Overordnet vurdering av personvern i digitale læremidler i Osloskolen

Versjon 1.0, sist oppdatert 27.01.23

Dette dokumentet er en overordnet beskrivelse av personvern i bruk av digitale læremidler. Dokumentet kan brukes som et grunnlag når det skal gjøres risikovurderinger og personvernkonsekvensvurderinger (DPIA) av digitale læremidler (videre omtalt som tjenester/apper) i Osloskolen.

Innhold

Innledning

Som en del av den kontinuerlige digitaliseringen av Osloskolen og målet om at IKT-løsninger skal fremme effektiv undervisning, er digitale læremidler som applikasjoner (apper), webtjenester og nettbrett eksempler på teknologi som får større plass, og bidrar til mer og bedre læring i skolehverdagen. I Osloskolen er det mange skoler og klasser hvor alle elevene har egen digital enhet (1:1 dekning), og per skolestart 2020 var det ca 40.000 nettbrett. En økning på nesten 10.000 enheter det siste året.

Utdanningsetaten har fått mandat til å vurdere personvern i de ulike appene/tjenestene skolene ønsker å ta i bruk, mens skolene selv har full råderett over hvilke digitale læremidler de ønsker å ta i bruk etter at de er godkjent. Kjøp/nedlastning av lisenser/tjenester/apper blir gjort på den enkelte skole. Det er mange fordeler ved at det er skolene selv som bestemmer hvilke apper de skal bruke, men økt bruk av læringsteknologi stiller også økte krav til å ivareta personvernet og informasjonssikkerheten til brukerne. Det er et stort mangfold av tjenester/apper tilgjengelig, både i omfang og kompleksitet, og skolene har ofte behov for apper som leveres av internasjonale aktører av ulik størrelse. Her er det mulige utfordringer knyttet til blant annet lagringssted, databehandleravtaler, oppfølging av underleverandører, tekniske sikkerhetstiltak og kontinuerlige oppdatering av tjenestene/appene som kan få konsekvenser for personvernet til brukerne. Dette kombinert med skolenes ulike behov, gjør at kompleksiteten og utfordringene knyttet til bruken av digitale læremidler øker, og det er derfor nødvendig å gjøre vurderinger av de ulike tjenestene/appene som brukes i Osloskolen.

For å sikre at denne vurderingen har kvalitet og innhold i henhold til. artikkel 35-7 i personvernforordningen, er benyttes Datatilsynets sjekkliste for vurdering av personvernkonsekvenser (DPIA). Etter innledningen er strukturen som følger:

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.

Osloskolens fremgangsmåte i vurdering av personvern i digitale læremidler

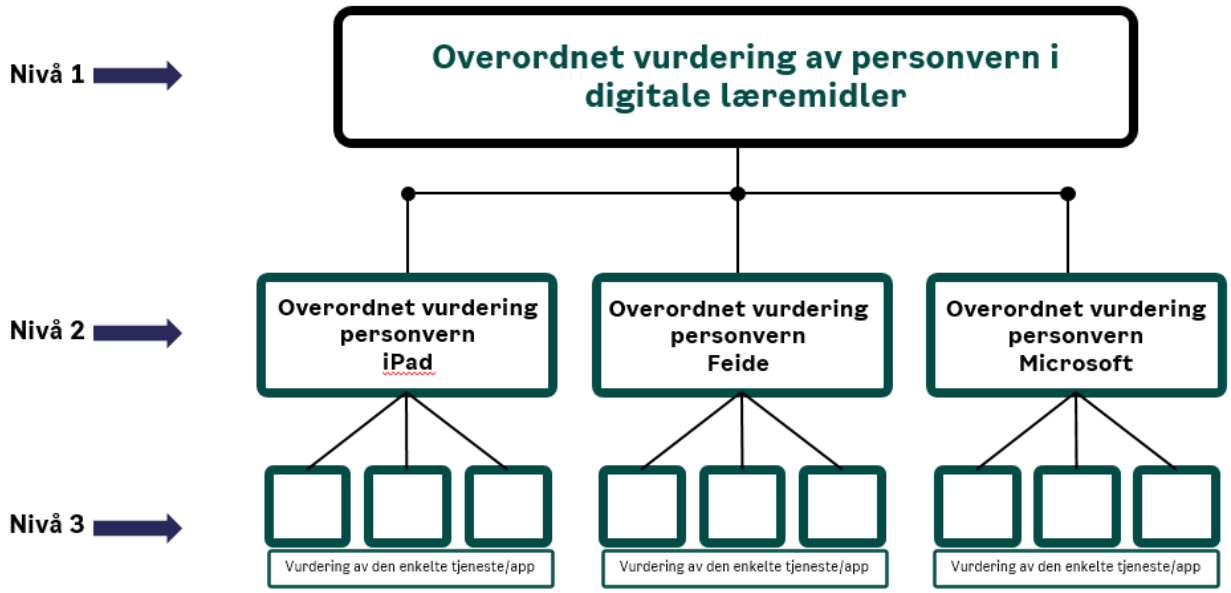
For å få kontroll på og vurdere digitale læremidler som brukes i Osloskolen, deles disse inn i ulike "univers". Dette er hensiktsmessig fordi det er visse likheter for tjenestene/appene i de samme universene, og dermed blir vurderingene mer effektive. .
Universene er:

- Feide-universet, hvor tjenestene er tilgjengelig via Skoleplattformen. Her er det lik måte å autentisere brukerne på.
- Microsoft-universet, hvor tjenestene har en relasjon til Microsoft.
- iPad-universet, hvor appene er tilgjengelige via Apple School Manager, og det kan settes en del retningslinjer for bruken av appene via Lightspeed.
- Andre webtjenester, hvor tjenesten brukes gjennom webplattform. Det er ikke gjort en egen overordnet vurdering av dette universet, da personvernet ivaretas i vurderingene for Feide, iPad og Microsoft, og i vurderinger på tjenestenivå.

Vurderinger av personvern i digitale læremidler gjøres på tre ulike nivåer:

1. **Overordnet vurdering av personvern i digitale læremidler** (dette dokumentet), hvor formålet er å gi et bilde av det som er felles for alle universene knyttet til personvern, samt en beskrivelse av prosessen for vurdering av tjenestene/appene. Denne informasjonen er tilgjengelig i en på Utdanningsetatens nyhetsrom, under denne landingssiden. Hierarkiet for vurderingene vises i figur 1.
2. **Vurdering av personvern for det enkelte univers** (iPad, Feide og Microsoft). Vurderingen i nivå 1 ligger som grunnlag til disse vurderingene. Denne informasjonen finnes på Utdanningsetatens nyhetsrom i side for iPad, Feide, andre webtjenester og Microsoft (under arbeid).
3. **Vurdering av den enkelte tjeneste/app**. Her vurderes personvern i den enkelte tjenesten eller appen, og det gis en begrunnelse for om tjenesten er godkjent/ikke godkjent, med retningslinjer for bruk. Oversikt over vurderte tjenester/apper er publisert på https://aktuelt.osloskolen.no/sok-i-digitale-laremidler-og-verktoy/

Noen tjenester/apper har brukergrensesnitt inn i flere av universene og da må vurderingsprosessene ta høyde for dette, både med tanke på innhenting av relevant informasjon og utarbeidelse av databehandleravtale (DBA) og informasjon til brukerne.



Figur 1: oversikt hierarki i vurderinger av digitale læremidler.

Utfordringer knyttet til bruk av digitale læremidler - lovverket

En del av tjenestene/appene som er tilgjengelige og skolene ønsker å bruke er utviklet av leverandører utenfor EU/EØS, og det er for disse tjenestene/appene personvernutfordringene er størst. Etter personvernforordningen trådte i kraft i 2018 er det kommet flere rettsavgjørelser og veiledning om personopplysninger om europeiske borgere skal behandles, også utenfor EU/EØS. I Schrems II-dommen understreker EU-domstolen at behandlingsansvarlig alltid må undersøke om personopplysningers beskyttelsesnivå i praksis er tilstrekkelig.. Dommene erklærte overføringsgrunnlaget mellom Europa og USA "Privacy Shield" (USA) ugyldig. fordi det var i strid med kravene til et tilstrekkelig beskyttelsesnivå i personvernforordningen. Sentralt i disse vurderingene var amerikansk etterretning sine vide hjemler, og ikke gode nok muligheter for europeiske borgere til å overprøve beslutningene om overvåkning.

EU-kommisjonens standard personvernbestemmelser (SCC) er fremdeles et gyldig overføringsgrunnlag, men dette er ikke alltid tilstrekkelig i seg selv. SCC skal garantere et tilstrekkelig beskyttelsesnivå etter at personopplysningene er overført ut av EU/EØS, men man må vurdere hvorvidt dette beskyttelsesnivået vil opprettholdes i praksis før data overføres. SCC er ikke bindende for tredjelandets myndigheter, og tredjelandets lover kan gå foran SCC. Det er i 2021 kommet ny versjon av EU-kommisjonens SCC, og etter 27.09.21 skal disse brukes for alle nye behandlinger utenfor EU/EØS, mens SCC for eksisterende behandlinger må være oppdatert innen 27.12.2022.

Det er viktig å være oppmerksom på at det er ikke bare USA beskyttelsesnivået i praksis kan bli undergravd av forhold i tredjeland. EU-kommisjonen har besluttet at det er en rekke land som ivaretar personvernet på tilsvarende måte som i EU/EØS, og overføringen vil være sammenlignbar med overføringer mellom land innenfor EU/EØS. Ved overføringer til disse landene er det ikke nødvendig med ytterligere vurderinger.

For at Osloskolen skal kunne benytte tjenester/apper med leverandører utenfor EU/EØS, må det gjøres grundige vurderinger om disse tjenestene/appene vil behandle personopplysninger.

Terskelen for å godkjenne disse tjenestene/appene bør som en følge av det totale risikobildet være høy.

Forutsetninger for leverandører utenfor EU/EØS

På grunn av Schrems II-dommen er det viktig å gjøre vurderinger av leverandørene utenfor EU/EØS som ikke er på EU-kommisjonens liste over områder med tilstrekkelig beskyttelsesnivå. I iPad-universet er mange av leverandørene fra USA.

For å godkjenne apper til bruk i Osloskolen med leverandører utenfor EU/EØS, bør derfor en av følgende forutsetning være på plass:

1. *Leverandør behandler ikke personopplysninger om elever, foresatte eller lærere.*

Begrunnelse for forutsetning: Dersom personopplysninger ikke behandles utsettes ikke brukerne for noen risikoer knyttet til personvern.

2. Leverandøren opererer i et av områdene EU-kommisjonen har besluttet at har tilstrekkelig beskyttelsesnivå, jf. personvernforordningen artikkel 45. |

Begrunnelse for forutsetning: Overføringen er sammenlignbar med overføringer mellom land innenfor EØS, og det er tilstrekkelig med databehandleravtale.

3. Det er tilstrekkelige tiltak/mekanismer på plass for å ivareta personvernet til brukerne, herunder:
    a. Gyldig overføringsgrunnlag, standard personvernbestemmelser (SCC):
        i. Bruk av de gamle SCC gjelder kun for eksisterende behandlinger, og er kun gjeldende frem til desember 2022. I disse tilfellene må man også etablere databehandleravtale med leverandøren, samt vurdere ytterligere tekniske, juridiske og organisatoriske tiltak for å vurdere om beskyttelsesnivået i praksis vil bli overholdt. Alle gamle SCC må være oppdatert innen 27.12.22.
        ii. Bruk av de nye SCC godkjent av EU-kommisjonen juni 2021 gjelder ved nye behandlinger. I disse tilfellene er det ikke nødvendig å inngå databehandleravtale, da dette er dekket av nye SCC. Man må allikevel gjøre ytterligere vurderinger av at beskyttelsesnivået vil bli overholdt i praksis.

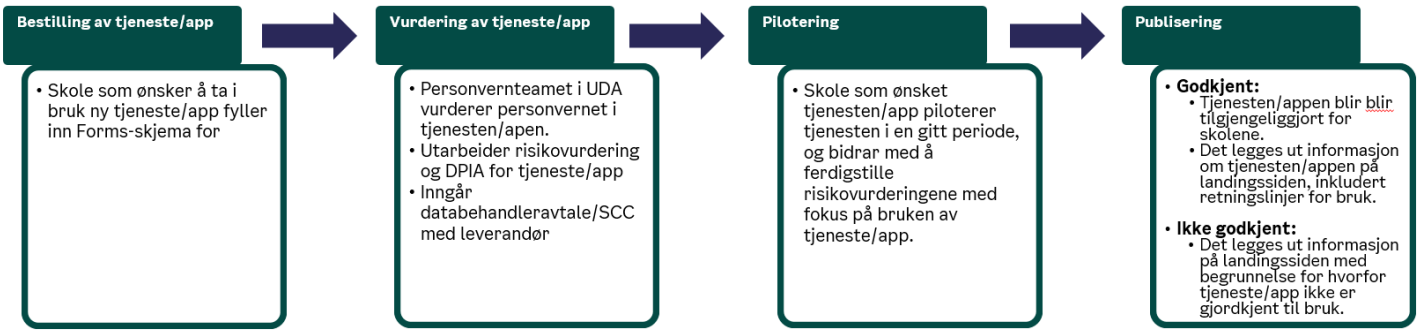
Begrunnelse for forutsetning: Ytterligere tiltak bidrar til å redusere risikoen for de registrerte.

Disse forutsetningene kan endre seg på grunn av utviklingen etter Schrems II-dommen og hvordan de nye SCC fungerer i praksis.

1. En systematisk beskrivelse av behandlingen

Livssyklus

Uavhengig av hvilket univers tjenesten/appen hører til, er prosessen for å gjennomføre personverngodkjenning i hovedsak slik:



Figur 2: prosess for personverngodkjenning

Detaljert beskrivelse av prosessen:

1. **Nytt produkt**: Behov for tjenesten identifiseres ved at en skole melder behovet til skoleleder/IKT-ansvarlig ved skolen, som videre rapporterer behovet til skoleeier.
2. **Kartlegging**: skolen henter informasjon fra/om leverandør om tjeneste/app gjennom et spørreskjema (Feide / iPad / Microsoft). Informasjon om tjeneste/app danner grunnlag for utfylling av foreløpig ROS-analyse, utkast til databehandleravtale/vurdering av personvernbestemmelser (SCC) for overføring til tredjeland (EUs SCC) og vurdering av behov for DPIA.
3. **DPIA**: Skoleeier vurderer behovet for å utføre egen DPIA for produktet, basert på sjekkliste i mal for gjennomføring av DPIA.
4. **DBA / nye standard personvernbestemmelser for overføring til tredjeland (EUs SCC)**: Databehandleravtale mellom leverandøren og skoleeier signeres. Avtalen baseres på Digitaliseringsdirektoratets mal. / For godkjenning av leverandører utenfor EU/EØS vil det være standard personvernbestemmelser (SSC) som vil være overføringsgrunnlaget, enten de nye vedtatt i 2021 eller de gamle med tilleggstiltak.
5. **Pilot**: Skolen(-e) som har meldt behovet for nye tjenester/apper skal pilotere og utforske produktet. Skoleeier avtaler en hensiktsmessig piloteringsperiode i samråd med skolen, typisk 1-3 måneder. Mot slutten av piloteringsperioden skal skolen fylle ut et skjema med informasjon til skoleeier om erfaringer med produktet. Hensikten med piloteringen er å få et kunnskapsgrunnlag til å utarbeide en risiko- og sårbarhetsanalyse med realistiske scenarier og treffsikre tiltak, samt formulere gode og tydelige retningslinjer for bruk av produktet.
6. **Policy for bruk**: I løpet av piloteringsfasen skal skoleeier med innspill fra piloteringsskolen utarbeide retningslinjer for god bruk av tjenesten. I denne prosessen bør det vurderes om det er behov for ytterligere opplæring.
7. **Systemansvar**: Representanter fra pilotskolen inngår i et team som får systemansvar for tjenesten.
8. **ROS**: Den foreløpige risiko- og sårbarhetsanalysen oppdateres med risikoer som er blitt identifisert i løpet av piloteringen og hensiktsmessige tiltak iverksettes. Eventuell restrisiko presenteres for toppledelsen hos skoleeier, eller andre som har fått dette mandatet. Risikobildet blir enten vedtatt og tjenesten godkjent for bruk hos skoleeier, forkastet eller skoleeier ber om en forhåndssamtale med Datatilsynet, jf. personvernforordningen artikkel 36, nr. 5. Dersom et produkt forkastes, og det er hensiktsmessig, skal leverandørens informeres om hva som må endres for at en

godkjenning kan gis, og gis mulighet til å starte prosessen på nytt når dette er innfridd. Dette vil typisk gjelde tjenester/apper utviklet av leverandører innenfor Feide-universet.

9. **Protokoll**: Protokollen oppdateres med informasjon om tilhørende dokumenter, blant annet:
    a. DPIA for tjenesten
    b. ROS for tjenesten
    c. DBA/SCC for tjenesten, som blant annet inneholder informasjon om formål, kategorier av registrerte og personopplysninger, mottakere (f.eks. underleverandører og tredjestater), sletterutiner samt tekniske og organisatoriske sikkerhetstiltak.
    d. Navn og kontaktinfo til medlemmer av systemeiergruppen (minst en representant fra både skoleeier og en skole)
    e. Peker til opplæringsmateriell / retningslinjer for bruk
    f. Peker til informasjon om tjenesten rettet mot elever og foresatte
10. **Bruk**: Tjenestene som er registrert som godkjente gjøres tilgjengelig for bruk av alle skoler. Dette gjøres teknisk ved at skoleeier aktiverer produktet i Feides kundeportal/Apple School Manager/Microsoft 365 Administration Centre.
11. **Oppdatere**: Systemeier består av representanter fra den/de skolen(e) som har pilotert produktet. Disse får et særlig ansvar for å følge med på produktet, gjøre seg kjent med kommende oppdateringer og, i samråd med skoleeier, vurdere om endringene er av en slik karakter at tjenesten må igjennom en ny godkjenningsprosess, eller om det er tilstrekkelig å oppdatere deler av personverndokumentasjonen. Dersom skolen(e) som opprinnelig piloterte produktet slutter å bruke det, beslutter skoleeier (basert på statistikk over bruk av produktet) hvilke(n) skole(r) som skal involveres i systemeiergruppen.
12. **Utfase**: Dersom et produkt fjernes fra markedet, ikke lengre brukes eller ingen skoler er villige til å ta på seg systemeierrollen, merkes tjenesten som "utfaset" i protokollen og tjenesten deaktiveres i Feides kundeportal/Apple School Manager/ Microsoft 365 Administration Centre. Det vil være mulig å reaktivere et utfaset produkt dersom tilsvarende forutsetninger som nevnt i punktene over igjen blir gjeldende.

Behandlingens art og omfang

For å få innsyn i behandlingens art, både hvordan personopplysninger om elever og ansatte blir tilgjengelig i de ulike universene og omfanget av personopplysninger som behandles, se egen vurdering av universene (Feide / iPad / Microsoft).

Skoleeier er **behandlingsansvarlig** for personopplysningene som behandles om lærere og elever i Osloskolen. I en digital hverdag skjer de fleste av disse behandlingene i en digital tjeneste/app utviklet og levert av en ekstern part (utenfor Oslo kommune). Det er da leverandørene av disse som blir **databehandler**, og for at de skal behandle personopplysningene må det være gjort en vurdering av skoleeier om denne behandlingen er lovlig. Det må også være etablert en **databehandleravtale** som regulerer hva databehandleren kan og ikke kan gjøre med personopplysningene. Er det snakk om leverandører utenfor EU/EØS må leverandøren benytte seg av SCC istedenfor databehandleravtale. I Osloskolen brukes en databehandleravtale basert på Digitaliseringsdirektoratets mal, og EU-kommisjonens standard personvernbestemmelser

(SCC). Skoleeier inngår databehandleravtaler og følger opp evt. SCC med leverandører på vegne av alle Osloskolene.

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 tjeneste/app. Jo større del av undervisningen skolen velger å gjennomføre digitalt, 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 skriveøkt 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 vurderingsgrunnlaget. Dette danner de generelle rammene for lagringstid.

Hvilke digitale læremidler som tas i bruk bestemmes av den enkelte skolen, og tilgjengeliggjøres gjennom ulike plattformer (Skoleplattformen, Apple School Manager og Microsoft 365 Administration Centre). Utvalget av verktøy kan være forskjellig for ulike brukergrupper (elever, ansatte og foresatte). De digitale læringsressursene har ulike leverandører (databehandlere), og når elever bruker disse ressursene, legger de igjen aktivitetsdata som behandles av databehandlerne. Aktivitetsdataen kan være informasjon om eleven, hvilke oppgaver elevene har løst og hvordan de har løst dem. 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 og tjenesten/appen. I en del tilfeller er tjenesten/appen gratis, mot at leverandøren får bruke den innsamlede informasjonen til statistikk, videreutvikling av tjeneste/app, rette reklame mot brukeren/selge videre til eksterne i forbindelse med for eksempel reklame. Tjenester/apper som gjør sistnevnte med elevdata vil ikke bli godkjent av skoleeier til bruk i Osloskolen.

Behandlingens formål

Tilpasset opplæring

Formålet med bruk av behandlingen (bruk av digitale læremidler) er å gi elevene opplæring, vurdering og bedre tilpasset opplæring som de har rett på. Dette er et krevende arbeid hvor dagens teknologi kan spille en stor rolle og gi elever muligheter i å få læringsoppgaver som er tilpasset deres arbeidssituasjon. Elever har tilgang til flere ulike digitale læringsressurser, og disse vil i mindre eller større grad samle inn aktivitetsdata om brukerne. Det er viktig å differensiere aktivitetsdataen som Osloskolen tillater at skal behandles. Ulik aktivitetsdata kan ha ulikt formål og behandlingsgrunnlag og ulikt behov for sikring. Det er viktig at Osloskolen er oppmerksom på og regulerer hva slags informasjon som behandles. Aktivitetsdata kan differensieres på følgende måte:

- Informasjon for å gi faglærer, skoleleder og skoleeier et bedre grunnlag for sitt vurderingsarbeid. Dette kan være informasjon om hvilke oppgaver elevene har løst og hvordan de er løst. I noen tilfeller kan denne informasjonen generere nye oppgaver og ressurser som passer for den enkelte elev. Tjenester som automatisk tilpasser på denne måten kalles adaptive produkter. Tilpasningen påvirker ikke eleven i betydelig grad og gir heller ikke rettsvirkninger for vedkommende. Dermed kommer ikke personvernforordningen artikkel 22 til anvendelse her.
- Informasjon en leverandør samler inn for eget formål, for eksempel for å videreutvikle tjenesten ved å bruke informasjonen til statistikk eller forskning. Her må Osloskolen

kontrollere at leverandør spesifiserer i databehandleravtale at informasjonen anonymiseres/pseudonymiseres tilstrekkelig, så den ikke kan kobles tilbake til den enkelte elev.

Aktivitetsdata er en kilde til innsikt i elevenes læringssituasjon i ulike fag, for eksempel ved å finne mønster i elevers interaksjon med verktøy eller deres respons på arbeidsoppgaver. Det er viktig at dette er formålet med behandlingen, og at leverandører ikke tillates å utnytte denne informasjonen.

Eksempler på hva aktivitetsdata kan omfatte:

- Personopplysninger om elev (navn, brukernavn som skoleplattformbruker)
- Hvilken oppgave eleven har jobbet med (eks. <tittel på læreverk>, oppgave nr. 6 i kapittelprøve for kapittel "Tall og algebra").
- Hvilken skole eleven går på, og hvilken kommune skolen ligger i (eks. Abildsø skole i Oslo kommune).
- Navn på leverandøren av læremidlet (eks. Aschehoug)
- Beskrivelse av selve oppgaven (eks. Hvilke er likninger?)
- Hva eleven har svart (eks. 4-3*(2-X) / fritekst).
- Om svaret eleven ga var riktig/galt, hvor mange poeng eleven fikk og hvor mange poeng som var mulig å få (eks. galt svar, 0 poeng av 3 mulige).
- Henvisning til ett eller flere elementer i læreplanen som oppgaven er relatert til
    - **Mål**: F.eks. "Mål for opplæringa er at eleven skal kunne lage, løyse og forklare likningar knytte til praktiske situasjonar")
    - **Verb**: F.eks. "Forklare", "Lage", "Løyse".
    - **Grunnleggende ferdigheter**: "Å kunne regne"
    - **Tverrfaglige tema:** F.eks. Folkehelse og livsmestring
    - **Kjerneelementer:** F.eks. "Modellering og anvendingar"
- Henvisning til ett eller flere områder i et mer detaljert fagkart enn læreplanen (eks. "Algebra", "Likningar" fra rammeverket fagkart.no)
- Angivelse av hvor vanskelig oppgaven er for elever på et gitt alderstrinn.
- For videoer og animasjoner angis hvilke knapper eleven har trykket på (eks. Startet video)
- Hvor lang tid eleven har brukt på oppgaven (eks. 1 min og 3 sek)
- Eventuell bruk av hint (eks. "I alle likninger finner du likhetstegnet (=)")

Aktivitetsdata som samles inn i forbindelse med bruk av tjenester/apper i skolesammenheng skal ikke inneholde private opplysninger av typen adresse/lokasjon, opplysninger om økonomi, bekjentskapskrets, eller liknende. Det skal heller ikke samles inn aktivitetsdata som inneholder særlige kategorier av personopplysninger, som for eksempel opplysninger om helse, etnisitet eller religion, jf. personvernforordningen artikkel 9. Unntak fra dette kan foreligge i de tilfellene en tjeneste/app brukes til å for eksempel teste elever for dysleksi, eller der elever har behov for

digitale hjelpemidler som spesialstøtte. Det er derfor viktig å gjennomføre gode vurderinger av tjenestene/appene som skolene ønsker å ta i bruk, for å sikre at tjenestene/appene ivaretar personvernet, og at Osloskolen har god oversikt over hvilke apper de bør være ekstra oppmerksome på bruken av.

Vurdering
"Formålet med vurdering i fag er å fremje læring og bidra til lærelyst undervegs, og å gi informasjon om kompetanse undervegs og ved avslutninga av opplæringa i faget", jf. forskrift til opplæringslova § 3-3. I lærerens vurderingsarbeid vil analyserte aktivitetsdata, strukturert ved hjelp av elementer i læreplanen og eventuelt områder i et fagkart, gi en verdifull oversikt over elevens arbeid, styrker og utviklingsområder. Aktivitetsdata skal brukes til å avdekke mønstre hos eleven for å kunne gi tilpassede oppgaver og anbefale videre læringsressurser.

Aktivitetsdata til vurdering kan benyttes både i forbindelse med lærers underveis- og sluttvurdering, som et verktøy i skole-hjem-samarbeid, jf. opplæringslova §§ 1-1 og 8-2, og i skolebasert kvalitetsutviklingsarbeid, jf. opplæringslova § 13-3e. Dette er et systematisk arbeid som er pålagt (se utfyllende beskrivelser i avsnittet om rettslig grunnlag). Den enkelte lærer er ansvarlig for å skaffe et bredt og utfyllende vurderingsgrunnlag for sine elever, inkludert hva de mestrer og gi veiledning i hvordan de kan arbeide videre for å øke kompetansen sin.

Aktivitetsdataene vil ikke viderebehandles til nye eller andre formål og har heller ikke et kontrollformål.

Hvilken sammenheng behandlingen utføres i
Konteksten for behandlingen av personopplysninger er skole og undervisning. Representanten for behandlingsansvarlig vil for elevens vedkommende som regel være læreren, som har et mandat for undervisningen og dermed står i et maktforhold til eleven. I praksis betyr det at lærer bestemmer hvilke læremidler eleven skal benytte og hvilke oppgaver eleven skal jobbe med. Eleven selv har imidlertid kontroll på hvordan de ulike oppgavene løses og hvilke aktivitetsdata eleven produserer i det enkelte læremidlet, på samme måte som elevene selv bestemmer hva de vil skrive i ulike kladde- og innføringsbøker. På den måten vil behandlingen oppfattes som forutsigbar for eleven.

Lagringstid
Lagringstiden er definert i databehandleravtalen/SCC mellom skoleeier (behandlingsansvarlig) og den enkelte leverandør (databehandler). Lagringstiden vil være begrunnet ut fra et pedagogisk behov, i hovedsak basert på varigheten av vurderingsperioden som aktivitetsdataene inngår i. For eksempel til eleven er ferdig med skoleåret / grunnskolen.

Konfidensialitet, integritet og tilgjengelighet
På lik linje med analoge læremidler, er det viktig at elevenes rettigheter blir ivaretatt, både når det kommer til konfidensialitet (at informasjon om eleven kun er tilgjengelig for de som har behov for den), integritet (at informasjon om elever og deres aktivitet er korrekte) og tilgjengelighet (at de har tilgang til de digitale læremidlene, eller alternativer, når de har behov for det for å oppfylle læringsmålene). Dette da vurdering av elevarbeid får konsekvenser både for elevens videre valgmuligheter og motivasjon.

Sårbare grupper
Elever i grunnutdanningen er barn i alderen 6 - 19 år, , og forordningen krever en særlig beskyttelse av denne gruppen registrerte. Privatlivet skal i størst mulig grad beskyttes, for eksempel ved at arbeid utført utenfor skolen i minst mulig grad skal logges. Eksempler på dette kan være at nøyaktig tidspunkt for når en oppgave løses ikke bør tilgjengeliggjøres for lærer.

Erfaringer
Personvernbruddene som har blitt sanksjonert av Datatilsynet siden 2018 har i stor grad handlet om behandling av personopplysninger uten behandlingsgrunnlag, utilstrekkelig beskyttelse av personopplysningene, ulovlig overføring av personopplysninger til tredjeland, og manglende oversikt over behandlingene som utføres av behandlingsansvarlig. Det har også vært flere eksempler på brudd innen skolesektoren, for eksempel i forbindelse med bruk av Strava, Skolemelding og Vigilo. Det er tydelig at dette er en viktig sektor å følge opp fra Datatilsynets side.

Erfaringene fra tilsynsvirksomheten til Datatilsynet viser at det er viktig å ha kontroll på hva slags personopplysninger som behandles hvor, hvilke leverandører som brukes, og at det er har gjort gode nok vurderinger av tjenestene/appene som skal brukes i skolen. Videre må det være fokus på bevisstgjøring om personvern blant lærerne. Involvering av lærere (gjennom godkjenning av apper) og elever (i innspill til overordnede vurderinger) inn i arbeidet med personverngodkjenning vil ha en positiv effekt på dette.

Ulike datasett og formål
Hvordan datasett og formål defineres for de ulike tjenestene/appene er beskrevet i vurderingene for de ulike universene.

Kilder, mottakere, informasjonssikkerhet og ansvarsforhold
Alle problemstillinger i dette avsnittet er ivaretatt av databehandleravtalen, som er basert på Digitaliseringsdirektoratets mal. Dette er også områder som skal være ivaretatt i SCC.

Disse områdene vil variere for de ulike universene, og dette er beskrevet i vurderingene for de ulike universene.

2. Nødvendighet og proporsjonalitet

Personvernprinsippene
Personvernforordningens grunnleggende prinsipper krever at personopplysninger skal behandles på en lovlig, rettferdig og åpen måte, jf. personvernforordningen art. 5 nr. 1. Dette betyr at det må finnes et rettslig grunnlag for at behandlingen skal være lovlig, behandlingen skal respektere de registrertes interesser, og den skal være oversiktlig og forutsigbar.

Dette kan deles inn i mer detaljerte prinsipper, og nedenfor står det hvordan dette gjøres i Osloskolen.

Formålsbegrensning (Rettslig grunnlag)

Personopplysninger skal kun behandles for spesifikke, uttrykkelige angitte og legitime formål, og for at behandlingen av personopplysninger skal være lovlig må det foreligge et behandlingsgrunnlag, jf. artikkel 6 i personvernforordningen. I utdanningssektoren er det særlig følgende rettslige grunnlag i art. 6 som er aktuelle:

- behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige (nr. 1, bokstav c)
- behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt (nr. 1, bokstav e)

Det er en forutsetning at dette er fastsatt i nasjonal rett som et supplerende rettsgrunnlag. For digitale læringsmidler er dette lov om grunnskolen og den videregående opplæringa (opplæringslova) (Kunnskapsdepartementet, 1998), forskrift om utfylling av dei overordna måla og prinsippa for opplæringa i grunnskolen og i den vidaregåande opplæringa (Kunnskapsdepartementet, 2017) og forskrift til opplæringslova (Kunnskapsdepartementet, 2006).

Personvernforordningen artikkel 6 nr. 1 bokstav c vil være behandlingsgrunnlag for behandlingen som skjer i de aller fleste digitale læremidler og verktøy der formålet er opplæring og/eller vurdering/tilpassing relatert til kompetansemål i læreplanen. Art. 6 nr. 1 bokstav e er aktuell tilfeller der det supplerende rettsgrunnlaget for behandlingen ikke er like eksplisitt. Et eksempel på dette kan være forbedring/videreutvikling av produkter eller algoritmer for vurdering/tilpassing. I slike tilfeller har eleven/foresatte rett til å protestere, jf. personvernforordningen artikkel 21 nr. 1.

Det vises videre til drøftningene i høringsnotatet fra Kunnskapsdepartementet til forslag om endringer i opplæringslova, avsnitt 2.1.3 (Rettslig grunnlag for behandling av personopplysninger).

Her trekkes noen av de viktigste hjemlene (*kursivert skrift*) fram med kommentarer for å vise at personopplysninger som håndteres i digitale læremidler er basert på lovlighet, rettferdighet og åpenhet.

Fra opplæringslova - spesifikt for grunnskolen

§ 2-1.Rett og plikt til grunnskoleopplæring

Barn og unge har plikt til grunnskoleopplæring, og rett til ein offentleg grunnskoleopplæring i samsvar med denne lova og tilhøyrande forskrifter. Plikten kan ivaretakast gjennom offentleg grunnskoleopplæring eller gjennom anna, tilsvarande opplæring.
Her slås det fast at alle barn har plikt til opplæring og at den offentlige skolen er en av flere muligheter til å oppfylle denne plikten.

§ 13-1.Plikt for kommunen til å sørgje for grunnskoleopplæring

Kommunen skal oppfylle retten til grunnskoleopplæring etter denne lova for alle som er busette i kommunen.

Her slås det fast at det er kommunen som har plikt til å oppfylle denne rettigheten til elever i grunnutdanningen.

§ 2-3. Innhald og vurdering i grunnskoleopplæringa
Departementet gir forskrifter om fag, om mål for opplæringa, om omfanget av opplæringa i faga og om gjennomføringa av opplæringa (...).
Departementet gir forskrifter om vurdering av elevar (...).

Elevane skal vere aktivt med i opplæringa. Undervisningspersonalet skal tilretteleggje og gjennomføre opplæringa i samsvar med læreplanar gitt etter lova her.

Her slås det fast at mål og innhold i skolen være det som departementet har fastsatt i forskriften, som vi også kaller læreplanen (jf. forskriften § 1.1). Forskriften setter også rammene for vurderingsarbeidet. Til slutt slås det fast at elevene har en plikt til å delta i den undervisningen som undervisningspersonalet legger til rette for i tråd med forskriften.

Fra opplæringslova - spesifikt for videregående

§ 3-1.Rett til vidaregåande opplæring for ungdom
Elevar, lærlingar, praksisbrevkandidatar og lærekandidatar har rett til opplæring i samsvar med denne lova og tilhøyrande forskrifter.
Her slås det fast at ungdommer har rett til opplæring.

§ 13-3.Plikt for fylkeskommunen til å sørgje for vidaregåande opplæring
Fylkeskommunen skal oppfylle retten til vidaregåande opplæring etter denne lova for alle som er busette i fylkeskommunen.
Her slås det fast at det er fylkeskommunen som har plikt til å oppfylle denne rettigheten til elever i grunnutdanningen.

§ 3-4.Innhald og vurdering i den vidaregåande opplæringa
Departementet gir forskrifter om trinn og programområde, om fag, om mål for opplæringa, om omfanget av opplæringa i faga og om gjennomføringa av opplæringa. Departementet gir forskrifter om opplæring i fellesfag og programfag for praksisbrevkandidatar.
Departementet gir forskrifter om vurdering av elevar, lærlingar, praksisbrevkandidatar, lærekandidatar, privatistar og praksiskandidatar (...)

Elevane, lærlingane, praksisbrevkandidatane og lærekandidatane skal vere aktivt med i opplæringa. Undervisningspersonalet skal tilretteleggje og gjennomføre opplæringa i samsvar med læreplanar gitt etter lova her.

Her slås det fast at mål og innhold i skolen være det som departementet har fastsatt i forskriften, som vi også kaller læreplanen (jf. forskriften § 1.3). Forskriften setter også rammene for vurderingsarbeidet. Til slutt slås det fast at elevene har en plikt til å delta i den undervisningen som undervisningspersonalet legger til rette for i tråd med forskriften.

Fra opplæringslova - generelt

§ 1-3.Tilpassa opplæring
Opplæringa skal tilpassast evnene og føresetnadene hjå den enkelte eleven, lærlingen, praksisbrevkandidaten og lærekandidaten.
Her slås det fast at opplæringen skal være tilpasset evnene og forutsetningene til den lærende. Kunnskapsgrunnlaget for denne tilpasningen er i hovedsak resultatene av skolens systematiske vurderingsarbeid.

§ 13-3e. Plikt for kommunen og fylkeskommunen til å arbeide med kvalitetsutvikling
Kommunen og fylkeskommunen skal sørgje for at skolane jamleg vurderer i kva grad organiseringa, tilrettelegginga og gjennomføringa av opplæringa medverkar til å nå dei måla som er fastsette i Læreplanverket for Kunnskapsløftet. Elevane skal involverast i denne vurderinga.
Her slås det fast at skolen jevnlig skal vurdere om opplæringen bidrar til å nå målene i læreplanen og at skoleeieren har ansvar for dette.

§ 15-10. Behandling av personopplysningar
Kommunar, fylkeskommunar og lærebedrifter kan behandle personopplysningar, inkludert personopplysningar som nemnde i personvernforordninga artikkel 9 og 10, når det er nødvendig for å utføre oppgåver etter lova.
Her slås det fast at skolen kan behandle personopplysninger når det er nødvendig for å utføre oppgaver som loven krever.

Fra forskrift til opplæringslova - generelt

§ 3-1.Rett til vurdering
Elevar i offentleg grunnskoleopplæring og elevar, lærlingar, praksisbrevkandidatar og lærekandidatar i offentleg vidaregåande opplæring har rett til vurdering etter reglane i dette kapitlet. Retten til vurdering inneber både ein rett til undervegsvurdering og sluttvurdering og ein rett til dokumentasjon av opplæringa.
Skoleeigar har ansvaret for at eleven, lærlingen, praksisbrevkandidaten eller lærekandidaten sin rett til vurdering blir oppfylt (...)

Her slås det fast at de lærende har rett til både underveisvurdering, sluttvurdering og dokumentasjon og at det er skoleeier (kommune/fylke) som har ansvaret for dette.

§ 3-2.Formålet med vurdering
Formålet med vurdering i fag er å fremje læring undervegs og uttrykkje kompetansen til eleven, lærlingen, praksisbrevkandidaten og lærekandidaten undervegs og ved avslutninga av opplæringa i faget. Vurderinga skal gi god tilbakemelding og rettleiing til elevane, lærlingane, praksisbrevkandidatane og lærekandidatane.
Her slås det fast at formålet både er å fremme læring og å uttrykke kompetansen underveis og ved avslutningen av faget.

§ 3-3.Grunnlaget for vurdering i fag
Grunnlaget for vurdering i fag er kompetansemåla i læreplanane for fag slik dei er fastsette i læreplanverket (...)

Eleven, lærlingen, praksisbrevkandidaten og lærekandidaten skal møte fram og delta aktivt i opplæringa slik at læraren og instruktøren får grunnlag til å vurdere eleven, lærlingen, praksisbrevkandidaten og lærekandidaten sin kompetanse i faget.

Her slås det fast at grunnlaget for vurderingen er den deltakelsen/aktiviteten elevene har vist sett i lys av målene i læreplanen.

§ 3-11.Undervegsvurdering

Undervegsvurdering i fag skal brukast som ein reiskap i læreprosessen, som grunnlag for tilpassa opplæring og bidra til at eleven, lærlingen, praksisbrevkandidaten og lærekandidaten aukar kompetansen sin i fag. Undervegsvurderinga i fag, i orden og i åtferd skal givast løpande og systematisk og kan vere både munnleg og skriftleg.

Undervegsvurderinga skal innehalde informasjon om kompetansen til eleven, lærlingen, praksisbrevkandidaten og lærekandidaten og gi rettleiing om korleis ho eller han kan utvikle kompetansen sin i faget.

Her slås det fast at underveisvurderingen skal gis løpende og systematisk, og brukes som grunnlag for tilpasset opplæring for å gi økt kompetanse. Videre skal underveisvurderingen inneholde informasjon om oppnådd kompetanse og veiledning om hvordan kompetansen kan videreutvikles.

§ 3-16.Samanhengen mellom undervegsvurderinga og standpunktkarakteren i fag
Undervegsvurderinga skal fremje læring og gi eleven høve til å forbetre kompetansen sin gjennom opplæringstida i faget. Den kompetansen eleven har vist undervegs i opplæringa er ein del av grunnlaget for vurderinga når standpunktkarakteren i fag skal fastsetjast.
Her slås det fast at underveisvurderingen også skal være en del av grunnlaget for fastsetting av standpunktkarakter.

§ 22A-2. Krav til tilgangsstyring
Kommunar og fylkeskommunar skal sørgje for tilgangsstyring slik at dei som arbeider for verksemda, berre har tilgang til personopplysningar dersom og i den utstrekning dei treng opplysningane for formål som nemnde i opplæringslova § 15-10. Kommunar og fylkeskommunar skal sørgje for at den som arbeider for verksemda, har nødvendig kunnskap om personvern og informasjonstryggleik før vedkommande får tilgang til personopplysningar.
Krava i første ledd gjeld personopplysningar som er omfatta av personopplysningsloven, og som blir behandla med heimel i opplæringslova.

Her slås det fast at ansatte som har tilgang til personinformasjon, skal ha tilstrekkelig kunnskap om personvern og informasjonssikkerhet og at personinformasjon skal tilgangsstyres til dem som har tjenstlig behov.

Forskriftens krav om bruk av digitale verktøy

Overordnet del

Overordnet del av læreplanen er hjemlet i Forskrift om utfylling av dei overordna måla og prinsippa for opplæringa i grunnskolen og i den vidaregåande opplæringa. Denne slår fast og utdyper flere av prinsippene som allerede er diskutert i dette dokumentet, blant annet vurdering av elevenes faglige kompetanse og tilpasset opplæring for den enkelte elev.

Læreplaner
Det er omtrent 5000 læreplaner i Utdanningsdirektoratets oversikt over fagplaner for grunnutdanningen (grunnskole + videregående opplæring). Oversikten omfatter både utgåtte, gjeldende og kommende planer. Ordet "digital" er nevnt over 700 ganger i kompetansemålene for de gamle læreplanene og det digitale fokuset er enda høyre i nye læreplaner, som blant annet har innført programmering som nytt konsept i flere fag. Ofte er dette formuleringer av typen *Eleven skal kunne <gjøre noe fagspesifikt> ved bruk av digitale verktøy*.

Digitale ferdigheter er også definert som en av fem grunnleggende ferdigheter i læreplanen/forskriften. Hvert fag har en egen tekst om hver av de grunnleggende ferdighetene som beskriver hva hver av de fem grunnleggende ferdighetene innebærer i faget, og hvordan ferdighetene utvikles. I kompetansemålene er de grunnleggende ferdighetene integrert som en del av den kompetansen eleven skal utvikle i det aktuelle faget. Utdanningsdirektoratet har utarbeidet egne rammeverk for hver av de grunnleggende ferdighetene, inkludert digitale ferdigheter.

Sentrale føringer
Det er også gitt en rekke sentrale føringer som utfyller det supplerende rettsgrunnlaget. Nasjonale myndigheter støtter og legger til rette for digitalisering i utdanningssektoren, blant annet ved selv å eie og forvalte Feide som den viktigste fellestjenesten for sektoren. Vi vil også trekke fram noen andre sentrale føringer.
Kunnskapsdepartementets Digitaliseringsstrategi for grunnopplæringen 2017–2021 (utvidet periode til 2022) *Framtid, fornyelse og digitalisering*, nevner blant annet at

digitale læringsressurser utvider mulighetene for ulike metoder og innfallsvinkler, og for tilpasning av undervisningen både for høyt presterende elever, elever som strever i fag eller elever med særskilte opplæringsbehov. (s. 19).

videre står det at

Når skolen skal velge digitale læremidler er det derfor behov for også å vurdere hvordan læremiddelet utnytter det digitale mediets muligheter på ulike måter. Nye teknologier og bruk av store datamengder åpner for nye muligheter for adaptive læremidler og læringsanalyse, men krever også økt oppmerksomhet om kvalitet, etikk, personvern og informasjonssikkerhet. For lærere vil det være særlig utfordrende å vurdere hvilke forhåndsdefinerte valg som gjøres i et adaptivt læremiddel, for eksempel hva som måles, hvilket elev- og læringssyn som legges til grunn og hva slags oppgaver og lærestoff som blir tilgjengelig for hvilke elever. (s. 19)

Handlingsplanen innenfor denne digitaliseringsstrategien er i hovedsak viet til arbeid med digitale læringsressurser med ekstra fokus på personvern og informasjonssikkerhetsarbeidet.

Som hjelp til å finne gode digitale læremidler har Utdanningsdirektoratet utviklet kvalitetskriterier for læremidler.

Dette er et eksempel fra disse kvalitetskriteriene som indikerer at det er ønskelig at digitale læremidler lagrer elevenes aktivitetsdata og tilgjengeliggjør disse for læreren umiddelbart:

Kilde: *kvalitetskriterier for læremidler i matematikk (for lærere)*

Dataminimering

Dataminimering ivaretas ved at hver enkelt tjeneste/app, uavhengig av univers, skal gjennomgå en egen godkjenningsprosess (se avsnittet "Livssyklus"). I denne prosessen skal det angis hva formålet med behandlingen er, samt hvilke aktivitetsdata som lagres. Godkjenningsprosessen vil sikre at det kun åpnes for data som er nødvendig for formålet som er definert.

Riktighet

Se avsnittet *Integritet* under *Hvilken sammenheng behandlingen utføres i ("kontekst")*.

Lagringsbegrensning

Lagringsbegrensning avtales i databehandleravtalen/SCC mellom skoleeier og leverandør. Fagets varighet er utgangspunktet for vurdering av hvor lenge aktivitetsdata kan lagres hos leverandøren.

De registrertes rettigheter

De registrerte har rett til rettferdig og gjennomsiktig behandling, jf. personvernforordningen artikkel 12, 13 og 14. Bruken av digitale læremidler i Osloskolen legger ikke opp til behandlingsgrunnlag basert på samtykke, se avsnittet *Rettslig grunnlag* under *Personvernprinsippene*. Retten til innsyn ivaretas av innsynsfunksjonaliteten i Feide-universet, og i de andre universene ved å sikre at leverandør tilrettelegger for at brukere kan få innsyn i egne personopplysninger via en innsynsfunksjonalitet.

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.

Det skal ikke brukes tjenester/apper som inneholder automatiserte avgjørelser.

Integritet, konfidensialitet og ansvarlighet
Se avsnittet *Integritet* under *Hvilken sammenheng behandlingen utføres i (kontekst)*.

Det at det er gjort en overordnet vurdering av personvern i digitale læremidler, for hvert av de enkelte universene og for hver av de enkelte tjenestene/appene er tiltak som er med på å sikre personopplysningene til elever og lærere.

De registrertes friheter
Universene representerer ingen begrensninger i relasjon til Den europeiske menneskerettskonvensjonen.

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

Medbestemmelse, åpenhet, forutsigbarhet
Dette avsnittet gjør en overordnet vurdering av risikoer for den registrertes rettigheter og friheter, samt overordnede tiltak innenfor tre områder:

1. Manglende reell medbestemmelse
2. Manglende reell åpenhet
3. Manglende forutsigbarhet ved behandlingen

Spesifikke aspekter ved disse risikoene er beskrevet i vurderingene av universet.

Risiko: Manglende reell medbestemmelse
Elever har en rettigheter knyttet til medbestemmelse over egen opplæring. Dette er lovfestet i ulike deler av opplæringsloven med forskrift, for eksempel at skolen er forpliktet til å etablere skolemiljøutvalg, elevråd og foreldreråd med arbeidsutvalg (FAU), se blant annet opplæringsloven § 9 A-9 og opplæringsloven kapittel 11. Dette er også nevnt i læreplanens overordnede del under avsnittet Sosial utvikling og læring. Dette er overordnede rettigheter som også omfatter den digitale arenaen som elever og deres foresatte forholder seg til gjennom skolen. organene representerer forum der elever og foresatte kan ta opp saker de er opptatt av og dermed sikre å få reell innflytelse. Konsekvensen av manglende medbestemmelse kan være frustrasjon, mistrivsel og mangel på motivasjon for skolearbeidet. Her er det viktig å være oppmerksom på at det er forskjell på medbestemmelse over egen opplæring og medbestemmelse når det gjelder selve behandlingen av personopplysninger, ref. avsnitt formålsbegrensning (rettslig grunnlag).

Aktuelle tiltak for å sikre elevenes reelle medbestemmelse er at skolene gir god informasjon om personopplysninger i de digitale løsningene som brukes i skolen og hva dette betyr for elevenes rettigheter. Dette kan for eksempel settes på dagsorden i foraene som er nevnt over.

Risiko: Manglende reell åpenhet
Omfanget av digitale løsninger i skolen er stort og økende. Det kan være krevende for eleven å forstå hvilke løsninger som inneholder personopplysninger og hvilke som ikke gjør det.

Konsekvensen av dette kan være at eleven legger igjen digitale spor uten å være klar over det, og at eleven ville ha agert annerledes dersom eleven var klar over situasjonen.

Tiltak kan være å tydeliggjøre hvordan de enkelte digitale løsninger som elevene bruker registrerer og behandler personopplysninger. Personvern er satt opp som eget tema i samfunnsfag i den nye læreplanen. Eksempler på dette er

- **Grunnleggende ferdigheter:** *Digitale ferdigheter i samfunnsfag (...) vil videre seie å kunne kommunisere og samarbeide digitalt om samfunnsfaglege tema, og å følgje reglar og normer for nettbasert kommunikasjon, medrekna personvern og opphavsrett.*
- **Kompetansemål etter 4. trinn**: *Mål for opplæringen er at eleven skal kunne bruke grunnleggjande nettvett i digital samhandling og ha kunnskap om reglar for personvern i digitale medium*
- **Kompetansemål etter 7. trinn**: *Mål for opplæringen er at eleven skal kunne bruke digitale verktøy til å presentere samfunnsfagleg arbeid og følgje reglar for personvern og opphavsrett*

Risiko: Manglende forutsigbarhet ved behandlingen

Hva slags informasjon behandles? Hvem som har tilgang til hva kan være utfordrende for elever å få oversikt over. Er det flere enn faglæreren min som ser den oppgaven jeg nettopp har levert? Ser mine foreldre bare lærers vurdering, eller hele oppgaven min? Forstår lærer alltid hvilke andre personer som har innsyn i vurderinger som skrives digitalt om elevene?

Dette er spørsmål som elevene har krav på å få gode svar på.

- *Digitale læremidler utviklet til utdanningssektoren* har den fordelen at de er skreddersydd til dette spesifikke formålet og at de er utviklet av pedagoger som har god forståelse for skoledomenet. De fleste løsningene har dermed høyt fokus på å bygge personvern inn i løsningene. I en del tjenester/apper vil det være mulig å etablere god og forutsigbar tilgangsstyring til personopplysninger basert på roller.
- *Tjenester/apper som ikke er utviklet spesifikt til utdanningssektoren* kan være utfordrende å kunne sikre forutsigbarhet ved behandlingen. Det har vært et økt fokus på innebygd personvern etter innføringen av den nye personopplysningsloven, men dette vil være noe varierende. Det er derfor viktig å ha gode rutiner og prosesser for å tilrettelegge for forutsigbarhet. Dette ved å dokumentere hva slags personopplysninger som behandles, og ikke godkjenne tjenester/apper hvor det ikke er mulig å sikre forutsigbarhet.

4. Ledelsens validering av overordnet vurdering av personvern i digitale læremidler

Sammenstilling og presentasjon av funn

Med digitale læremidler kommer det mange muligheter for å tilrettelegge for god og motiverende undervisning for elevene. Sammen med dette kommer det også noen utfordringer knyttet til personvern som det må tas stilling til. Ved å etablere gode prosesser for personverngodkjenning av tjenester/apper, vil det være enklere for lærere å bruke digitale hjelpemidler som ivaretar personvernet til elevene. Det er viktig at lærere inkluderes i dette

arbeidet for å sikre at kun de tjenestene/appene skolene faktisk ønsker å ta i bruk vurderes, og for å øke bevissthet og kompetanse på personvernområdet.
Enkelte av universene har høyere tillitt enn andre, basert på hvor de er lokalisert, hvilke områder de jobber mot og hvem som er involvert i utvikling/forvaltning av tjenestene. Her er det viktig å huske at ingen digitale løsninger kommer uten risiko, og det er viktig å gjøre tilstrekkelige vurderinger av de tjenestene/appene man ønsker å ta i bruk.

Osloskolen bør fortsette å prioritere de strategiske nasjonale initiativene innen skolesektoren, både for å bidra med egen erfaring og kompetanse, dra nytte av andres og være med å sette standarden for hvordan man skal jobbe med personvern i skolesektoren.

Ved å gjennomføre vurderingsprosessene etablert i Osloskolen kan det gjøres vurderinger for å legge til rette for å kunne bruke tjenester/apper på en god måte, og at det kun er godkjente tjenester/apper som blir tatt i bruk av skolene.

Synspunkter fra personvernombud (artikkel 35 nr. 2)
Overordnet vurdering av personvern i digitale læremidler ble presentert for personvernombudet i Oslo kommune november 2021, sammen med overordnet vurdering for universene Feide og iPad.

Personvernombudet har gitt følgende kommentar:

Viser til de tre personvernkonsekvensvurderingene Utdanningsetaten har utarbeidet («Overordnet vurdering av personvern i digitale læremidler», «Vurdering av personvern i Feide-universet», «Vurdering av personvern i iPad-universet»). Dokumentene er versjon 0.8 versjon på gjennomgått tidspunkt. Ombudet har vært involvert underveis i prosessen og er positiv til det velfungerende, løpende samarbeidet. Ombudet deler tilnærmingen til dette omfattende komplekset, hvor etaten har valgt å lage tre ulike nivåer, hvor disse tre vurderingene utgjør de to øverste nivåene (sammen med; «Vurdering av personvern i Windows-universet» når denne er ferdig), mens et tredje nivå vil omfatte «mini-DPIA-er for de enkelte tjenestene, risiko- og sårbarhetsvurderinger og informasjon til de registrerte. Både ombudet og det sentrale fagmiljøet for personvern i Oslo kommune har vært involvert i arbeidet og fått rikelig med muligheter til å komme med innspill. Ombudet har derfor ingen substansielle innvendinger mot de utkastene som foreligger og de innspillene, tilbakemeldingene, kommentarene og forslagene som har kommet opp har blitt vurdert om implementert i vurderingene. Ombudet har lagt vekt på tydelighet, oversiktlighet, klart språk og en faglig tilnærming som i størst mulig grad avspeiler kommunens øvrige malverk eller (som her) Datatilsynets sjekklister for personvernkonsekvensvurderinger (DPIA). I den avsluttende fasen av dette arbeidet håper ombudet at det blir rom for å ytterligere involvering av relevante brukergrupper som foreldreutvalget for grunnskolen (FUG) og Elevorganisasjonen (EO).

Informasjon fra Personverngruppen i UDA:
Tilbakemeldingene fra personvernombud har stort sett gått på ønske om ytterligere tydeliggjøring av prosesser, samt justering i struktur for å gjøre det mer forståelig. Disse endringene ble implementert i 0.9 versjonen som ble sendt på høring til Elevorganisasjonen (EO), Foreldreutvalget for grunnopplæringen (FUG) og Utdanningsforbundet.

Synspunkter fra de registrerte eller deres representanter (artikkel 35 nr. 9).
Overordnet vurdering av personvern i digitale læremidler ble oversendt til Foreldreutvalget for grunnopplæringen (FUG), Elevorganisasjonen (EO) og lærere. Grunnutdanningen omfatter elever i aldersspennet 5,5 år til et stykke opp i myndighetsalder. Det er derfor viktig å inkludere interesseorganisasjonen som representerer foreldrene for å ivareta interessen til de minste elevene, mens Elevorganisasjonen er den viktigste stemmen for elever i ungdomsskolealder og på videregående nivå. Disse organisasjonene representerer de registrerte i denne sammenhengen og deres innspill er tatt med i dette avsnittet.

Vurderingene som er gjennomført på overordnet nivå for digitale læremidler, iPad, Feide og Microsoft ble sendt ut på høring, med invitasjon til å gi skriftlig tilbakemelding. Videre ble det invitert til et fysisk høringsmøte (04.05.22), hvor også personvernombud i Oslo kommune var til stede. I møtet gikk UDE gjennom innspillene som hadde blitt sendt inn i forkant, samt åpnet for diskusjon rundt dette og videre arbeid. Representanten fra FUG kunne ikke delta pga sykdom, og det ble gjennomført et tilsvarende møte med vedkommende i etterkant (09.05.22).

Oppsummering av innspillene fra de registrertes representanter er;

Elevens medbestemmelsesrett

Innspill oppsummert:
- Ønskelig at elevene velger selv hva slags informasjon de skal dele, og ha mer innsyn i dette.

Svar:
- Det skal ikke samles inn mer informasjon enn hva som er nødvendig ifm undervisning. Dette er informasjon elevene ikke kan motsette seg.
- I vurderingsprosessen av digitale læremidler utarbeides det informasjon om tjenestene, som skal ligge tilgjengelig for elever, foresatte og lærere. Dette inkluderer hva slags informasjon som lagres.

Systematisk overvåkning

Innspill oppsummert:
- Digitale verktøy gjør det mulig for lærere å følge elevens faglige progresjon tett og se (overvåke) hva elevene holder på med i verktøyet til enhver tid er problematisk.

Svar:
- Høy bevissthet rundt dette internt i Osloskolen, ikke ønskelig å drive systematisk overvåkning.
- Risikoelement som avdekker om dette er mulig i tjenesten – i så fall veier dette tungt i vurderingene (tiltak og godkjenning/ikke godkjenning).
- IKT gjør tekniske tiltak hvor mulig, for eksempel skru av funksjonalitet for overvåkning.

Kontroll over digitale læremidler og personopplysninger

Innspill oppsummert:
- Har man oversikt over hvilke digitale læremidler som brukes, og hva slags personopplysninger som tilgjengeliggjøres via disse?

Svar:
- Oversikt over alle digitale læremidler som brukes i Osloskolen.
- Kontinuerlige vurderinger av tjenester.
- Risikoelementer som ivaretas i prosess:
  - At det ikke behandles mer informasjon enn nødvendig.
  - At uautoriserte ikke har tilgang til informasjonen.

Disse innspillene er inkludert og ivaretatt i vurderingene som er gjort på overordnet nivå, i tillegg til at det er inkludert i vurderingene som gjøres av hver enkelt tjeneste.

Kontroll over digitale læremidler og personopplysninger

Innspill oppsummert:

1. Har man oversikt over hvilke digitale læremidler som brukes, og hva slags personopplysninger som tilgjengeliggjøres via disse?

Svar:

1. Oversikt over alle digitale læremidler som brukes i Osloskolen.
2. Kontinuerlige vurderinger av tjenester.
3. Risikoelementer som ivaretas i prosess:
    a. At det ikke behandles mer informasjon enn nødvendig

Ledelsens gjennomgang, beslutning og godkjenning

Denne overordnede vurderingen av personvern i digitale læremidler, inkludert rutine for personverngodkjenning, blir lagt til godkjent på ledernivå i Utdanningsadministrasjonen etter at innspillene fra Personvernombudet, FUG og EO er implementert.

Versjonshistorikk

Versjon	**Dato**	**Forfatter**
0.8 utkast sendt til personvernombud for innspill	November 2021	Brian Jørgensen og Kaja Felix Sønslien (innleid konsulent)
0.9 etter innspill fra personvernombud, sendes på høring til de registrerte	19.01.2022	Brian Jørgensen (UDE) og Kaja Felix Sønslien (innleid konsulent)
0.91 klargjøring for språkvask	08.09.2022	Brian Jørgensen (UDE), Heli Kristiina Kananen og Kaja Felix Sønslien (innleide konsulenter)
1.0 Til ledergodkjenning	27.01.2023	Brian Jørgensen (UDE) og Cathrine Lund (innleid konsulent)