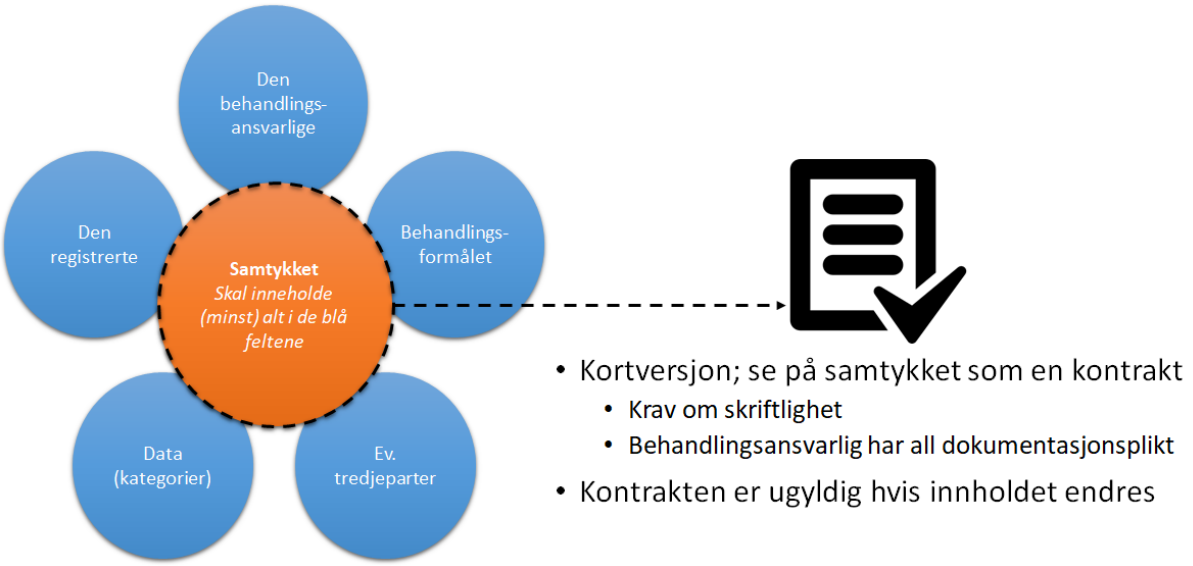
Generelle betraktninger – tiltak som gjelder de aller fleste

Noen løsninger kan ikke vurderes tilstrekkelig uten reelle brukerkontoer fra en skole. Disse løsningene legges i en egen kategori, men med en indikasjon basert på de forhold vi *kan* si noe om utenfra.

Det er viktig å understreke at samtykker i offentlig sektor normalt sett er et saksdokument, i det de både blir til som ledd i en behandlingsprosess og tjener ytterligere som bevis for behandlingsansvarlig. Da følger det også konkrete krav til dokumentasjonen, blant annet arkivplikten[13].

Det betyr at hvis foreldrene til Peder har inngått et samtykke den 1.3.2021 , er det da en "avtale" om at man kan bruke de spesifikke personopplysningene til akkurat det formålet som samtykkeerklæringen tilsier. Hvis foreldrene til Peder trekker tilbake dataene den 30.3.2021 så må man som behandlingsansvarlig forholde seg til den "avtalen", og avstå fra videre behandling av de aktuelle personopplysningene etter tidspunktet for tilbaketrekking.

[13] https://lovdata.no/NL/lov/1992-12-04-126/§2



På lik måte må avtaler endringshåndteres hvis ett eller flere av elementene i avtalen endres. Hvis f.eks. *Leverandør X* deler data med *Leverandør Y*, og så ønsker å dele data med en ny *Leverandør Z*, må endringen aksepteres av alle parter før man kan gjennomføre dette - *Leverandør X* kan ikke uten videre dele dataene med en ny tredjepart.

Det bør gis en utfyllende veiledning til innkjøper/ skole om når det kreves samtykke fra foreldre/ foresatte, slik at nødvendige rutiner og praksis kan etableres før løsningen tas i bruk.

De aller fleste løsningene vi har undersøkt har en lang vei å gå med hensyn til kommunikasjon med elevene. Ihht personvernforordningen skal samtykkeerklæringer og personvernerklæringer være tilpasset mottaker. I praksis betyr dette at budskapet skal være enkelt og kortfattet, uten lange, juridiske utgreiinger, og det skal ikke gjemmes bort i bruksvilkår eller andre lange dokumenter. Hovedmengden av våre funn er preget av vanskelig tilgjengelig informasjon, og/eller unødvendig tungt språk.

Når hovedgruppen av sluttbrukere er skoleelever, må kommunikasjonen tilpasses spesielt til denne målgruppen.

Det er kun unntaksvis at vi har funnet samtykkeerklæringer som egne, separate erklæringer. Samtykkevilkårene synes oftest å være inkludert i personvernerklæringen og er derfor unødvendig vanskelig å forholde seg til for eleven. En slik praksis gjør også at man ikke kan bruke løsningen uten å samtykke til "alt". Det er ikke lagt opp til en differensiering hvor man som elev kan samtykke til noe, men ikke til noe annet, og fremdeles bruke løsningen.

Det er ingen av løsningene som har tilrettelagt for samtykke fra foresatte, men dette er et ansvar som dyttes over på skolen. Det er også ofte litt uklart hvilke behandlingsgrunnlag som legges til grunn; om det er rene samtykkebaserte løsninger, eller om det er opp til skolen å finne behandlingsgrunnlag, samt om løsningen behandler data for å utføre en lovmessig plikt.

Med unntak av punktet over, er det generelt tilfredsstillende informasjon i personvernerklæringene, og der hvor det er tydelige samtykker, er det også enkelt å trekke dem tilbake. Det er også ofte enkelt å slette kontoer og dermed data, med noen unntak.

Kun to av de undersøkte løsningene innhenter nye samtykker når det gjøres endringer i behandlingen eller samtykkeerklæringen. Her kan det være avvik for tilfeller hvor innhentingen gjøres rutinemessig utenfor løsningen, eller gjennomføres på andre måter.

Det er ingen tydelige sammenhenger med de produktene som skårer høyt eller lavt, utover at norske leverandører oftere har informasjon på norsk, som trekker opp, jf. første avsnitt. Selskap fra USA har en tendens til å ha mye informasjon i sine erklæringer. Dette skyldes sannsynligvis at de skal dekke flere lovverk samtidig, og gjør at det ikke er enkelt å forholde seg til som elev. Denne praksisen bidrar til at vurderingsresultatet i vår undersøkelse trekkes noe ned.

Oppsummering om samtykker i læremidlene

Godkjent	
Leverandør A	Leverandør A fremstår stort sett godt mtp personvern. Det som gjenstår er mer tydelighet på hva som er samtykkebasert og hva som har andre behandlingsgrunnlag, samt enklere tilbaketrekking av samtykker.

Forbedringspotensiale	
Leverandør B	Leverandør B må gjøre samtykkene eksplisitte og rydde i personvernerklæringen slik at den er forståelig for elevene.
Leverandør C	Samtykkene er for så vidt godt utformet, men Leverandør C må rydde i personvernerklæringen slik at den er forståelig for elevene. Det må også etableres løsning for å trekke tilbake samtykker. Løsningen baserer seg på andre vilkår ved Education Plan, som ikke er vurdert i dybden i denne fase 1. Løsningen skåres til denne kategorien under forutsetning av at dette stemmer.
Leverandør D	Leverandør D må rydde i personvernerklæringen slik at den er forståelig for eleven. Det må etableres samtykke for deling av data med Google for markedsføringsformål.
Leverandør E	Leverandør E må tydeliggjøre hva som er samtykkebasert behandling og hva som behandles under andre behandlingsgrunnlag.

Ikke godkjent	
Leverandør F	Leverandør F må endre samtykkeknappen slik at det kommer klart frem at det er et samtykke, og det må lenkes til samtykkeerklæringen her. Leverandør F må rydde i

	personvernerklæringen slik at den er forståelig for eleven. Det mangler innhold om formål og bruk av underleverandører. Andre samtykker, som f.eks. e-postkontakt, er tilfredsstillende håndtert.
Leverandør G	Leverandør G må etablere samtykke for opprettelse av foreldrekonto, og må i tillegg rydde i personvernerklæringen slik at den er forståelig for eleven. De må også etablere varsling til eleven ved endringer i behandlingen eller samtykkeerklæringen.
Leverandør H	Leverandør H må etablere lenke mellom samtykkeerklæring og personvernvilkår. I dag lenkes bare bruksvilkår, som ikke inneholder nødvendig informasjon for å danne et gyldig samtykke. Det må også legges inn nødvendig informasjon i personvernerklæringen om hvem som er behandlingsansvarlig samt bruk av underleverandører. De må rydde i personvernerklæringen slik at den er forståelig for eleven. Leverandør H må også etablere mulighet for enkel tilbaketrekking av samtykke for bruk, samt varsling av endringer i personvernerklæring.
Leverandør I	Samtykket må gjøres eksplisitt. Personvernerklæringen må også ryddes i for å gjøre den forståelig. Det må være enklere å trekke samtykket tilbake. Det finnes ingen oversikt over samtykker og hva man har samtykket til når man er logget inn i løsningen.

Ikke tilstrekkelig vurdert	
Leverandør J	Leverandør J må etablere varsling til eleven ved endringer i personvernerklæringen, samt at det mangler noe informasjon i personvernerklæringen. *Forbedringspotensiale*
Leverandør K	Leverandør K må beskrive hvordan de varsler elevene ved endringer. Ellers får Leverandør K pluss for å ha en egen erklæring for barn. *Godkjent*
Leverandør L	Leverandør må lenke til relevant personverninformasjon for denne løsningen, og ikke til den generelle personvernerklæringen for konsernet. Det kan være dette ser annerledes ut fra innsiden, men per nå finnes det ikke nok informasjon til å vurdere løsningen. *Ikke tilstrekkelig vurdert*

Leverandør M	Samtykke brukes i liten grad i løsningen. Sett bort fra dette, synes det meste å være på plass. Samtykkebasert behandling handler i stor grad om markedsføring o.l., og dette formålet håndteres bra i dokumentasjonen. *Godkjent*

Ikke vurdert	
Leverandør N	Leverandør N må tydeliggjøre hvilket behandlingsgrunnlag de har. De beskriver samtykker i personvernerklæringen, men vi finner ingen steder å avgi samtykke; dette må etableres. Erklæringen må også inneholde informasjon som hvem som er behandlingsansvarlig og om formålet med behandlingen. *Ikke vurdert på bakgrunn av mangelfull informasjon*

Oppsummerende vurderinger om personvern for de enkelte læremidlene

Merk at dette er utdrag fra rådata, men det er forsøkt å gi en konkretisering/vurdering i problemstillingene i fase 2.

Leverandør A	Leverandør A fremstår gode mtp personvern; de fleste relevante områder synes å være dekket på en ryddig og god måte, noe som gir økt trygghetsfølelse med hensyn til forventet ansvarlighet hos leverandøren. Dokumentasjonen, avtalene og prosessene var også veldig bra.
Leverandør B	For Leverandør B er det uklarheter knyttet til deling av data, om data (kan) sammenstilles med tredjepartsdata. Det er uklart om personopplysninger krypteres. Vi kan ikke se at det finnes varslingsrutiner til eleven ved eventuelle endringer i personvern- og samtykkeerklæring.
Leverandør C	Leverandør C må rydde i personvernerklæringen slik at den er forståelig for elevene. Det må også etableres løsning for å trekke tilbake samtykker. Løsningen baserer seg på andre vilkår ved Education Plan, som ikke er vurdert i dybden i denne fasen. Data samles inn via, og deles med, tredjeparter. De presenterer imidlertid en ryddig oversikt over databehandlere/tredjeparter. Profilerer brukerne for markedsføringsformål. Det er uklart om personopplysninger krypteres.
Leverandør D	Leverandør D må rydde i personvernerklæringen slik at den er forståelig for eleven. Sammenstiller data fra ulike enheter og datakilder, uten at det er beskrevet i detalj hva som sammenstilles, eller hvordan dette gjøres. Sier eksplisitt at de *ikke* kontrollerer, overvåker eller responderer vedrørende tredjeparters bruk av informasjon som er samlet inn gjennom Leverandør D. Tilbys gjennom USA-basert tjenesteleverandør. Oppdaterer listen over databehandlere/tredjeparter jevnlig, men har ikke tydelige varslingsrutiner til elevene om dette.
Leverandør E	Leverandør E leveres gjennom tjenesteleverandører lokalisert i USA og Spania. Uklarheter i behandlingsgrunnlag(ene); ikke tydelig hvilke grunnlag som brukes når og for hvilke opplysninger. Deler som utgangspunkt ikke data med andre for markedsformål, og genererer heller ikke personprofiler. Kan

	imidlertid overføre brukerinformasjon til tredjepart, uten at dette er beskrevet noe nærmere. Mindre datainnsamling for mindreårige sluttbrukere/elever. Uklart om personopplysninger/data slettes når eleven ber om det, eller om det bare deaktiveres/gjøres utilgjengelig. Eleven varsles i forkant av eventuelle endringer i personvernerklæringen.
Leverandør F	Leverandør F sammenstiller data fra ulike enheter og datakilder, uten at det er beskrevet i detalj hva som sammenstilles, eller hvordan dette gjøres. De lar også tredjepart aksessere elevens informasjon, og tredjepart kan hente ut data for egen sammenstilling. Det er uklart hvilken rettsstilling man har overfor tredjepart hvis man f.eks. ønsker at tredjepart skal slette innhentede data. Databehandlere og tredjeparter er ikke konkretisert, utover at de har mange partnere som de samarbeider med. Alt innhold gjennomgås (automatisert) av Leverandør F, med formål om å overholde sin egen innholdspolicy. Leverandør F må rydde i personvernerklæringen slik at den er forståelig for eleven. Det mangler innhold om formål og bruk av underleverandører. Sletting av brukerkontoen garanterer ikke fjerning av all personlig informasjon fra løsningen. Det er uklart om personopplysninger krypteres. Ikke klart om eleven blir varslet ved endring av personvern- eller samtykkeerklæring.
Leverandør G	Leverandør G må etablere samtykke for opprettelse av foreldrekonto og må i tillegg rydde i personvernerklæringen slik at den er forståelig for eleven. Skiller mellom brukere i tre typer; lærere/administratorer, studenter og foreldre. Tjenesteleveransen er basert i USA/Canada. Leverandør G overfører personopplysninger ut av EU.

	Fremstår som fullintegrert med produktet til en annen leverandør vurdert her Leverandør E, men Leverandør E står ikke i listen over databehandlere/tredjepartsleverandører. Det er ikke klart om eleven varsles ved endringer i behandlingen, eller i personvern- eller samtykkeerklæringen.
Leverandør H	Leverandør H må etablere lenke mellom samtykkeerklæring og personvernvilkår. I dag lenkes bare bruksvilkår, som ikke inneholder nødvendig informasjon for å danne et gyldig samtykke. Det må også legges inn nødvendig informasjon i personvernerklæringen om hvem som er behandlingsansvarlig samt bruk av underleverandører. De må rydde i personvernerklæringen slik at den er forståelig for eleven. Leverandør H må også etablere mulighet for enkel tilbaketrekking av samtykke for bruk, samt varsling av endringer i personvernerklæring.
Leverandør I	Vi mottok ikke databehandleravtale fra Leverandør I på forespørsel, men de var ellers imøtekommende og responsive med tanke på spørsmål rundt personvern. Personvernerklæringen må ryddes i for å gjøre den forståelig for elevene. Det må være enklere å trekke samtykket tilbake og det bør finnes en oversikt over hva man har samtykket til når man er logget inn i løsningen. Uklart om brukergenerert innhold blir behandlet/filtrert før publisering, samt uklart om dialog mellom brukere blir moderert.
Leverandør J	Leverandør J leveres via Amazon Web Services i Irland, og viser for øvrig oversikt over databehandlere i Norge, Romania og USA. Benytter bruksmønster og lokasjon for tilpasning av markedsmateriell. Varsler ikke ved oppdatering av personvernerklæring.
Leverandør K	Leverandør K må beskrive hvordan de varsler elevene ved endringer i personvern- og samtykkeerklæring. Positivt at de har en egen erklæring for barn. Uklart hvor informasjonen lagres (“Denne informasjonen lagrer vi på noen store datamaskiner koblet til internett som kalles

	servere. Disse serverne står i Norge eller i andre land i EU eller i USA").
Leverandør L	Leverandør må lenke til relevant personvernerklæring for denne løsningen, og ikke til den generelle personvernerklæringen for konsernet. Det er vanskelig å skille produktet til konsernet og løsning ut fra tilgjengelig dokumentasjon; i noen tilfeller henvises det til selskapet, i andre til produktet. Per nå har vi ikke tilstrekkelig informasjon til å vurdere leverandøren eller løsningen for dette området.
Leverandør M	Løsningen henviser primært til danske vilkår. Leverandøren skisserer ikke annet enn at man bruker AWS og Superoffice som underbehandler. Kan derfor være mer tydelig på til hvem, hva som overføres og hvilke data. Samt hva som skjer med dataene og når om samtykket trekkes tilbake eller kontrakten avsluttes. Selskapet har lagt ut ekstern vurdering fra Danmark basert på ISAE 3000 - standarden for sikkerhet for ikke-økonomisk informasjon.
Leverandør N	Løsningen tilbyr personlig, lokal lagring for eleven og faller utenfor området for denne undersøkelsen.