UNIVERSITETET
I OSLO

Læringsanalyse og kvalitet i utdanningene ved UiO:

Forslag til personvernpolicy

En rapport fra arbeidsgruppen for utvikling av en GDPR-policy
for arbeid med kvalitet i utdanningene ved UiO. Mai 2022.

Arbeidsgruppen var satt ned av UiOs viserektor for utdanning i desember 2021 og består av:

Malcolm Langford, Professor, JUS, senterleder CELL, UiO (leder)
Marte Blikstad-Balas, Professor, UV
Johann Andreas Bolle Bull-Berg, Studentrepresentant, JUS
Jan Arild Dolonen, Sjefingeniør, UV, UiO
Roger Markgraf-Bye, personvernombud, UiO
Vilde Nenseth jurist, USIT, UiO (ersttatet *Are Evju* i permisjonstiden)
Jørgen Hammer Skogan, Studentrepresentant, Studentparlamentet,UiO
Emily-Mary Weitzenboeck, Førsteamanuensis, OsloMet og CELL, UiO
Lena Charlotte Finseth, Studieavdelingen, sekretariat for arbeidsgruppen.

Innholdsfortegnelse

Sammendraget

Bakgrunn. I de siste årene har den høyere utdanningssektoren sett en økende bruk og interesse for *læringsanalyse*. Den handler om registrering, innsamling, analyse og rapportering av data om studenter i en kontekst, der målsettingen er å forstå og forbedre læringsprosessen og det sosiale miljøet der læring foregår. Universitetet i Oslo (UiO) har en lovlig plikt og uttalt ambisjon om å systematisk utvikle arbeidet med kvalitet i utdanningene – der det spesielt vektlegges at arbeidet må være kunnskapsbasert og forankret i empiri, data og analyser. Samtidig har lite skjedd på UiO og i Norge sammenlignet med andre land, av to grunner. Det er komplisert å samle inn data fra mange systemer, og det har vært bekymring rundt personvernhensyn, nærmere bestemt personvernforordningen (GDPR). Behovet for en mer overordnet policy som klargjør UiOs prinsipper og praksis knyttet til læringsanalyse er derfor påkrevet, og denne arbeidsgruppen ble satt ned av rektoratet for å vurdere behov for og innhold i en personvernpolicy for læringsanalyse.

Mandat. Arbeidsgruppen fikk mandat til å vurdere juridiske, personvernmessige og etiske spørsmål knyttet til å etablere læringsanalyse som en pågående og systematisk aktivitet ved UiO – der oppgaven er å utforme prinsipper som kan ligge til grunn for en institusjonell policy for hvordan læringsanalyse kan utformes. Arbeidsgruppen ble bedt om å (1) tydeliggjøre rommet for skjønn som i dag ligger i GDPRs regelverk og i Lov om høyere utdanning; (2) antyde hvordan hensyn knyttet til personvern og etikk kan balanseres mot de samfunnsmessige og institusjonelle gevinster som kan skapes gjennom læringsanalyse; og (3) konkretisere prinsipper for forvaltning og gjennomføring av et UiO-regime for læringsanalyse. I arbeidet ble arbeidsgruppen bedt om å reflektere hvordan prinsippene som foreslås slår ut for ulike interessenter, ikke minst studenter og undervisere, og hvilket ansvar en fremtidig policy har for UiO.

Former for læringsanalyse. Definisjon av læringsanalyse er bred og dekker mange spesifikke formål og mange former. Det er vanlig å skille mellom fem ulike former for læringsanalyse:

(1) ***grunnleggende læringsanalyse*** som innebærer å benytte analysefunksjonene som ligger innbakt i de fleste læringsplattformene som benyttes i dag.

(2) ***prediktiv analyse***, hvor statiske data kombineres med dynamiske data for å forutsi hvordan det kommer til å gå for hver enkelt deltaker, identifisere karakteristiske læringsmønstre for ulike grupper og sette inn relevante tiltak på et tidlig tidspunkt;

(3) ***adaptiv læringsanalyse*** som bygger modeller av deltakernes forståelse av spesifikke tema slik at det blir mulig å automatisere individuelle tilbakemeldinger til deltakerne

(4) ***analyse av sosiale nettverk*** for å synliggjøre relasjoner for å identifisere deltakere som ikke er sosialt og faglig integrert;

(5) ***diskursanalyse***, hvor kvaliteten på det som blir skrevet av deltakerne analyseres slik at systemet vil kunne gi spesifikke tilbakemeldinger til lærere og deltakere om kvaliteten på deres bidrag.

Læringsanalyse har per definisjon samme formål som Universitets- og høgskoleloven § 1-6, som skal sikre og videreutvikle kvaliteten i utdanningen, og som også er videre beskrevet i studietilsynsforskriften § 4-1 om at institusjonen systematisk skal innhente informasjon fra relevante kilder for å kunne vurdere kvaliteten i studietilbudene.

Teknologiske trender. Globalt sett er det i høyere utdanning i USA vi ser den mest omfattende bruken av studenters data til læringsanalyser, ofte med fokus på reduksjon av frafall og prestasjonsgap. Situasjonen i Norge og Europa er annerledes. UH-sektoren i Europa har i liten

grad tatt i bruk læringsanalyse av flere grunner; blant annet mindre konkurranse blant universiteter om utdanningskvalitet, mindre investering i og fokus på kunstig intelligens, og strengere regulering av personvern. Til tross for det ser vi en utvikling på enkelte områder og i enkelte land. Høyere utdanning i Europa har i stadig større grad blitt digitalisert med et fokus på individualisering, plattformisering og infrastrukturering, og datadrevne metoder.

Pedagogisk nytte. Mye av forskningen som er gjennomført om digital læringsanalyse har empiriske data fra høyere utdanning. Flere studier viser forbedret engasjement og læringsutbytte, blant annet hvor studenter bruker dashboards for å kontrollere egen progresjon kan gi forbedret selvregulering, økt motivasjon, og forbedrer sjansene for å gjennomføre emner og karakterer. Flere studier har vist hvordan man kan predikere frafall og deretter gjøre tiltak for å forbedre gjennomstrømming og karaktersnittet til studentene. Mange studier er også gjort på intelligente veiledningssystemer som kan gi automatisert tilbakemelding for å støtte studenters akademiske skriving, problemløsning i STEM-fag, og analysere hvordan studenter samarbeider og løser komplekse problemer i ulike digitaliserte læringsomgivelser. Til tross for flere studier med positive resultater, er det fortsatt vanskelig å påvise tydelige sammenhenger mellom digital læringsanalyse og bedre studentresultater eller studentvelferd. Det er flere årsaker til dette, særlig fordi få institusjonene i UH-sektoren har erfaring med å systematisk ta i bruk læringsanalyse for å forbedre studentenes utdanningstilbud, samt en rekke metodologiske utfordringer innen dette relativt unge forskningsfeltet.

Bruk av læringsanalyse på UiO. Det er stort potensiale for økt bruk av læringsanalyse på UiO. I mange emner er det slik at studentene ikke får noen systematisk vurdering av hvordan emnet går før emnet er sluttvurdert i form av en eksamen, til tross for at alle undervisere kan bruke emneevalueringer underveis. Økt og aktiv bruk av læringsanalyse kan styrke studentenes egen selvregulering ved at de får innblikk i hvordan de ligger an i studiet, og kanskje får automatisert tilbakemelding på hvilke tiltak de kan iverksette for å forbedre progresjonen underveis i emnet. Det kan også hjelpe læreres og institusjonens muligheter til å følge opp og forbedre læring. Per i dag har UiO en god del studieadministrative data i Felles studentsystem (FS) som kan kobles opp til andre data til disse formålene, og læringsanalysemuligheter i eksisterende og framtidige skytjenester på UiO kan bli bedre utnyttet.

Etikk. Læringsanalyse reiser en rekke spørsmål om personvern og praksis. Mange studenter kan allerede oppleve at de digitale systemene til UiO er for inngripende. Den rene mengden av kommunikasjon kan føre til at varsler kan deaktiveres i større grad, som også gjør læringsanalyse mindre nyttig på sikt. Forskning om hva studenter vil ha fra læringsanalyse er litt sprikende, særlig om de vil vite om hvordan deres innsats er sammenlignet med andre. Studenter har høy tillit til høyere utdanningsinstitusjoner og personvernpolitikk, men mange er opptatt av å bli informert, ha muligheter til å medvirke, at samtykke burde brukes hvor mulig (særlig om bruk av sensitive data) og at data ikke selges til private aktører. Det er sterk skepsis til å samle lokasjonsdata uten samtykke, og det burde vært klart for studenter når data skal brukes til pedagogiske formål eller forskning.

Andre etiske problemstillinger med læringsanalyse inkluderer risikoen for standardisering. Konstant analyse og tilbakemelding basert på studentenes aktivitet kan også føre til at studentene opplever å måtte studere og tilegne seg kunnskap på en foreskrevet måte. Dersom mye av dataene som spores i tillegg knyttes til enkeltindivider, vil det kunne påvirke studentene til å samarbeide mindre enn de gjør i dag, eller føre til at færre begynner å samarbeide i fremtiden. Læringsanalyse for samarbeid blir også viktig. Som mange andre teknologier er det i tillegg en bekymring om læringsanalyse er presis nok for spesifikke formål, gitt at datasett eller algoritmer kan inneholde feil.

Personvern og GDPR. Behandling av personopplysninger i læringsanalyse berører rett til privatlivets fred, en viktig menneskerettighet, hjemlet blant annet i Grunnloven og menneskerettighetskonvensjoner. Inngrep krever en tilstrekkelig lovhjemmel, at staten forfølger et legitimt formål, og at inngrepet er forholdsmessig. Behandling av personopplysninger er regulert i detalj i personopplysningsloven, og EUs personvernforordning (GDPR). Det kreves at behandling av personopplysninger er i samsvar med lovlighet, rettferdighet og åpenhet; formålsbegrensningsprinsippet; og dataminimeringsprinsippet – og at personopplysninger skal være adekvate, relevante og riktige, behandlet på en sikker måte og at noen er ansvarlig for å ivareta prinsippene.

Særlig om rettslig grunnlag. All behandling av personopplysninger i forbindelse med utvikling og/eller bruk av læringsanalyseverktøy krever et rettslig grunnlag. I praksis kan flere rettslige grunnlag være aktuelle, men for læringsanalyseformål er det særlig behandlinger som er i allmennhetens interesse og som kan hjemles i et supplerende rettslig grunnlag i nasjonal rett som vil være aktuelt. Universitets- og høyskoleloven § 1-6 og studiekvalitetsforskriften § 2-1, knytter seg eksempelvis til utdanningsinstitusjonens systematiske arbeid for å sikre og utvikle kvaliteten i egne studietilbud gjennom et system for kvalitetssikring. Behandling av særlige kategorier personopplysninger er i utgangspunktet forbudt, men kan behandles dersom det kan hjemles i ett av unntakene i GDPR art. 9(2). Dersom UiO ønsker å gjenbruke allerede (lovlige) innsamlede personopplysninger til læringsanalyse, må det vurderes om denne viderebehandlingen er forenlig med det opprinnelige formålet.

De registrertes rettigheter og dataminimering under GDPR. Før læringsanalysesystemer og -løsninger tas i bruk, er det et krav at både studenter og lærere informeres om systemet og løsningen, og personopplysninger som behandles må være korrekte og, om nødvendig, oppdaterte. En student har rett til å ikke være gjenstand for en avgjørelse som *utelukkende* er basert på automatisert behandling og som har rettsvirkning for eller på tilsvarende måte i betydelig grad kan påvirke vedkommende – med mindre man tilfredsstiller de forskjellige kravene i GDPR. Når personopplysninger er behandlet har den registrerte vanligvis til enhver tid, rett til å protestere mot behandlingen. Ved utvikling, anskaffelse eller annen form for valg av læringsanalysesystem og -løsning, skal det sørges at det eventuelle systemet og løsningen som utvikles/velges overholder krav til innebygd personvern og personvern som standardinnstilling. Når det er sannsynlig at en type behandling «vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlig før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet», såkalt «DPIA» (*Data Protection Impact Assessment*). Hvis personopplysninger er behandlet utenfor EU/EØS er det nødvendig å sørge for at det høye beskyttelsesnivået under GDPR opprettholdes i praksis.

Medvirkning. Forskning og tilbakemelding fra studentrepresentanter viser at studenter vil medvirke til bruk av deres opplysninger selv om tillit til institusjoner er ganske høy. Studentenes individuelle rett til kontroll over egne data er regulert gjennom personopplysningsloven, men også i uhl. § 4-1, hvor studentorganene skal «høres i alle saker som angår studentene på det aktuelle nivå». Dessuten har studenter en eksplisitt rett til å delta i spørsmål som gjelder læringsmiljø, uhl. § 4-3 (1), som inkluderer deltagelse i læringsmiljøutvalget, der studentene har like mange representanter som institusjonen. Datainnsamling og læringsanalyse kan innebære omfattende og inngripende prosesser som berører studentene direkte og deres læringsmiljø. Etter vår vurdering er det viktig at studenter informeres om rettighetene de har i innsamlingen av data, på en tydelig måte som er offentlig kjent; at de har en reservasjonsrett med «opt-in» og «opt-out» løsninger for bruk av

læringsanalyse i bruk av data i sensitive områder (for eksempel intervensjoner rettet mot studenters helse), eller som krever mye av studenters oppmerksomhet eller tid; at UiOs læringsmiljøutvalg bør få et spesifisert ansvar for å sikre etterlevelsen av universitetets plikter i forbindelse med læringsanalyse; de lokale læringsmiljøutvalgene ved fakultetene ser løpende på bruk av læringsanalyse; behandlingen av dataene til læringsanalyse bør avgrenses til dem som har behov for tilgang ut fra formålene til bruk av personopplysninger; og resultatene, konklusjonene og beslutningene som fattes med bakgrunn i innsamlet datamateriale bør være offentlig tilgjengelige.

Underviseres autonomi og medvirkning. Vitenskapelige ansatte og andre som gir undervisning har et selvstendig faglig ansvar for innhold og opplegg av denne innenfor de rammer som institusjonen fastsetter eller som følger av lov eller i medhold av lov (§1-5 andre ledd). Systematisk arbeid for kvalitetssikring, inkludert læringsanalyse, vil påvirke rammer til undervisning. Undervisere har særlig frihet når det gjelder fremstilling av materiale, perspektiver som fremheves, og det rent kildemessige, så lenge temaene i relevante studieplaner blir ivaretatt, og de har et ansvar for læringsmiljø i relevante undervisningssituasjoner. Læringsanalyse som knyttes til studentrelasjoner og undervisningopplegg vil også være tjent med forutsigbarhet skapt gjennom en diskusjon av hvordan man som miljø skal etablere endringer for å fremme kvalitet. For foreleseres tillit er det dessuten viktig at statistikken læringsanalyse gir ikke muliggjør uthenging eller skaper unødvendig sammenligner mellom forelesere.

Institusjonalisering. I dag har ikke UiO et koordinert og helhetlig system for kvalitetssikring av digital læringsanalyse, særlig i forhold til vurdering av de juridiske kravene, etiske hensyn og tilstrekkelig medvirkning. UiO har etablerte rutiner som dekker mange elementer for bruk av læringsanalyse på UiO, særlig når det gjelder tjenester til databehandling, innkjøp av nye digitale skytjenester, samt forskning med læringsanalyse. Men det er manglende veiledning til systemeiere og USIT om det rettslige grunnlaget for læringsanalyse (som betyr at læringsanalyse ofte ikke er tatt i bruk), sterk desentralisering av søknadsprosessen til systemeiere for tilgang til data for bruk som faller utenfor prosesser for innkjøp av skytjenester; manglende direkte involvering av studenter og ansatte for avgjørelser om bruk av personopplysninger i læringsanalyse; manglende oversikt av i hvilken grad studenters og læreres data er brukt i eksisterende læringsanalyse på UiO; og manglende støtte til ansatte som vil bruke verktøy som krever overføringer av personopplysninger ut av EØS.

Modeller og kompetanseheving. Arbeidsgruppen har skissert tre forskjellige modeller for vurdering av verktøy som inneholder læringsanalyse for kvalitetsarbeid:

1. *Hybrid*. UiO fortsetter med dagens modell med blanding av sentraliserte og desentraliserte prosesser, men med ekstra veiledning og støtte.
2. *Sentralisert*. UiO skaper en ny intern rutine for bruk av personopplysninger til kvalitetsarbeid.
3. *Delegert*. UiO delegerer vurdering av personopplysninger til kvalitetsarbeid til en ekstern aktør som Sikt.

Dersom UiO ønsker økt bruk av læringsanalyse, forutsetter dette også en målrettet kompetanseheving både på fakultet og instituttnivå, slik at dataene kan brukes til å forbedre emner over tid og evaluere på emnenivå, og alle er bevisst om de etiske dilemmaene og juridiske kravene.

På grunn av disse konklusjoner har arbeidsgrupper utviklet et forslag om de følgende prinsipper:

Forslag til UiO-prinsipper om personvern i læringsanalyse for kvalitetsarbeid

1. Innledning

1. **Definisjon**. Læringsanalyse omfatter registrering, innsamling, analyse og rapportering om studenter i en kontekst, der målsettingen er å forstå og forbedre læringsprosessen og det sosiale miljøet der læring foregår.
2. **Formål**. Læringsanalyse er et viktig, og til dels nødvendig, element i oppfyllelsen av UiOs forpliktelser i Universitets- og høgskoleloven ved å sikre et «internt system for kvalitetssikring som skal sikre og videreutvikle kvaliteten i utdanningen» (§1-6).[1]

2. Personvern

3. **Personopplysninger**. Læringsanalyse kan skje ved å bruke personopplysninger, for eksempel ved å bistå en student enkeltvis eller tillate en lærer enkeltvis, eller ved å bruke aggregerte og anonymiserte data til å hjelpe andre studenter.
4. **Etikk og studenter**. Læringsanalyse skal brukes til studentenes beste, bruk av personopplysninger skal minimeres, og studenter og ansatte skal ha muligheten til å medvirke bruk av deres personopplysninger.
5. **Rett til privatliv**. UiOs behandling av personopplysninger for læringsanalyse skal skje i samsvar med *rett til privatliv* som er hjemlet bl.a. i Grl. § 102 og Den europeiske menneskerettighetskonvensjonen (EMK) art. 8[2] Inngrep krever en tilstrekkelig hjemmel, at staten forfølger et legitimt formål, og at inngrepet er forholdsmessig.
6. **Personvernforordning**. UiOs behandling av personopplysninger for læringsanalyse skal skje i samsvar med *personvernforordningen,* og prinsippene i artikkel 5 i personvernforordningen som understreker at personopplysninger skal:
    a. behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),
    b. samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles på en måte som er uforenlig med disse formålene;
    c. være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),
    d. være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),
    e. lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for;
    f. behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene

3. Det rettslige grunnlaget i GDPR og prinsippene til konkret vurdering

7. **Behandlingsgrunnlag**. I prinsippet kan disse behandlingsgrunnlagene i personvernforordningen artikkel 6 nr. 1 bli relevant for læringsanalyse for kvalitetsarbeid: (a) samtykke (b) oppfyllelse av avtale (c) rettslig forpliktelse; (e) utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet; (f) berettigede interesser.

---

[1] Kvalitetsarbeid innebærer, ifølge Forskrift om kvalitetssikring og kvalitetsutvikling i høyere utdanning og fagskoleutdanning, at UiO «skal» jobbe «systematisk», «legge til rette for løpende utvikling», «kunne avdekke sviktende kvalitet i studietilbudene» og «sikre tilfredsstillende dokumentasjon av kvalitetsarbeidet.»

[2] Som er inkorporert i norsk lov: jf. menneskerettsloven, § 2 nr. 1.

8. **Relevant behandlingsgrunnlag**. I praksis er de mest relevante grunnlaget *i denne sammenheng* artikkel 6(1)(e), i tilfeller der det:
   a. er nødvendig for å oppnå formålet som er i allmennhetens interesse eller ved utøvelse av offentlig myndighet;
   b. kan dokumenteres at læringsanalyse virkelig er nødvendig for å oppnå dette formålet, og at det ikke finnes noe alternativ;
   c. kan forankres i et supplerende rettslig grunnlag i unionsretten eller i nasjonal rett, som vanligvis betyr at det skal sikre og videreutvikle kvaliteten i utdanningen etter uh-loven §1-6.

   Samtykke i artikkel 6(1)(a) skal som regel ikke anvendes som rettslig grunnlag siden samtykket må være frivillig, og maktforholdet mellom studenter eller ansatte og UiO som behandlingsansvarlig er ubalansert.
9. **Konkret vurdering**. UiO skal videreutvikle prinsipper eller atferdsnormer til å bistå i konkrete vurderinger om behandling av personopplysninger i konkrete læringsanalyseprosjekter oppfyller kriteriene i artikkel 6(1)(e).
10. **Rettslig forpliktelse.** UiO skal utforske i hvilken grad de relevante rettslige forpliktelser i uh-loven er klare og tydelige nok slik at artikkel 6(1)(c) kan vurderes som et rettslig grunnlag til enkelte former for læringsanalyse.
11. **Særlige kategorier av personopplysninger**. Behandling av særlige kategorier av personopplysninger skal bare skje hvis hjemlet i ett av unntakene i GDPR art. 9(2), for eksempel at behandlingen er nødvendig av hensyn til viktige allmenne interesser (bokstav g). I utgangspunktet skal ikke UiO utvikle, anvende, anskaffe eller bruke verktøy som behandler særlige kategorier personopplysninger. Dersom særlige kategorier likevel skal behandles skal det være tydelig og godt dokumentert at studenters læringsprosess og læringsmiljøet vil forbedres. UiO skal som regel forsøke å gi studenter reservasjonsrett i slike situasjoner.
12. **Gjenbruk av data**. Dersom allerede innsamlede personopplysninger for et annet formål skal gjenbrukes til læringsanalyse, må det vurderes om denne viderebehandlingen er forenlig med det opprinnelige formålet. Det er viktig at hver behandlingsaktivitet vurderes konkret og for seg.
13. **Innebygd personvern**. Ved utvikling, anskaffelse eller annen form for valg av læringsanalysesystem og -løsning, skal det sørges at det eventuelle systemet og løsningen som utvikles/velges overholder krav til innebygd personvern og personvern som standardinnstilling.
14. **DPIA (*Data Protection Impact Assessment*), personvernkonsekvensanalyse.** Hvis læringsanalyse inkluderer behandling av personopplysninger skal den behandlingsansvarlige alltid før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet, en DPIA, i tråd med Datatilsynets liste over behandlingsaktiviteter som alltid krever en vurdering av personvernkonsekvenser.
15. **Overføring til andre land**. Personopplysningsvernet som studenter og ansatte har innen EU/EØS skal opprettholdes i praksis dersom personopplysninger overføres til tredjeland. UiO skal støtte bedre vurderingsprosesser og forhandlinger med leverandører om løsninger som imøtekommer personvernkravene (se prinsipp § 31).

4. Registrertes rettigheter og medvirkning

16. **Rett til informasjon.** Før læringsanalysesystemer og -løsninger tas i bruk må både studenter og lærere informeres om systemet og løsningen på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk.
17. **Rett til retting.** UiO skal sikre at personopplysninger som behandles er korrekte og, om nødvendig, oppdaterte.
18. **Helautomatiserte individuelle avgjørelser.** En student har rett til å ikke være gjenstand for avgjørelser som *utelukkende* er basert på automatisert behandling, herunder profilering, og som

har rettsvirkning for eller på tilsvarende måte i betydelig grad kan påvirke vedkommende. Eventuell bruk må inkludere tiltak og garantier etter art. 22(3) i personvernforordningen, lovhjemmel etter art. 22(2), samt informasjonen til de registrerte om den underliggende logikken og forventede konsekvenser. Bruk av profilering krever godkjenning av universitetsstyret.

19. **Rett til å protestere** Når behandlingsgrunnlag er hjemlet i enten GDPR artikkel 6 nr. 1 bokstav e eller f har den registrerte til enhver tid, rett til å protestere mot behandlingen.

5. Studentmedvirkning og underviseres autonomi

20. **Studentmedvirkning**. Studentorganer har rett til å bli hørt i alle saker som angår bruk av studentenes personopplysninger i læringsanalyse på det aktuelle nivået, inkludert når det påvirker læringsmiljøet (i uhl. § 4-1, 4-3).
21. **Informasjon og reservasjonsrett**. Studenter skal informeres om rettighetene de har ved innsamling av data og at de har reservasjonsrett for bruk av data på sensitive områder eller på områder som krever mye av studentenes oppmerksomhet. Konklusjonene og beslutningene som fattes med bakgrunn i innsamlet datamateriale bør være offentlig tilgjengelige.
22. **Læringsmiljøutvalg.** UiOs læringsmiljøutvalg, evt. lokale læringsmiljøutvalg, skal få et spesifisert ansvar for å sikre etterlevelsen av universitetets plikter i forbindelse med læringsanalyse.
23. **Underviseres autonomi**. Vitenskapelige ansatte og andre som gir undervisning har et selvstendig faglig ansvar for innhold og opplegg av denne innenfor de rammer som institusjonen fastsetter eller som følger av lov eller i medhold av lov (§ 1-5 andre ledd). Systematisk arbeid for kvalitetssikring, inkludert læringsanalyse, kan påvirke disse rammene. Undervisere har særlig frihet når det gjelder fremstilling av materiale, perspektiver som fremheves, og det rent kildemessige, så lenge temaene i relevante studieplaner blir ivaretatt.
24. **Ansvar for læringsmiljø og deltagelse**. Undervisere har delansvar for læringsmiljø i relevante undervisningssituasjoner, og læringsanalyse som knyttes til studentrelasjoner og undervisningsopplegg vil også være tjent med forutsigbarhet skapt gjennom en diskusjon av hvordan man som miljø skal etablere endringer for å fremme kvalitet. For foreleseres tillit er det viktig at statistikken læringsanalyse gir ikke muliggjør uthenging eller skaper unødvendig sammenligning mellom forelesere.

6. Institusjonalisering

25. **System for kvalitetssikring og kontroll**. UiO skal sikre at det blir et koordinert og helhetlig system for kvalitetssikring av digital læringsanalyse, særlig i forhold til vurdering av de juridiske kravene, etiske hensyn og tilstrekkelig medvirkning
26. **Veiledning**. UiO skal utvikle tilstrekkelig veiledning til systemeiere, USIT og andre om det rettslige grunnlaget til læringsanalyse
27. **Åpenhet**. UiO skal publisere en oversikt over i hvilken grad studenters og læreres data er brukt i eksisterende læringsanalyse på UiO
28. **Tredjeland.** UiO skal koordinere og forbedre støtte til ansatte som vil bruke verktøy som krever overføringer av personopplysninger ut av EØS, særlig gitt kravene i Schrems II-dommen.
29. **Vurdering av søknader**. UiO skal utvikle et effektivt system for vurdering av søknader, enten det er et kvalitetsløft i dagens hybride system, et sentralisert system eller delegert arbeid til en ekstern aktør.
30. **Kompetanseheving**. UiO skal sikre målrettet kompetanseheving både på fakultet og instituttnivå, slik at dataene kan brukes til å forbedre utdanning, og at alle er bevisst de etiske dilemmaene og juridiske kravene.

1. Introduksjon

1.1 Bakgrunn

I de siste årene har den høyere utdanningssektoren sett en økende bruk og interesse for *læringsanalyse*. Den er gjerne definert som «registrering, innsamling, analyse og rapportering av data om [studenter] i en kontekst, der målsettingen er å forstå og forbedre læringsprosessen og det sosiale miljøet der læring foregår» (Dahl, 2015:2). Innføring av digitale plattformer på universiteter, samling av store mengder data om studenter og læringsprosesser, samt forskning- og utviklingsprosjekter har signalisert muligheter til å forbedre utdanningspraksiser.

Universitetet i Oslo (UiO) har en lovlig plikt og uttalt ambisjon om å systematisk utvikle arbeidet med kvalitet i utdanningene – der det spesielt vektlegges at arbeidet må være kunnskapsbasert og forankret i empiri, data og analyser. Det har blitt pekt på at UiO derfor må teste ut og akselerere bruk av læringsanalyse der det kan forbedre kvaliteten på utdanningen. I dag finnes det allerede mye data om studentene, deres resultater og deres læringsløp ved UiO. Det har i noen tid vært arbeidet en del med å tilrettelegge for gode læringsanalyser ved UiO (f.eks. gjennom enkle oversikter i såkalte "dashboard" i Canvas) – og arbeidet har blitt aktualisert gjennom den digitale oppskalering som har skjedd gjennom pandemien, hvor nye digitale plattformer har blitt tatt i bruk, samt den økte bruken av ulike undersøkelser rettet mot studentenes læringsmiljø og evaluering av undervisning.

Samtidig har lite skjedd på UiO og i Norge sammenlignet med andre land. Det er to grunner til dette, som henger sammen. For det første er det slik at mange data fra ett system som samles inn, i liten grad kan koples med andre typer data fra andre systemer, noe som ville muliggjort dypere og mer innsiktsfulle analyser av studentenes læringsløp, og hvilke faktorer som positivt og negativt påvirker studentenes læringsutbytte og velferd. For det andre har arbeidet med å samle inn og sammenstille data for bruk av læringsanalyse stoppet opp på grunn av bekymring rundt personvernhensyn, nærmere personvernforordningen (GDPR). I dette arbeidet har UiO i økende grad sett at utfordringer for å kunne utvikle læringsanalyse har mange dimensjoner – inkludert juridiske og etiske aspekter. Lovgivningen – slik som den er utformet – gir et rom for juridisk skjønn som det kan være utfordrende å håndtere i det daglige arbeidet, ikke minst fordi det både er tidkrevende og kan skape en lite systematisk og effektiv håndtering av læringsanalysearbeidet. Opplæringsutvalget NOU 2019: 23 noterte eksplisitt manglende utvikling av atferdsnormer (en "Code of Conduct") for GDPR-baserte vurderinger av læringsanalyse i Norge.

Behovet for en mer overordnet policy som klargjør UiOs prinsipper og praksis knyttet til læringsanalyse er derfor påkrevet. En arbeidsgruppe ble satt ned av rektoratet for å vurdere behov for og innhold i en personvernpolicy for læringsanalyse. UiO er for øvrig kjent med at det er oppnevnt en nasjonal ekspertgruppe for læringsanalyse, og UiOs arbeid med en GDPR-policy kan bli et verdifullt bidrag inn i dette nasjonale initiativet. To av medlemmene i UiOs arbeidsgruppe sitter også i den nasjonale ekspertgruppen, men uttaler seg i denne rapporten bare på vegne av UiOs arbeidsgruppe.

1.2 Mandat og representanter

Arbeidsgruppen skal vurdere juridiske, personvernmessige og etiske spørsmål knyttet til å etablere læringsanalyse som en pågående og systematisk aktivitet ved UiO – der oppgaven er å utforme prinsipper som kan ligge til grunn for en institusjonell policy for hvordan læringsanalyse kan utformes. Arbeidsgruppen ble bedt om å:

- Tydeliggjøre rommet for skjønn som i dag ligger i GDPRs regelverk og i Lov om høyere utdanning – ikke minst vurdert mot det ansvaret som universiteter og høyskoler har for å sikre studenters læring.
- Antyde hvordan hensyn knyttet til personvern og etikk kan balanseres mot de samfunnsmessige og institusjonelle gevinster som kan skapes gjennom læringsanalyse
- Konkretisere prinsipper for forvaltning og gjennomføring av et UiO-regime for læringsanalyse, inklusive innsamling og utlevering av data, som kan støtte opp under et systematisk arbeid for å utvikle studiekvalitetsarbeidet og studentenes læringsprosesser. Prinsippene bør også adressere hvordan data som er samlet inn kan utnyttes til forskning innen dette feltet.

I arbeidet ble arbeidsgruppen bedt om å reflektere hvordan prinsippene som foreslås slår ut for ulike interessenter, ikke minst studenter og undervisere, og hvilket ansvar som en fremtidig policy har for UiO. Arbeidsgruppen ble også bedt om å antyde hvordan arbeidet med å opprette et regime for læringsanalyse kan opprettes og hvilke praksiser og rutiner som eventuelt må utvikles i denne forbindelse.

UiO ser det som hensiktsmessig at arbeidsgruppen har en representasjon som balanserer ulike hensyn. Juridisk, pedagogisk, teknisk og organisatorisk kompetanse og ekspertise er derfor viktig å inkludere. Samtidig bør både undervisere og studenter ha representasjon i gruppen. Gruppen består av:

- *Malcolm Langford*, JUS/CELL (leder)
- *Jan Arild Dolonen*, UV
- *Roger Markgraf-Bye*, personvernombud
- *Are Evju*, USIT, jurist (*Vilde Nenseth* fungerer i permisjonstiden)
- *Johann Andreas Bolle Bull-Berg*, Studentrepresentant, JUS
- *Jørgen Hammer Skogan*, Studentrepresentant, Studentparlamentet
- *Emily-Mary Weitzenboeck*, CELL/OsloMet
- *Marte Blikstad-Balas*, UV
- *Lena Charlotte Finseth*, Studieavdelingen, sekretariat for arbeidsgruppen.

1.3 Rapportens struktur og avgrensinger

Rapporten begynner i del 2 med en kort oversikt av definisjoner og konsepter, deretter en diskusjon i del 3 av innledende problemstillinger av teknologisk, pedagogisk og etisk art. Denne diskusjonen er viktig både som bakgrunn og konkret faktagrunnlag til vurdering av juridiske og etiske spørsmål. I del 4 diskuterer vi personvernforordningen med fokus på personvernsprinsipper, det rettslige grunnlaget til databehandling, registrertes rettigheter og minimering av risiko. I del 5 analyserer vi muligheter for medvirkning av studenter og ansatte om databruk, samt institusjonalisering av personvernforordningen i læringsanalyseprosesser på

UiO (f.eks. søknader, cybersikkerhet og kontroll). I del 6 konkluderer vi analysen og introduserer vårt forslag til prinsipper.

Fokuset i denne rapporten er på kvalitetsarbeid med utdanning, ikke forskning på utdanning. Forskning på og ved bruk av læringsanalyse i høyre utdanning må skje i samsvar med eksisterende ordninger, blant annet gjennom melding til Sikt (tidl. NSD) for en personvernvurdering og godkjenning på UiO hvis Sikt vurderer at prosjektet innebærer høy risiko. Se UiOs *Rutine for forskning med personopplysninger*. [3] Samtidig er det mange læringsanalyseprosjekter- og systemer som inkluderer forskning og kvalitetsarbeid, både sekvensielt og samtidig. Vi har derfor foreslått at rutinene for forskning og kvalitetsarbeid (inkludert vårt forslag om læringsanalyse) avklarer grensene og gjør det enklere for forskere, administrative ansatte, utviklere og andre til å forstå når de forskjellige rutinene må tas i bruk og oppdateres underveis.

2. Definisjoner og konsepter

Læringsanalyse eller digital læringsanalyse er de vanlige norske uttrykkene for det engelske «learning analytics». Oversettelsen fungerer ikke særlig godt. Begrepet «analytics» impliserer at læringsanalyse har med digital teknologi og statistisk analyse å gjøre, noe som ikke tilsvarer det norske «analyse». I følge Oxford English Dictionary, er analytics «systematic computational analysis of data or statistics». I denne rapporten bruker vi læringsanalyse etter den engelske forståelsen.

Læringsanalyse er vanligvis definert som «the measurement, collection, analysis, and reporting of data about learners and their contexts, for the purposes of understanding and optimizing learning and the environments in which it occurs.»[4]

På den ene siden er det en bred definisjon som dekker mange formål og mange former læringsanalyse, som har store implikasjoner for etiske og juridiske vurdering. Både MOOC-utvalget og UNESCO Institute for Information Technologies in Education skiller mellom fem ulike former for læringsanalyse:

> (1) ***grunnleggende læringsanalyse*** som innebærer å benytte analysefunksjonene som ligger innbakt i de fleste læringsplattformene som benyttes i dag (f.eks. for å visualisere datalogger og synliggjøre aktivitet);
>
> (2) ***prediktiv analyse***, hvor statiske data (f.eks. demografi og tidligere studieresultater) kombineres med dynamiske data (f.eks. innloggingsmønstre på et *learning management system* (LMS)) for å forutsi hvordan det kommer til å gå for hver enkelt deltaker, identifisere karakteristiske læringsmønstre for ulike grupper og sette inn relevante tiltak på et tidlig tidspunkt;
>
> (3) ***adaptiv læringsanalyse*** som bygger modeller av deltakernes forståelse av spesifikke tema slik at det blir mulig å automatisere individuelle tilbakemeldinger til deltakerne
>
> (4) ***analyse av sosiale nettverk*** for å synliggjøre relasjoner for å identifisere deltakere som ikke er sosialt og faglig integrert;

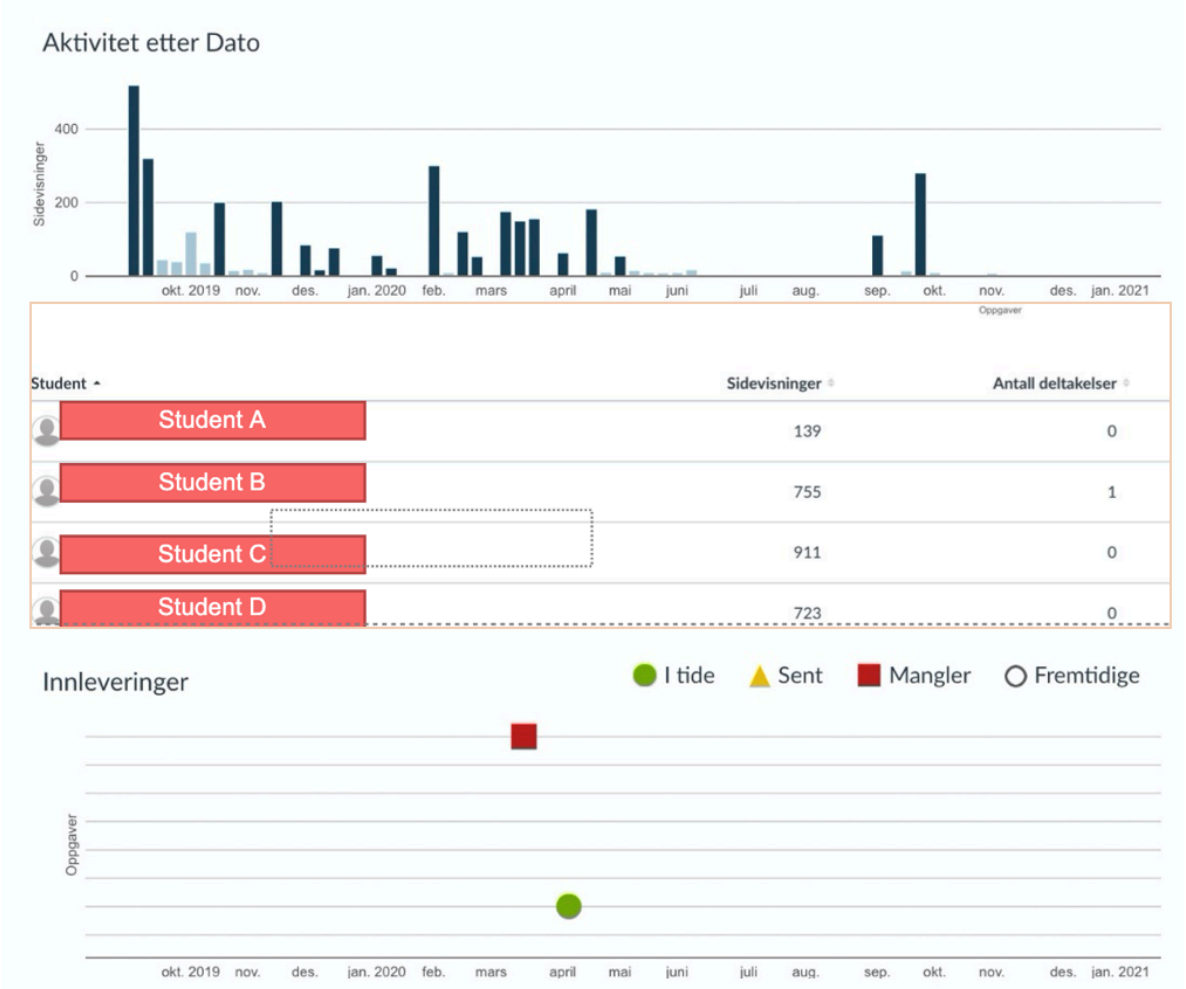
[3] https://www.uio.no/for-ansatte/arbeidsstotte/personvern/rutine-for-forskning-med-personopplysninger.html
[4] SOLA 2011.

(5) ***diskursanalyse***, hvor kvaliteten på det som blir skrevet av deltakerne analyseres slik at systemet vil kunne gi spesifikke tilbakemeldinger til lærere og deltakere om kvaliteten på deres bidrag.

Dessuten kan de datavitenskapelige metodene variere betydelig fra beskrivende statistikk og standard regresjonsanalyser til datavitenskapelig tekst- og nettverksanalyser til kunstig intelligens med bruk av regelbasert programmering og maskinlæring.

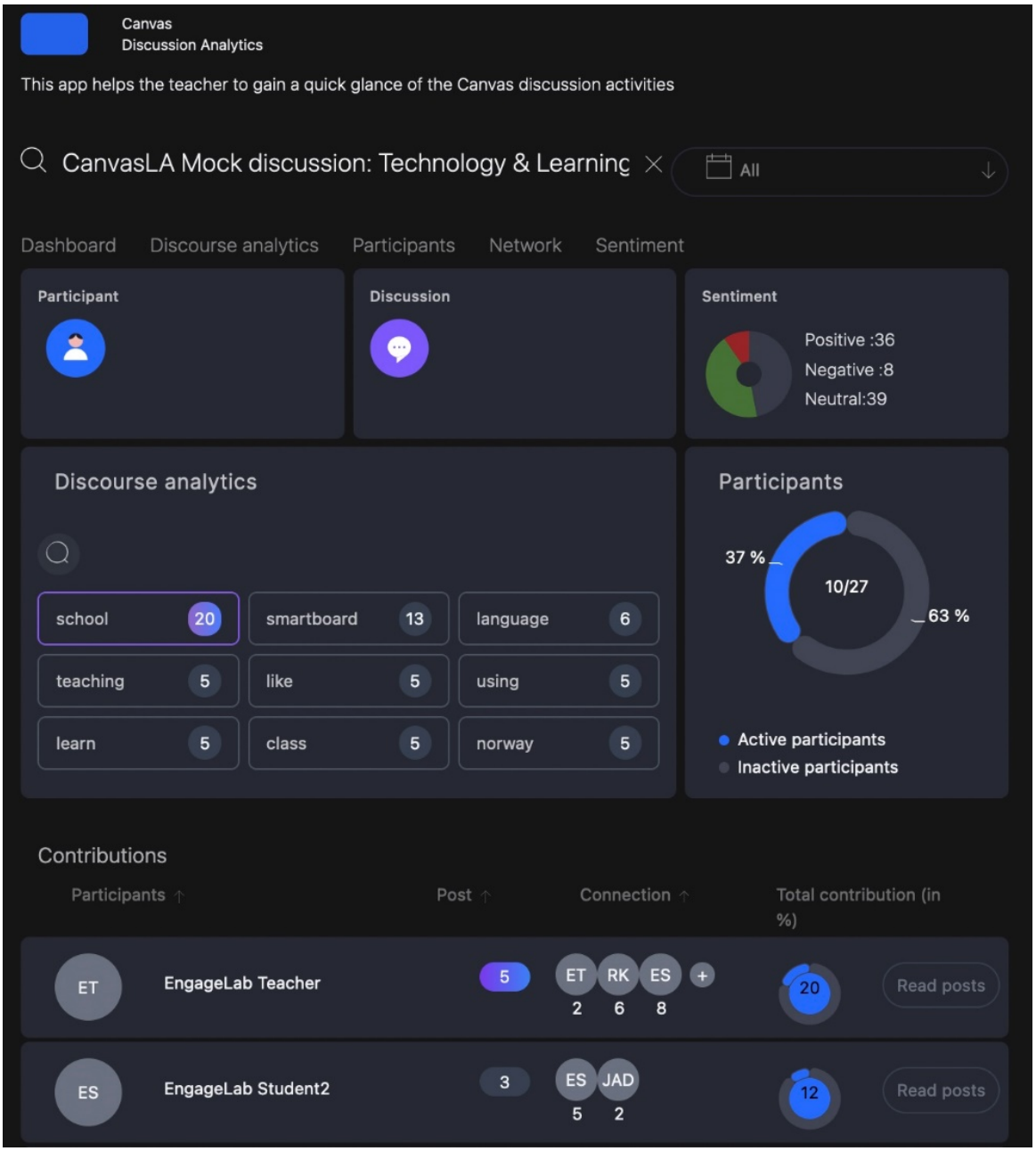
I figurene under viser vi noen eksempler på læringsanalyse. I figur 1 viser vi et Dashboard fra Canvas om en enkeltstudent hvor underviser får en enkel oversikt over studentens handlinger i LMSet som sidehenvisninger, individuell aktivitet, og om innleveringer er i tide, for sent eller mangler.

Figur 1 Dashboard fra Canvas



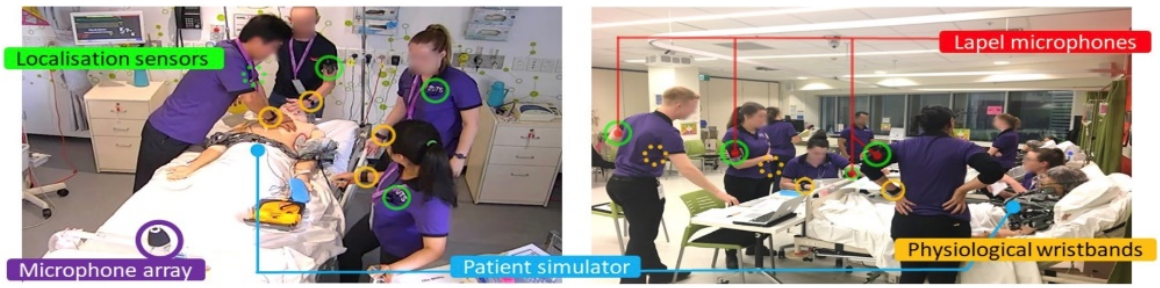
I figur 2 viser vi et Canvas diskusjonsanalyseverktøy utviklet ved UiO. Rasjonalet bak verktøyet er å støtte arbeid i diskusjonsforum for å kunne justere undervisningsopplegget underveis. Med et raskt blikk får underviser oversikt over deltakelse og bruk av fagbegreper, hvem studentene interagerer med, og i hvilken grad ytringene i forumet (sentimentet) er av positiv eller negativ karakter (Kaliisa & Dolonen, 2022).

Figur 2 Canvas Dashboard Analytics



I figur 3 viser vi et eksempel på multimodal læringsanalyse fra Monash University, Australia der de samler inn data fra ulike sensorer (lokasjon, puls, svette, m.m.), medisinsk mannekeng, video og audio for å kunne utsi noe om studentgruppers evne til å håndtere komplekse problemløsningssituasjoner. Gjennom innsamlede multimodale data, og en modell for problemløsning med et regelbasert system for tolkning, genererer systemet automatiserte rapporter med tilbakemelding til studentgruppene og lærere på om gruppene løser oppgavene (Echeverria mfl., 2019).

Figur 3 Multimodal læringsanalyse fra Monash University



Please click here to see the teacher summary report:

Print

Rule	Team Feedback	Outcome
prioritisation of care - 4 BEDS a. Initial Handover - Priority - za. Bed 4. Patient recovery	priorisation could have been improved in this scenario For the selected period, the team spent **17.64 %** (percent) of their time on **Bed 3**	
Administer Naloxone l. Bed 4. Administer Naloxone - After - k. Bed 4. Cease PCA	The team reacted on time and provided the right medication for the patient. After PCA overdose Naloxone was an alternative to improve the patient's status.	
Administer Oxygen f. Bed 4. Administer Oxygen - After - e. Bed 4. Patient Clinical deterioration - respiratory depression	Well done, after patient respiratory depression the patient developed SOB (Shortness of Breath) and the team correctly validated how to provide oxygen supply.	

På den andre siden er læringsanalyse begrenset og burde ikke dekke all bruk av teknologier for læring eller alle digitale tilnærminger til utvikling av kvaliteten i utdanningen. For eksempel er det mange aspekter av adaptiv læringsanalyse som ikke faller godt inn under definisjon av læringsanalyse (Ekspertgruppen for digital læringsanalyse, 2022: kap. 3.4). Det adaptive elementet – som innebærer en form for automatisert, individualisert tilpasning til en student i undervisning, eller vurdering ved hjelp av algoritmer – er sannsynligvis utenfor, men systemene frembringer kontinuerlig data for læringsanalyse, direkte til studenten, men også til undervisere og utdanningsinstitusjoner.

Denne hybriditeten reiser en organisatorisk utfordring siden læringsanalysesystemer ofte er innebygget i mange forskjellige teknologier, fra Canvas og Zoom til avanserte språkteknologier som gir automatiserte tilbakemeldinger – som UiO både anskaffer og utvikler selv. Et viktig spørsmål er i hvilken grad UiO burde utvikle retningslinjer om personvern som dekker (1) bare læringsanalyse-rettet verktøy; (2) alle digitale verktøy som inneholder læringsanalyse; eller (3) alle digitale verktøy som brukes til utdanning og relatert kvalitetsarbeid. Diskusjoner med UiOs utdanningskomité tydet på at man burde tenke bredt gitt at feltet er i utvikling.

3. Innledende problemstillinger

3.1 Teknologi

I denne delen skal vi se på hovedtrendene innenfor utvikling av digitale læringsanalyser og hvilke typer verktøy vi kan se i norske og europeiske forhold. Globalt sett er det i høyere utdanning i USA vi ser den mest omfattende bruken av studenters data til læringsanalyser. For eksempel begynte Georgia State universitet å bruke prediktiv analyse allerede i 2012, hvor de opplyser at daglig dekker de 800 forskjellige risikofaktorer for mer enn 40 000 studenter, med cirka 90 000 intervensjoner årlig basert på varslene.[5] Ved Purdue University i USA, har de også brukt et prediktivt system kalt 'Course Signal' i over 10 år, og gjennom tiltak ovenfor studenter i faresonen påstår at de har klart å heve både gjennomsnittskarakterer samtidig som frafallet sank signifikant. Ved University of Michigan har de laget Canvas dashboards både for studenter og undervisere som gir de muligheter til å sjekke progresjon i emner, og gi adaptive tilbakemeldinger til studentene basert på prestasjoner, og hvordan de ligger an i forhold til eksamen. Et stort flertall (89%) av studentene rapportere at dashboardet er enkelt å bruke, og et viktig hjelpemiddel i studiene.

Situasjonen i Norge og Europa er annerledes. Praksisfeltet tyder på at UH-sektoren i Europa i liten grad har tatt i bruk læringsanalyse av flere grunner, blant annet mindre konkurranse blant universiteter om utdanningskvalitet, mindre investering i og fokus på kunstig intelligens og strengere regulering av personvern. I en større studie blant 45 institusjoner fra 23 europeiske land fant Tsai mfl. (2020) at de aller fleste institusjonene hadde svært begrenset erfaring med læringsanalyse, og kun prøvde det ut i liten skala innen enkelte emner. Kun en tredjedel hadde løsninger der data fra lærings- og studiesystemer ble samlet inn, og prøvde å bruke det vertikalt i organisasjonen (f.eks. til beslutningstaking på ledelsesnivå). Studien har i tillegg en viss skjevhet da kun institusjoner som var interessert i læringsanalyse ønsket å delta, og det er derfor trolig at erfaring med læringsanalyse er enda lavere enn rapportert. Ser man på de mer etablerte (elite)universitetene så er de fortsatt campusbaserte der digitale ressurser og læringsanalyse tas i bruk, men avgrenset til enkeltemner.

Til tross for det ser vi en utvikling på enkelte områder og land. Høyere utdanning i Europa har i stadig større grad blitt digitalisert med et fokus på individualisering, plattformisering og infrastrukturering og datadrevne metoder. Læringsanalyse er en del av denne digitaliseringstrenden, og oppsto som eget forskningsfelt i kjølvannet av introduksjon av Massive Open Online Courses (MOOCs), og nye teknikker innen statistikk og maskinlæring for ca. 15 år siden. De mest sentrale forskningsaktørene på læringsanalyse i Europa finner man ved institusjoner som har hovedandelen av sin utdanningsvirksomhet i digitale omgivelser (on-line omgivelser) som f.eks. Open University UK og Nederland.

I flere europeiske land prøver man å jobbe systematisk med dette gjennom UH-sektoren. I Storbritannia har Jisc hatt læringsanalyse på dagsorden i snart 10 år, og har utviklet infrastruktur og prinsipper for læringsanalyse både i forskning, og for utvikling av studiekvalitet, med et særlig fokus på etikk og jus (Schlater, 2016). I Nederland jobber man nå med tilsvarende retningslinjer gjennom SURF konsortiet. Jisc og SURF tilsvarer Sikt (tidl. Unit) i Norge. I Spania har man opprettet forskernettverket SNOLA (Spanish Network Of Learning Analytics) som med finansiering fra spanske myndigheter prøver å skape arenaer der forskning, næringsliv og utdanningsinstitusjoner kan utveksle erfaringer, og gå sammen om

[5] Leading With Predictive Analytics, https://success.gsu.edu/approach/

læringsanalytiske prosjekter. Gjennom samarbeidsprosjekter tilrettelagt av SNOLA har flere spanske universiteter implementert løsninger for læringsanalyse (Muñoz Merino mfl., 2022). I Tyskland prøver man gjennom forskningsprosjekter å utvikle retningslinjer og infrastruktur for læringsanalyse, men ettersom tysk utdanning er desentralisert så preges implementasjonen av enkeltinitiativer blant universiteter og høyskoler (Nouri mfl., 2019).

I Norge ble det i 2015 opprettet et nasjonalt senter for læringsanalyse (SLATE) ved Universitetet i Bergen med støtte fra Kunnskapsdepartementet. SLATE har i liten grad påvirket UH-sektoren her hjemme, men gjør et viktig arbeid i grunnutdanningen der de siden 2017 har samarbeidet med Utdanningsetaten i Oslo i prosjektet «Aktivitetsdata for vurdering og tilpassing» (AVT) om å skape teknisk infrastruktur og juridisk rammeverk for læringsanalyse og kunstig intelligens i grunnskolen. Teknisk har de arbeidet frem spesifikasjoner av hvordan aktivitetsdata kan overføres og lagres, spesifikasjoner av tilgangsstyring og personvern, og et fagkart og en læringsmodell som kan knytte elevens handlingsdata til læringsmål for å identifisere elevens faglige nivå, og kunne gi automatisert tilpasset opplæring. Juridisk har man ikke helt klart å lande rammeverket da datatilsynet og AVT-prosjektet hadde ulike synspunkter på valg av rettslig grunnlag (se videre i del 4 nedenfor), og det var uklart hvilke konsekvenser læringsanalyse og KI har for elevenes personvern.[6] Imidlertid er grunnutdanningen og UH-sektoren ikke underlagt samme juridiske lovverk, men noen av prinsippene ved prosessen kan nok gjenbrukes.

Ved UiO har man i flere år brukt Tableau for å visualisere data fra Felles studentsystem (FS) og datavarehuset STAR for datadrevet beslutningsstøtte. I hvilken grad dette brukes systematisk av enhetene er usikkert. I tillegg vet vi at både Avdeling for studieadministrasjon og USIT ønsker å bruke loggdata fra ulike systemer (f.eks. Canvas, Mine Studier, Leganto m.m.) sammen med data fra FS til læringsanalytiske formål, men har blitt avskåret pga. mangel på lovlig behandlingsgrunnlag.

Teknikker og algoritmer som brukes til læringsanalyse har tradisjonelt hentet inspirasjon fra educational data mining (datagruvedrift) med sine nye metoder innen statistikk, kunstig intelligens og maskinlæring. De mest brukte metodene er deskriptiv statistikk, sannsynlighet (Bayesiansk nettverk, beslutningstrær), klassifisering, gruppering, assosiering, og analyser av tidsserier, og nettverksmodellering. Innen statistikk gjøres analysene manuelt for blant annet oversikter, sannsynlighetsberegning og prediksjoner for beslutningsstøtte. Innen maskinlæring bruker man automatiserte analyser for beslutningsstøtte ved å trene opp algoritmene til å gjenkjenne mønstre; enten gjennom veiledet læring der man trener algoritmen ved å la den analysere deler av et datasett der både inndata og resultat er gitt, før den selv analyserer resten av datasettet, eller gjennom ikke-veiledet læring der man lar algoritmen selv finne optimale mønstre i datasett på egenhånd. Spesielt i sistnevnte tilnærming kan algoritmer og parametere som brukes for modellering være lite tilgjengelig for brukere (såkalt blackboxing), og forståelsen av algoritmer og parametere verifiseres eventuelt utfra hvor godt den predikerer eller beskriver data. Innen forskning brukes mest sannsynlighetsberegninger for prediktiv modellering og anbefalingssystemer, og klassifisering og gruppering innen språkteknologi, nettverksmodellering og diskursanalyser.

Verktøy som brukes er spesialisert utfra forskningsformål som det finnes et utall av. Foruten mer ordinære statistiske verktøy som Excel, SPSS og Stata fins det et utall verktøy som støtter

6 https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/avt-sluttrapport/

kopling av datakilder, vasking av data, og ulike former for analyser. Populære verktøy og plattformer er f.eks. Educational Data Mining Workbench med muligheter for vasking av data, kategorisering, inter-rater reliability, og støtte for statistikk- og tekstanalyse; funksjoner som kan være viktig ved arbeid med ustrukturerte data (data på forskjellige formater). For mer strukturerte data er RapidMiner, KEEL (Knowledge Extraction based on Evolutionary Learning), og Orange som er forskjellige pakker for datamining og analyser, og som gir muligheter til f.eks. å bruke maskinlæringsteknikker uten programmeringskunnskaper. For de mer programmeringskyndige brukes Javascript, R, Python and Jupyter notebook som gir gode muligheter både for front-end programming (for visualiseringer og grensesnitt), og back-end (for f.eks. maskinlæringsalgoritmer) (Gasevic mfl., 2017). Videre forskes det på hvordan resultater fra disse analyseteknikkene og verktøyene kan visualiseres i et grensesnitt som gjør resultatene forståelige og bruksvennlige - både de som retter seg mot forskere, men også praksisfeltet (lærere og studenter) i form av dashboards.

I praksisfeltet (institusjonene i UH-sektoren) bruker man derimot i mindre grad sofistikerte teknikker for analyse og visualiseringer. De fleste institusjoner (slik som UiO) tilbyr enkle visualiseringer av deskriptiv statistikk i etablerte studieadministrative systemer, LMSer (f.eks. Canvas), MOOCs, og enkeltverktøy (Menti, Kahoot, osv.). For eksempel er det vanlig å vise styringsinformasjon (i form av opptakstall, utvikling i karakterer og studiepoeng, emnegjennomføring, m.m.) i Tableau-visualiseringer av FS-data, og individuell studentaktivitet (i form av påloggінger, sidehenvisninger, innleverte oppgaver, m.m.) i Canvas. Men slike systemer er sjelden sammenkoplet på grunn av usikkerhet rundt personvern, og som gjør at man ikke kan gjøre mer sofistikerte analyser.

Imidlertid fins det universiteter som ligger langt fremme og som har hovedandelen av sin utdanningsvirksomhet i digitale omgivelser (on-line omgivelser) slik som Nottingham Trent, Dublin City, Open University UK og Nederland (og spesielt universiteter i Australia og USA). Disse har skapt digitale plattformer og juridiske rammeverk slik at de kan håndtere data som studentene genererer i sine studieforløp. Eksempler på praksis er for eksempel et student-dashbord ved Nottingham Trent, som henter data fra blant annet bibliotek, oppmøte, LMS, m.m. og genererer statistikk for alle studentene for å støtte deltakelse og engasjement, mens Open University UK har utviklet verktøyet 'OUAnalyse' som bruker maskinlæringsteknikker basert på demografiske data og handlingsdata studentene legger igjen i LMS-et for å identifisere trender og predikere frafall.

3.2 Pedagogiske og utdanningsrettede

Målet med læringsanalyse er å forbedre læring og studentvelferd, men i hvilken grad er det dokumentert at det skjer, og under hvilke forhold? Dette er viktige spørsmål for personvernanalyser (se del 4) siden pedagogisk nytte er en del av enhver nødvendighetsvurdering. Dessuten vil svaret på disse spørsmålene kunne gi en indikasjon på i hvilken grad og hvor UiO burde satse på eksperimentering og implementering, samt kompetansebygging blant ansatte og studenter.

Digitalisering av høyere utdanning har påvirket både hvordan forelesere planlegger og gjennomfører undervisning og kommunikasjonen mellom studenter og forelesere. Den raske plattformiseringen av høyere utdanning har også ført til at vi har mer data enn noen gang tidligere om hvordan studentene forholder seg til ressursene som finnes i digitale læringsomgivelser. Det er i dag mulig å bruke slike data, primært fra læringsplattformer som Canvas, både til å vurdere progresjonen til en enkelt student eller en studentgruppe i sanntid, og til å systematisk evaluere og forbedre hele emner i ettertid. Nettopp potensialet til å ta

informerte valg som kan forbedre kvalitetssikring og videreutvikling av gode studietilbud, fremheves som den sentrale fordelen når temaet er digital læringsanalyse.

Mye av forskningen som er gjennomført om digital læringsanalyse har empiriske data fra høyere utdanning. Det er betydelig flere studier fra UH-sektoren enn fra grunnopplæringen. Det finnes flere studier på forbedret engasjement og læringsutbytte hvor man blant annet har vist at studenters bruk av dashboards for å kontrollere egen progresjon kan gi forbedret selvregulering, økt motivasjon, og forbedrer sjansene for å gjennomføre emner og karakterer (Foster & Francis, 2020; Aljohani & Davis, 2013; Rogers & Dolonen, 2022). Flere studier har også vist hvordan man kan predikere frafall (se for eksempel Arnold & Pistilli, 2012; Lauría mfl., 2013; Aiken mfl., 2020), og deretter gjøre tiltak for å forbedre gjennomstrømming og karaktersnittet til studentene. Ved Purdue University i USA klarte de ved hjelp av det prediktive systemet 'Course Signal', og påfølgende tiltak ovenfor studenter i faresonen, å øke rekrutteringen til fagene, heve gjennomsnittskarakterene samtidig som frafallet sank betydelig. Tilsvarende økte gjennomføringsgraden ved University of Nebraska-Lincoln med 3,8% på 4 år, mens Columbus State University College, Georgia, økte med 4,2%. Randomiserte kontrollstudier ved Marist College, New York, og Strayer University, Virginia, støtter opp om resultatene (Ifenthaler mfl., 2019). Mange studier er også gjort på intelligente veiledningssystemer (intelligent tutoring systems) som kan gi automatisert tilbakemelding for å støtte studenters akademiske skriving (Knight mfl., 2020), problemløsning i STEM-fag (science, technology, engineering, math) (Zawacki-Richter mfl., 2019), og analysere hvordan studenter samarbeider og løser komplekse problemer i ulike digitaliserte læringsomgivelser (Oshima mfl., 2020; Gašević mfl., 2019; Echeverria mfl., 2019).

Til tross for flere studier med positive resultater, er det fortsatt vanskelig å påvise tydelige sammenhenger mellom digital læringsanalyse og bedre studentresultater eller studentvelferd (Ferguson & Clow, 2017; Viberg mfl., 2018; Foster & Francis, 2020; Ahern, 2020). Det er flere årsaker til dette, og den viktigste er den vi allerede har antydet i del 2.1: Få av institusjonene i UH-sektoren har erfaring med å systematisk ta i bruk læringsanalyse for å forbedre studentenes utdanningstilbud. I tillegg er det en rekke metodologiske utfordringer innen dette relativt unge forskningsfeltet, som for eksempel at man vet for lite om konteksten for resultatene (hva som skaper virkningen), det er liten geografisk spredning i studiene, få studier har data fra mer enn én institusjon, for få studier forsøker å følge opp bruken av dataene i en læringsanalytisk syklus, og at det er begrenset fokus på forskningsetiske forhold i studiene (Ferguson & Clow, 2017; Foster & Francis, 2020). Videre fremheves det som en ulempe at det er forsket lite på kommersielle leverandører av læringsanalyse, selv om det er disse som i størst grad tas i bruk i UH-sektoren. Vi vil også legge til at mange av studiene om læringsanalyse er forskningsprosjektet der studenter er rekruttert som deltagere, og der hele studietilbudet som blir undersøkt ofte er designet nettopp som input i en vitenskapelig studie. Vi mangler altså data eller systematiske erfaringer fra situasjoner der studenter i en ordinær studentrolle eller forelesere som ikke selv forsker på læringsanalyse, tar i bruk læringsanalyse for å forbedre studentenes undervisning.

Læringsanalyse har per definisjon samme formål som Universitets- og høgskoleloven § 1-6 som skal sikre og videreutvikle kvaliteten i utdanningen, og som også er videre beskrevet i studietilsynsforskriften § 4-1 om at institusjonen systematisk skal innhente informasjon fra relevante kilder for å kunne vurdere kvaliteten i studietilbudene. For det første vil vi fremheve at studenter i dag i liten grad følges opp faglig dersom de ikke aktivt oppsøker oppfølging eller aktivt unngår obligatoriske krav i studieløpet. I mange emner, også ved UiO, er det slik at studentene ikke får noen systematisk vurdering av hvordan emnet går før emnet er sluttvurdert

i form av en eksamen. Riktignok har mengden periodevise emneevalueringer økt, og alle undervisere ved UiO skal ifølge kvalitetsbeskrivelsene bruke emneevalueringer for å ha dialog og tilbakemelding underveis. Utgangspunktet for denne type dialog vil likevel ofte være opplevd kvalitet og opplevd eller antatt læringsutbytte for studenten. Disse dataene er selvsagt viktige for dialogen underveis i et emne, men det kan stilles spørsmål ved om foreleserens muligheter til å justere kurs og tilpasse undervisningen til de studentene en har, er noe begrenset. I en rekke emner vil det fremdeles være slik at det er kun er sluttvurderingen, ofte i form av en individuell eksamen, at foreleser har tilgang på systematiske resultatdata om studentenes læring det aktuelle semesteret. For de aller fleste studentene vil dette være for sent, og det kan derfor tenkes at mer systematisk bruk av læringsanalyse for formativ vurdering kan styrke forelesernes innsyn i hvordan studentene deltar, og forholder seg til det den faglige diskursen som inngår i digitale læringsomgivelser for så å gi tilbakemelding (Rogers & Dolonen, 2022). Systematisk bruk kan også styrke studentenes egen selvregulering ved at de får innblikk i hvordan de ligger an i studiet, og kanskje får automatisert tilbakemelding på hvilke tiltak de kan iverksette for å forbedre progresjonen underveis i emnet (Rahal and Zainuba, 2016; Lu mfl., 2017). Dette potensialet kommer riktignok ikke uten potensielle ulemper: Det kan tenkes at noen studenter kan ha vanskeligheter med å forstå hvordan de skal bruke resultatene for å forbedre måten de studerer eller lærer på, og at økt innsamling og systematisering av data oppleves som uønsket overvåking hvis den ikke gir presis informasjon som oppleves relevant og nyttig i studiene (Velander, 2021).

For det andre vil økt systematisering av handlingsdata underveis kunne styrke data vi allerede har på systemnivå. Per i dag har vi en god del studieadministrative data i FS som blant annet demografiske og geografiske bakgrunnsdata, og aktivitetsdata om hvilket studieprogram og emne enkeltstudenter går på, karakterer, leverte obligatoriske kvalifiseringsoppgaver, og gjennomføringsgrad. Hvis vi kan finne sammenhenger mellom hvilke ressurser emner har og hvordan de er strukturert (forelesninger, gruppearbeid, digitale læringsomgivelser, obligatoriske oppgaver, pensum, m.m.), studentenes bruk av disse ressursene, og resultatdata i FS så kan vi på et tidligere tidspunkt bli oppmerksom på studenter som i liten grad deltar, er faresonen for å falle fra, og eventuelt gjøre tiltak. Dette vil kunne styrke utdanningstilbudet og på sikt føre til økt studentvelferd og økt gjennomføring.

3.3 Etiske

Mandatet retter oppmerksomhet mot de etiske problemstillingene rundt læringsanalyse. Viktige spørsmål er i hvilken grad UiOs policy burde gå lengre enn personvernforordningen og hvilke andre etiske spørsmål UiO burde ta hensyn til.

3.1 Personvern

Når det gjelder personvernforordningen er det tydelig fra del 4 nedenfor at det er en del juridiske begrensninger. Samtidig har arbeidsgruppen diskutert to områder hvor det er ekstra viktig å bli oppmerksom på etiske problemstillinger.

Overvåkning. Det første er at mange studentene allerede i dag kan oppleve at de digitale systemene til UiO er for inngripende. Studentrepresentanter ved UiO forteller at Canvas og automatiske pushvarsler gjør at det blir stadig vanskeligere å skille mellom studietid og fritid. For studentene blir det også stadig vanskeligere å skille mellom hvilke varslinger de bør prioritere. Overkommunikasjon på mange kanaler ble identifisert som en utfordring av studenter på begynnelsen av pandemien (Langford, Damsa, Larsen, Slåttå, Westbye og Wulff (2020: 15-17). Kombinasjonen av dette og den rene mengden fører til at varsler kan deaktiveres i større grad. En kan tenke seg at dersom enda mer av det studentene gjør spores digitalt, vil

det kunne føre til at studenter føler et press til å interagere med de digitale læringsomgivelsene kun med datagenerering og sporing av deres egen aktivitet som hensikt. Kvaliteten til dataene som samles inn påvirkes både av denne «overbruken» og kan potensielt både skape et falskt bilde av bruken, men også skape et høyere press for andre studenter som da ved statistikk ser at de 'henger bak' de andre (Velander 2021). Det faktum at studentene spores kan også føre til en motsatt effekt der studentene aktivt velger å ikke benytte seg av digitale ressurser de ellers hadde hatt nytte av. Dette vil være svært problematisk.

Forskning om hva studenter vil ha fra læringsanalyse er litt sprikende. I en undersøkelse av 394 studenter ved UiB fant Botnevik (2021: 65) at 38% av studentene fant læringsanalyse høyt ønskelig eller ønskelig, mens 25% ga uttrykk for at det var høyt uønskelig eller uønskelig. Det er særlig motstridende bevis om studentene vil vite om for eksempel om hvordan deres innsats er sammenlignet med andre (Jivet, 2021). For enkelte lavtpresterende studenter kan det være motiverende å se hvor høyt presterende studenter plasserer seg, men for andre kan effekten blir motsatt (Pintrich, 2000). Botnevik (2021: 65) fant at 31 % av studentene ikke ønsker denne sammenligning med andre studenter. Jivet mfl., (2021) argumenterer også for at «Students want to be able to decide what information is displayed, how it is arranged and whether they are compared with peers.» (s. 82).

Ønsket om tilstrekkelig medvirkning er også et funn i studien av Velander (2021). På den ene siden er det stor tillit til institusjoner. Selv om et mindretall av spurte studenter vet at høyere utdanningsinstitusjoner samler inn data om dem, og enda færre har satt seg inn i deres retningslinjer for personvern, stoler studentene på institusjonen da rundt 80 % av studentene oppgir at de er «not at all or just a little bit worried» om hvordan institusjonen bruker deres data (Velander, 2021).[7] På den andre siden er fokuset i den andre delen av undersøkelsen rettet mot hvordan disse brukes eller hva slags data som samles inn, og studentene er presentert med resultatene av svært inngående analyser av datasett og lokasjonsdata. Flertallet endret ikke sin mening om det faktum at institusjonen driver med datainnsamling og analyse. Men ved spørsmålet om hva som studentene synes er viktig ble informert samtykke fremhevet, med 61.5% som syntes at det er «very important» (Velander 2021). Følelsen av å bli overvåket blir ikke mindre med innsamlingen av lokasjonsdata. 85.7 % forventer å bli bedt om samtykke til å samle lokasjonsdata, og 66.7 % var ganske bekymret «quite worried» over hvem som hadde tilgang til informasjonen, og 42.9 % om hvordan den ble brukt. Enkelte svar som ble trukket frem handlet om tilliten til at institusjonen ikke selger informasjonen til private aktører og at institusjonen følger gjeldene lovverk om databehandling (Velander 2021). Å opprettholde tillit til hvordan institusjonen behandler data er sentralt for aksept rundt innsamlingen. Velander (2021) noterer at studentene ønsker seg involvering i spørsmål om datainnsamling av denne type i faser av semesteret der de uansett sitter med informasjon og valg av en administrativ sort. Dette er ved semesterregistrering «initial registration» eller ved hver emnepåmelding «as part of every module» (Velander 2021). Dette er også i tråd med tidligere undersøkelser som f.eks. Slade 2019 s. 241.

Sensitive data og områder. Forskning på studenters mening har i begrenset grad tatt opp spørsmål om bruk av sensitive data eller bruk av personopplysninger på sensitive områder. For eksempel kan læringsanalyser som kan predikere utfordringer med psykisk helse bringe store gevinster, men er likevel veldig inngripende personvernmessig. I tilfeller hvor slik bruk etter

[7] 76.9% av de spurte studentene verdsetter hvem som har tilgang til dataene («privacy control») og tillitt («trust») veldig høyt.

en konkret vurdering kan begrunnes i personvernforordningen (se del 4 nedenfor) kan det likevel bli etiske spørsmål om en ren juridisk tilnærming er tilfredsstillende. Man kan spørre om studenter burde få ekstra beskyttelse. Derfor burde det vurderes om studenter burde ha en reservasjonsrett mot bruk av data i visse typer læringsanalyse. Vi tar opp denne diskusjon i del 4.

Tvil om data skal brukes til pedagogiske formål eller forskning. Som vi har påpekt over, er det ikke uvanlig at forskere som selv er opptatt av læringsanalyse utvikler eller implementerer mer læringsanalyse i sine emner enn andre forelesere eller undervisere. Forskning på egen undervisning er kjernen i SOTL (Scholarship of Learning and Teaching) og UiOs egen merriteringordning. All forskning forutsetter frivillig, informert, uttrykkelig og dokumenterbart samtykke fra de som deltar. Dette gjelder selvsagt også for studenter. Vi er klar over at det er fullt mulig å innhente slikt samtykke også for studenter i studier om læringsanalyse. Samtidig vil vi påpeke at en sammenblanding av roller, der de som er ansvarlige for et emne også er eller kan oppfattes å være blant de som skal ha tilgang til data til både pedagogiske formål og forskningsformål, er uheldig og krever økt etisk bevissthet fra utdanningsinstitusjonen. Vi tror at dersom vi vil få en økt bruk av læringsanalyse ved UiO, vil også slike problemstillinger måtte håndteres langt oftere. Det bør være et uttalt mål for UiO at ingen studenter skal oppleve tvil om hva som er formålet med dataene som samles inn om dem. Poenget vårt er at målet med læringsanalyse er å forbedre studenters læring og bidra til økt studentvelferd, ikke å generere data som skal forskes på. Studenter ved UiO skal aldri måtte være i tvil om når de er i en studentrolle og når de eventuelt er deltagere i en studie de har samtykket til.

3.2 Andre etiske problemstillinger

Standardisering. Konstant analyse og tilbakemelding basert på studentenes aktivitet kan også føre til at studentene opplever å måtte studere og tilegne seg kunnskap på en foreskrevet måte (se diskusjon i kap 7. i *Læringsanalyse – noen sentrale dilemmaer*).[8] For eksempel kan rekkefølgen en student velger å tilnærme seg de digitale læringsressursene i eller hvor mange ganger en student velger å gå inn på bestemte ressurser, påvirkes av at studenten ved at hvert klikk generer data om den aktuelle studenten. Et viktig poeng med studentlivet er selv å finne ut av hvordan man tilegner seg kunnskap best, på sin egen måte. Ulikheten som ligger i de diverse studieteknikkene er verdifull og trekker frem det beste av individene. Når læringsanalysen skal anvendes på individuelt nivå risikerer man at den skaper rammer rundt studieteknikk. For studenter å oppleve følelsen av at en studieteknikk eller fremgangsmåte som ikke passer dem blir indirekte påtvunget vil dette kunne påvirke både de akademiske resultatene, men også den generelle studiemotivasjonen.

Individualisering og mindre samarbeid. En annen etisk dimensjon er at dersom mye av dataene som spores knyttes til enkeltindivider, vil det kunne påvirke studentene til å samarbeide mindre enn de gjør i dag eller føre til at færre begynner å samarbeide i fremtiden. Forskning viser at det digitale klasserommet kan innebære sterkere bruk av individuelle arbeidsformer (Blikstad-Balas & Klette, 2020; Gilje m.fl. 2020). Samtidig er det en ny generasjon av læringsanalyse, som måler gruppedynamikk og oppfordre til mer og bedre samarbeid mellom studenter (Fernandez-Nieto m.fl., 2021). Derfor burde UiO se på den overordnete balansen av læringsanalyse som innføres over tid, og at den ikke er for rettet i en individualisert retning.

[8] Ekspertgruppen for digital læringsanalyse (2022).

Det blir like viktig at for statistiske og overordnede analytiske formål at studenter deles inn i brukergrupper som f.eks. er basert på studieprogram eller fakultet. Enkelte studieprogrammer sliter mer med studiemiljø (bl.a. samarbeid) enn andre, og det bør derfor vurderes å ha ulike nivåer av læringsanalyse på de ulike programmene, eventuelt andre tiltak, for å motvirke at individuelle analyser fører til mindre samarbeid blant studentene.

Nøyaktighet. En vanlig bekymring med bruk av både statistikk, regelbasert programmering og maskinlæring er nøyaktighet. I hvilken grad er derfor læringsanalyse presis nok for spesifikke formål, gitt at datasett eller algoritmer kan inneholde feil? Som Schlater (2016) har kommentert: "Predictive analytics are worthless unless the data is accurate and the algorithms are valid", og han understreker at institusjoner må være kompetent nok til å håndtere læringsanalyse som kunne påvirke studenters karrierer og liv. Han anbefaler derfor at:

> It is vital that institutions monitor the quality, robustness and validity of their data and analytics processes in order to develop and maintain confidence in learning analytics and ensure it is used to the benefit of students. Institutions should ensure that: Inaccuracies in the data are understood and minimised; The implications of incomplete datasets are understood; The optimum range of data sources is selected; Spurious correlations are avoided.

4. Personopplysningsvern og rett til privatliv

4.1 Personvern som menneskerettighet

Rett til privatlivets fred (*privacy*) er en viktig menneskerettighet som «dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse».[9] Denne retten er hjemlet i Grl. § 102: «Enhver har rett til respekt for sitt privatliv […]. Statens myndigheter skal sikre et vern om den personlige integritet.» Den er også forankret i Den europeiske menneskerettighetskonvensjonen (EMK) art. 8, jf. menneskerettsloven, § 2 nr. 1. Den europeiske menneskerettighetsdomstolen (EMD) har anerkjent at beskyttelsen av personopplysninger er sentralt for en persons rett til respekt for privatliv.[10] Opplysninger som enten direkte eller indirekte identifiserer et menneske er personopplysninger.[11] Grunnloven og EMK regulerer bare offentlige myndigheter, eller private organer som staten har delegert ansvar til, ikke private leverandører.[12]

Høyesterett har lagt til grunn at et inngrep i retten til privatliv etter Grunnloven § 102 krever en tilstrekkelig hjemmel, at staten forfølger et legitimt formål og at inngrepet er forholdsmessig.[13] Ifølge EMK må inngrep i retten til privatliv «være i samsvar med loven og

[9] Personvernkommisjonen, NOU 2009:1 s. 32.

[10] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137; Z v. *Finland*, 1997, § 95.

[11] jf. GDPR art. 4 nr. 1.

[12] Derfor vil EMD for eksempel bare undersøke om staten har oppfylt sine positive forpliktelser til å forsikre rett til privat liv i lovgivning og regulering når tiltak som griper inn i beskyttelsen av personopplysninger blir truffet av en enkeltperson eller en enhet utelukkende i privat sektor, (*Craxi v. Italia* (nr. 2), 2003, §§ 68-76).

[13] jf. Rt. 2014 side 1105 avsnitt 28 og Rt. 2015 side 93 avsnitt 60.

[må være] nødvendig i et demokratisk samfunn», jf. art. 8(2). Det betyr at det må ha en tilstrekkelig hjemmel i nasjonal lov,[14] forfølge et legitimt mål,[15] møte et pressende sosialt behov og må ikke stå i uforholdsmessig forhold til de legitime målene som forfølges.[16] Krav til nødvendighet her innebærer at læringsanalysen må være «relevant og tilstrekkelig», forholdsmessig og i samsvar med de registrertes berettigede forventninger. For eksempel fant EMD at sensitive medisinske data på et sertifikat beregnet på ulike bruksområder var unødvendig.[17]

4.2 Personvernforordningen

Behandling av personopplysninger er blant annet regulert i detalj i personopplysningsloven og personvernforordningen (EU) 2016/679 (GDPR). Vi skal derfor fokusere mest på personvernforordningen, som også får en sentral plass i vårt mandat.

Personvernforordningen har også vært fokus for mesteparten av juridiske diskusjoner rundt læringsanalyse. Allerede i 2014, i sin høringsuttalelse til MOOC-utvalgets rapport, trakk Datatilsynet frem særlig prediktiv analyse og analyse av sosiale nettverk som problematiske med hensyn til å ivareta studentenes personvern. Når det gjelder prediktiv analyse, understrekte Datatilsynet at: «Det er vanskelig å se for seg hvilke rammer som skal gjelde for denne type læringsanalyse, og hva som er yttergrensen for hvilke opplysninger som kan være nyttige. [...] I tillegg vil det være svært utfordrende å forespeile studenten hva summen av de opplysningene som blir samlet inn vil vise, og hvilket bilde av vedkommende opplysningene samlet vil kunne gi.» Datatilsynet har dessuten også advart mot faren for datadeterminisme. Vedrørende analyse av sosiale nettverk, fremhevet Datatilsynet i sin høringsuttalelse at «det er et betimelig spørsmål om en så omfattende overvåking av studentenes atferd er et forholdsmessig virkemiddel for å oppnå mer samarbeid mellom studenter.» I sin høringsuttalelse i 2014, ga Datatilsynet en klar anbefaling om at det må gjennomføres en vurdering av personvernkonsekvenser (DPIA) av læringsanalyse. Det må her bemerkes at siden 2014, ligger behandling av personopplysninger «for å evaluere læring, mestring og trivsel i [...] alle utdanningsnivåer, fra barne- og ungdomsskole, videregående skoler og høyere utdanning» i Datatilsynets liste over behandlingsaktiviteter som alltid krever en DPIA, jf. GDPR artikkel 35 nr. 4. Dette tilsier at alle former læringsanalyse, herunder adaptiv læringsanalyse, i dag krever at det gjennomføres en DPIA.

Personvernprinsippene i GDPR art. 5 er ryggraden i personvernregelverket:

- Prinsippet om lovlighet, rettferdighet og åpenhet:
    - Det må foreligge et rettslig grunnlag for behandling av personopplysninger, jf. GDPR art. 6, 9 og 10.
    - Behandlingen skal ha respekt for den registrertes (dvs. studenters og læreres) interesser og rimelige forventinger.

[14] *Taylor-Sabori v. the United Kingdom*, 2002, §§ 17-19

[15] *Leander v. Sweden*, 1987, § 49.

[16] *Z v. Finland*, 1997, § 94.

[17] *Frâncu v. Romania*, 2020, §52.

    - Behandlingen skal skje i åpenhet (ikke skjult). Den behandlingsansvarlige må opplyse de registrerte om behandling av vedkommende personopplysninger, med mindre den registrerte allerede har denne informasjon.
- Formålsbegrensningsprinsippet: Personopplysninger skal «samles inn for spesifikke, uttrykkelige angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene».
- Dataminimeringsprinsippet: Personopplysninger skal «være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for». Personopplysninger bør bare behandles dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte.
- Prinsippet om riktighet: Personopplysninger skal «være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes»
- Lagringsbegrensningsprinsippet: Personopplysninger skal «lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for».
- Prinsippet om integritet og konfidensialitet: Personopplysninger skal «behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak».
- Ansvarlighetsprinsippet: Det er den behandlingsansvarlige som er ansvarlig for – og må kunne påvise at – personvernprinsippene overholdes.

4.3 Personopplysninger og anonymisert data

GDPR gjelder ved behandling av personopplysninger. Personopplysning er definert i artikkel 4(1) som:

> enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som *direkte* eller *indirekte* kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,

Anonymiserte data er ikke definert i personvernforordningen, og er betraktet som det motsatte av personopplysninger.[1] GDPR gjelder ikke for anonymiserte data, det vil si opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person eller der personopplysninger har blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres. Det er viktig å peke på at en opplysning som bare «indirekte» kan identifisere en person er regnet som personopplysning. Denne vide definisjonen skaper en stor utfordring for bruk av data for læringsanalyse hvor det er mange variabler eller ustrukturerte data (som tekst, lyd og video). Selv om ingen person er identifiserte «direkte», kan det bli mulig å identifisere personer gjennom en sammenstilling av data (Montjoye, Hidalgo, Verleysen and Blondel, 2013).[2] Nye teknologier kan gjøre det enklere over tid til å bedre identifisere personer, men også beskytte mot forsøk på å identifisere. Unngåelse av indirekte identifisering er i praksis også avhengig av lagrings- sikkerhets- og delingsrutiner til hver organisasjon.

Tolkningen av den relevante rettslige standarden for hva som er identifiserbart er like utfordrende. Etter fortalepunkt 26 GDPR:

> Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen bør det tas hensyn til alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utvikling.

Testen er av rimelig sannsynlighet for identifikasjon enten av den behandlingsansvarlige eller av en annen person som bruker avansert teknologi.[4] Det er en såkalt risikobasert tilnærming. Det kreves ifølge fortalepunkt 26 en vurdering av kostnaden for å gjennomføre identifikasjon, det tiltenkte formålet med behandlingen, risikoen for organisatoriske dysfunksjoner og tekniske feil, mulighetene for teknologisk utvikling i løpet av behandlingens levetid, tekniske og organisatoriske tiltak som er på plass for å hindre identifikasjon og hvor lang tid som kreves for identifikasjon.[5]

Samtidig tok Artikkel 29-gruppen i 2014 en strengere tilnærming. I Working Paper 216 ble det dagjeldende fortalepunkt 26 DPD tolket svært snevert. Artikkel 29-gruppen identifiserte tre risikoer som er avgjørende for anonymisering: utskillelse (muligheten for å isolere noen eller alle oppføringer som identifiserer et individ i datasettet); sammenkobling (muligheten til å koble sammen minst to oppføringer som gjelder samme registrerte); og uttrekking (muligheten til å utlede, med betydelig sannsynlighet, verdien av et attributt fra verdiene til et sett med andre attributter). Artikkel 29-gruppen brukte deretter det som er blitt kalt «en nullrisikotest». De uttalte at «anonymisering er resultatet av behandling av personopplysninger for å ***irreversibelt*** forhindre identifikasjon»[6]. Det betyr at anonymisering kan bli umulig for de fleste datasett, særlig ustrukturerte data, som også kan bety at data i praksis ikke vil være funksjonelle for maskinbehandling og overordnete formål som bedre læring (se diskusjon i Weitzenboeck, Lison, Cyndecka og Langford, 2022).

Hvilken tolkning som er den riktige, er ikke klart. European Data Protection Board (EDPB) refererer til Artikkel 29-gruppens WP 216 i nyere dokumenter, men de har ikke uttrykkelig godkjent den. Dessuten argumenterer akademikere for at den risikobaserte tilnærmingen er en bedre tolkning av fortalepunkt 26 (Esayas 2015; Weitzenboeck, Lison, Cyndecka og Langford, 2022). Det er også pågående diskusjoner i EDPB om den riktige tilnærmingen. Uansett er det viktig i en framtidig ordning på UiO at alle som planlegger bruk av anonymiserte data til læringsanalyse er kjent med at indirekte identifisering kan bety behov for en GDPR-vurdering.

Et annet sentralt poeng i denne sammenheng er at selv om GPDR også vil gjelde for indirekte identifiserbare opplysninger, vil pseudonymisering eller avidentifisering likevel være tiltak som bidrar til å sikre personvernet til de registrerte og kan bidra til at flere krav i GDPR, slik som forholdsmessighet, dataminimering og integritet, lettere er oppfylt.

4.4 Lovligheten

Behandling av studentenes og læreres personopplysninger i forbindelse med utvikling og/eller bruk av læringsanalyseverktøy krever rettslig grunnlag etter personopplysningsloven og GDPR artikkel 6 nr. 1. Behandling av særlige kategorier personopplysninger er i utgangspunktet forbudt med mindre det, i tillegg til et rettslig grunnlag i artikkel 6, kan hjemles i ett av behandlingsgrunnlagene i GDPR artikkel 9 nr. 2. Særlige kategorier personopplysninger er opplysninger om en persons rasemessige eller etniske opprinnelse, politisk oppfatning,

religion, filosofisk overbevisning eller fagforeningsmedlemskap, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, genetiske opplysninger og biometriske opplysninger som er behandlet med det formål å entydig identifisere en fysisk person.

Før det foretas noe læringsanalyse, bør de spesifikke målene med den påtenkte analysen defineres. Dette er viktig for å kunne spesifisere formålet med behandlingen (formålsbegrensningsprinsippet), og for å identifisere hvilke personopplysninger som er nødvendig for behandlingen (dataminimeringsprinsippet).

4.4.1 Behandlingsgrunnlagene

Behandlingsgrunnlag i GDPR artikkel 6 nr. 1 er følgende:

- **Samtykke** (art. 6(1)(a)): Et gyldig samtykke må være frivillig, spesifikt, informert og utvetydig, jf. GDPR art. 4 nr. 11. I vurderingen av om samtykket er frivillig, er styrkeforholdet mellom behandlingsansvarlig virksomhet og den enkelte et sentralt moment. Ved bruk av læringsanalyse ved UiO primært som en utdanningsinstitusjon vil samtykke sjelden være egnet som behandlingsgrunnlag på grunn av ubalanse i maktforhold mellom på den ene siden universitetet og på den andre siden studentene eller ansatte. Dersom en student/ansatt skulle oppleve negative konsekvenser ved å ikke samtykke, slik som dårligere læringsutbytte, vil samtykket heller ikke kunne sies å være avgitt frivillig.[18] Behandling av personopplysninger for vitenskapelige forskningsformål vil kunne hjemles i GDPR art. 6(1)(a), eller art. 6(1)(e), jf. pol. §§ 8 og 9 etter en konkret vurdering. For de tilfeller samtykke vurderes å være riktig behandlingsgrunnlag, må det huskes at den registrerte (student/ansatt) alltid må ha en reell mulighet til å trekke tilbake samtykke sitt.
- **Oppfyllelse av avtale (art. 6 (1)(b)):** Dersom behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, vil dette behandlingsgrunnlaget være aktuelt. Dette er særlig aktuelt ved oppfyllelse av arbeidsavtaler, der en behandling av personopplysninger må gjøres og er en forutsetning for at en ansatt skal kunne jobbe ved universitetet. Det er vanskeligere å se for seg at man kan bruke dette grunnlaget overfor studenter da vi i liten grad inngår avtaler med studentene våre (noen unntak er for eksempel avtale om utveksling etc.). Men vi noterer at den lovpålagte utdanningsplanen (uhl. § 4-2) kan tolkes som en avtale. På UiO har man tradisjonelt ikke pleid å gjøre det, men andre institusjoner gjør det.[19] Dessuten kunne noen former for læringsanalyse være nødvendig for å oppfylle arbeidskontrakten med den ansatte.
- **Rettslig forpliktelse** (art. 6(1)(c)): For å kunne behandle personopplysninger på dette grunnlaget, må den behandlingsansvarlige være forpliktet til å behandle personopplysninger, og formålet skal fremkomme av et supplerende rettsgrunnlag (f.eks. lov- eller forskriftsbestemmelse). Dessuten er det kun de personopplysninger som er nødvendig for å oppfylle dette formålet som kan behandles. Dette tilsier at det ikke er noen reelle alternativer til å oppnå formålet med behandlingen (den rettslige forpliktelsen) uten å behandle personopplysningene. Rettsgrunnlaget er derimot

[18] Se nærmere EDPBs Guidelines 05/2020 on consent under Regulation 2016/679.

[19] Se mer om hvordan UiO bruker utdanningsplanen på https://www.uio.no/studier/registrering/semesterregistrering/utdanningsplan.html

begrenset. Siden bruk av personopplysninger under artikkel 6(1)(c) ikke gir de registrerte noen rett til å protestere mot bruk av personopplysninger har denne bestemmelsen blitt fortolket forsiktig. Artikkel 29-gruppen skrev i 2014 at Artikkel 6(1)(c) kan brukes av offentlige myndigheter hvis det rettslige grunnlaget finnes i lovgivningen og er klar og tydelig.[20] Artikkel 29-gruppen er åpen til bruk av forskrifter, men setter krav om formålet og innhold som må komme frem i lovgivningen.[21] Det reiser derfor spørsmål om relevante rettslige forpliktelser i universitetsloven er klare og tydelige nok, f.eks. å sikre «internt system for kvalitetssikring som skal sikre og videreutvikle kvaliteten i utdanningen?» (Universitets- og høgskoleloven §1-6).

- **Oppgave i allmennhetens interesse** (art. 6(1)(e)): Grunnlaget er relevant hvis universitetet utfører en oppgave i allmennhetens interesse, for eksempel i henhold til lov om universiteter og høyskoler, og den aktuelle læringsanalysen er nødvendig for å oppfylle denne oppgaven. Institusjonen må selv kunne dokumentere at læringsanalyse virkelig er i allmennhetens interesse, og at det ikke finnes et mindre inngripende alternativ som er egnet til å nå formålet. Dessuten holder det ikke at personopplysningene som skal behandles er «interessante» eller «nyttige» – de må være nødvendige for å oppnå formålet. Også dette rettslige grunnlaget krever et supplerende rettslig grunnlag i unionsretten eller i nasjonal rett. Vilkårene som knytter seg til art. 6 nr. 1 bokstav c («rettslig forpliktelse») er formulert mer snevert enn vilkårene som knytter seg til «allmennhetens interesse» i art. 6 nr. 1 bokstav e. Hvis behandling gjøres for ett av grunnene i bokstav e (dvs. for å utføre en oppgave i allmennhetens interesse eller for å utøve offentlig myndighet), trenger ikke formålet fremkomme av det supplerende rettslige grunnlaget. «Det holder at formålet i seg selv er nødvendig for å utføre den aktuelle oppgaven eller utøve den aktuelle myndigheten.» Bokstav e gir altså behandlingsansvarlig rom til å definere formålet selv. Det vil si at kravene til det supplerende rettsgrunnlaget er noe mindre omfattende om behandlingen baseres på «allmennhetens interesse», enn om den baseres på «rettslig forpliktelse».[22]
- **Utøvelse av offentlig myndighet** (art. 6(1)(e)): En beslutning om enkeltvedtak anses å være utøving av offentlig myndighet. Etter norsk forvaltningspraksis, er evalueringer eller tilbakemeldinger av studentens resultater ansett å være en form for utøvelse av offentlig myndighet og krever rettsgrunnlag (legalitetsprinsippet og GDPR art. 6(3)). Institusjonen må selv kunne dokumentere at læringsanalyse virkelig er nødvendig for å oppnå dette formålet, og at det ikke finnes noe alternativ. Dessuten må personopplysningene som skal behandles være nødvendige for å oppnå formålet.
- **Berettigede interesser** (art. 6(1)(f)): Dette behandlingsgrunnlaget gir adgang til å behandle personopplysninger på bakgrunn av en interesseavveining.

[20] "Further, the legal obligation itself must be sufficiently clear as to the processing of personal data it requires. Thus, Article 7(c) applies on the basis of legal provisions referring explicitly to the nature and object of the processing. The controller should not have an undue degree of discretion on how to comply with the legal obligation." Del III.2.3, s. 19.

[21] "The legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level, for instance, either in secondary legislation or by a binding decision of a public authority in a concrete case. This may also lead to legal obligations under Article 7(c) provided that the nature and object of the processing is well defined and subject to an adequate legal basis." Del II.2.3, s. 20.

[22] Se *Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiO og Utdanningsetaten i Oslo kommune*, februar 2022, side 7.

Behandlingsgrunnlaget kan imidlertid ikke brukes ved «behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver». I forarbeidene til personopplysningsloven legges det til grunn at dette unntaket som utgangspunkt kun gjelder ved behandling av personopplysninger i forbindelse med utøvelse av offentlig myndighet.[23] Akkurat når UiO utøver offentlig myndighet kan tidvis være vanskelig å avgrense i forbindelse med læringsanalyse. Om noen former for læringsanalyse kan baseres på dette grunnlaget, må avgjøres etter en konkret vurdering og kun i de tilfeller der det er åpenbart at personverninngripen er lav og universitetets interesse i å behandle personopplysningene veier tyngre enn de registrertes interesser eller grunnleggende rettigheter og friheter. Dersom studentene som det behandles personopplysninger om er under 18 år, veier barns personvern særdeles tyngre, jf. ordlyden i art. 6 nr. 1 bokstav f. UiO har UNG-ordningen som er et tilbud til talentfulle elever som har forsert fag i videregående skole. Det gjelder ikke mange elever, men noen av dem vil være under 18 år.[24] Slik som omtalt i fortalepunkt 38: «Barns personopplysninger fortjener et særlig vern, ettersom barn kan være mindre bevisste på aktuelle risikoer, konsekvenser og garantier samt på de rettigheter de har når det gjelder behandling av personopplysninger.» Når det gjelder studenter kan det også være utfordrende å basere seg på dette behandlingsgrunnlaget all tid man som student har rett til å studere ved UiO og er i en form for avhengighetssituasjon til universitetet.

Om det finnes behandlingsgrunnlag for læringsanalyse etter GDPR art. 6 nr. 1 beror derfor på en konkret vurdering. Det bør blant annet klargjøres hva formålet med den påtenkte læringsanalysen er, hvilke type læringsanalyse som skal gjennomføres, hvilke type personopplysninger som er nødvendig for behandlingen, kilder til personopplysningene som skal behandles, om studenter/lærere kunne forvente at personopplysningene vil brukes for det påtenkte analyseformålet, og om behandling er nødvendig for å oppnå formålet.

4.4.2 Mulige supplerende rettslige grunnlag

Det finnes forskjellige bestemmelser i universitets- og høyskoleloven (uhl.) som vil kunne være aktuelle som supplerende rettslige grunnlag som kreves etter art. 6 nr. 1 bokstav c og e. Noen eksempler er:

- § 1-3 (institusjonens virksomhet) som må leses i lys av § 1-1 (lovens formål),
- §1-6 (kvalitetssikring og videreutvikling av kvaliteten i utdanningen) jf. § 2-1 studiekvalitetsforskriften,
- § 4-15 (innhenting og behandling av personopplysninger i studieadministrative systemer).

I tillegg, kan behandling som er nødvendig for vitenskapelig forskingsformål eller statistikkformål hjemles i pol. § 8 og § 9 og/eller i annen særlovgivning slik som helseforskningsloven.

Det kan være utfordrende å avgjøre hvorvidt en spesifikk behandling kan forankres i de overstående mulige supplerende rettslige grunnlagene. Universitets- og høyskoleloven § 1-6 og studiekvalitetsforskriften § 2-1, knytter seg eksempelvis til utdanningsinstitusjonens

[23] Prop. 56 LS (2017-2018) kap. 6.3.1.

[24] https://www.uio.no/om/samarbeid/skole/emner-vgs/

systematiske arbeid for å sikre og utvikle kvaliteten i egne studietilbud gjennom et system for kvalitetssikring. Man kan se for seg at dette rettslige grunnlaget kan være dekkende for læringsanalyse som har til formål å inngå i et slikt kvalitetssikringssystem. Det kan være vanskeligere å si at bestemmelsene er dekkende for læringsanalyse som har til hensikt å kartlegge en students læring og sette inn relevante tiltak på et tidlig tidspunkt overfor en student. Det var bekymringen til Unit i sitt høringsinnspill i 2019 til *Universitets- og høyskolelovutvalget*:

> Noen vil kunne hevde at bestemmelsen i uhl. § 1-6 om kvalitetssikring kan fungere som supplerende rettsgrunnlag for læringsanalyse. Units vurdering er imidlertid at denne bestemmelsen har sitt hovedfokus på internkontroll, og kan i beste fall brukes til læringsanalyse som omfatter evaluering av undervisning og egne ansatte. Bestemmelsen i uhl. § 1-6 er ikke dekkende for andre former for læringsanalyse som i større grad innebærer kartlegging av studenters aktivitet og læring.[25]

I 2022 kom temaet opp eksplisitt i Sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune.[26] I rapporten uttrykker Datatilsynet en lignende bekymring, men viser større åpenhet til bruk av eksisterende og lignende supplerende rettsgrunnlag i opplæringsloven:

> AVT-prosjektet har primært trukket frem opplæringslova § 13-3e, sammen med § 15-10, som supplerende rettsgrunnlag for behandling av personopplysninger for utviklingsfasen. Opplæringslova § 13-3e regulerer kommunenes plikt til å arbeide med kvalitetsutvikling i skolen. AVT-prosjektet argumenterer for at denne plikten innebærer at læringsanalysen skal være så nøyaktig og effektiv som mulig, noe som gjør det nødvendig å videreutvikle den anvendte algoritmen, herunder behandle elevers personopplysninger til etterlæring.
>
> Temaet har vært lite diskutert i sandkassen, fordi mesteparten av oppmerksomheten har vært rettet mot behandlingsgrunnlag for anvendelsesfasen. Datatilsynet synes det er utfordrende å finne et tydelig supplerende rettsgrunnlag for utviklingsfasen i opplæringslova eller lovens forskrift, men utelukker ikke at grunnlaget AVT-prosjektet har basert behandlingen på kan benyttes. Dette er ikke en unik utfordring for utdanningssektoren, men noe de fleste offentlige virksomheter som ønsker å bidra til utvikling av KI-verktøy risikerer å støte på. Problemstillingen er også berørt i sluttrapporten fra NAV-prosjektet som løp parallelt med dette prosjektet i sandkassen. Kunnskapsdepartementet jobber for tiden med en ny opplæringslov, som vil være klar tidligst i 2023. Innenfor utdanningssektoren har man derfor nå en unik mulighet til å klargjøre skolenes handlingsrom for å bidra i utvikling av KI-verktøy til bruk i undervisningen.

I lys av Grunnloven og EMK vil det kunne stilles strengere krav til det supplerende rettslige grunnlaget avhengig av hvor inngripende en behandling er. Jo mer inngripende, jo strengere krav vil stilles til at det rettslige grunnlaget er tilstrekkelig tydelig og presist og at anvendelsen av det er forutsigbart overfor den enkelte. Det er uansett klart at hvorvidt det finnes et

[25] *Innspill til Universitets- og høyskolelovutvalget,* Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning, s. 20.

[26] Februar 2022. https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/avt-sluttrapport/

supplerende rettslig grunnlag for læringsanalyse må vurderes konkret etter at formål(ene) med det planlagte læringsanalysen er fastsatt.

4.4.3 Særlige kategorier personopplysninger

Behandling av særlige kategorier personopplysninger er i utgangspunktet forbudt, men kan behandles dersom det kan hjemles i ett av unntakene i GDPR art. 9(2). Flere av alternativene i art. 9(2) inneholder vilkår som dels gjelder den aktuelle behandlingen av personopplysninger og dels gjelder krav til supplerende rettsgrunnlag i norsk rett. Læringsanalyse for forskningsformål kan, etter en konkret vurdering, forankres i unntaket knyttet til vitenskapelig forskning (bokstav j) med supplerende rettslig grunnlag i personopplysningsloven §§ 8 og 9.

Mulige aktuelle unntak for læringsanalyse for andre formål kan være uttrykkelig samtykke (bokstav a) - med de utfordringene vist over knyttet til bruk av samtykke i utdanningen – eller at behandlingen er nødvendig av hensyn til viktige allmenne interesser (bokstav g). Dette er imidlertid et unntak som må forankres i et supplerende rettslig grunnlag som må oppfylle flere krav, blant annet skal det stå i rimelig forhold til formålet med behandlingen. Når det gjelder utvikling, valg eller bruk av læringsanalyseverktøy, anbefaler vi en føre-var-tilnærming, det vil si at utgangspunktet skal være at det *ikke* skal utvikles, anvendes, anskaffes eller brukes verktøy som behandler særlige kategorier personopplysninger. Det må bli et veldig godt og dokumentert behov.

4.4.4 Anbefaling

Etter arbeidsgruppens syn bør man ved vurdering av om det foreligger et rettslig grunnlag for læringsanalyse, ta utgangspunkt i GDPR art. 6(1)(e). Avhengig av den konkrete behandlingen og det relevante supplerende rettsgrunnlaget, kan det utredes videre om og hvorvidt art. 6(1)(c) kan utgjøre rettslig grunnlag (istedenfor art. 6(1)(e)), dvs. hvorvidt behandling av personopplysninger gjennom læringsanalyse er nødvendig for å oppfylle en rettslig forpliktelse som påhviler UiO. UiO bør også følge med på den nasjonale ekspertgruppens arbeid og anbefalingene i dette spørsmålet, samt bidra med konkrete forslag til hvordan rettslige forpliktelser bedre kan defineres, slik Datatilsynet har anbefalt.

4.5 Gjenbruk av personopplysninger

Utdanningsinstitusjoner slik som UiO samler inn mange personopplysninger for diverse formål. Dersom institusjonen ønsker å gjenbruke allerede (lovlige) innsamlede personopplysninger til læringsanalyse, må det vurderes om denne viderebehandlingen er forenlig med det opprinnelige formålet. GDPR Artikkel 6 nr. 4 inneholder en liste over sentrale momenter i vurderingen av om en behandling er uforenlig med det opprinnelige formål. Hovedregelen er at personopplysninger ikke kan viderebehandles på en måte som er uforenlig med det opprinnelige formålet, jf. formålsbegrensningsprinsippet, jf. GDPR artikkel 5 nr. 1 bokstav b. Gjenbruk av personopplysninger til arkivformål i allmenhetens interesse, vitenskapelige eller historiske forskningsformål eller til statistiske formål er ikke uforenlig med opprinnelig formål dersom behandlingen er underlagt nødvendige garantier, jf. artikkel 89 nr. 1. Dersom formålet er uforenlig, må gjenbruk enten være lovfestet eller det må innhentes (nytt) samtykke, jf. artikkel 6 nr. 4.

Det er viktig at hver behandlingsaktivitet vurderes konkret og for seg. Bruk/anvendelse av et læringsanalyseverktøy bør, for eksempel, skilles fra selve utviklingsfasen som innebærer blant annet at læringsanalysesystemer bruker studentenes aktivitetsdata til å trene opp algoritmen, slik at den kan bli stadig mer treffsikker i sine prediksjoner. Mye tilsier at disse er to separate

behandlingsaktiviteter som ikke er forenlige med hverandre. Hver av dem vil da kreve separat behandlingsgrunnlag.

4.6 De registrertes rettigheter

4.6.1 Rett til informasjon som forutsetning for utøvelse av de registrertes rettigheter

Før læringsanalysesystemer og -løsninger tas i bruk, er det et krav at både studenter og lærere informeres om systemet og løsningen «på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk», jf. GDPR art. 12(1), jf. åpenhetsprinsippet etter art. 5(1)(a). God og tydelig informasjon, herunder informasjon av hvilke rettigheter den registrerte har, er nødvendig for at vedkommende registrerte – om det er en student eller lærer – vil kunne utøve sine rettigheter, herunder rett til å kreve innsyn i personopplysninger som behandles, rett til å kreve retting av uriktige personopplysninger, eventuelt supplering eller komplettering av ufullstendige personopplysninger, rett til å kreve sletting ('rett til å bli glemt'), og rett til å ikke være gjenstand for en avgjørelse, herunder profilering, som utelukkende er basert på automatisert behandling.

Dersom personopplysninger skal viderebehandles til et annet formål enn det opplysningene ble samlet inn for, er det et krav at den behandlingsansvarlige før nevnte viderebehandling skal gi den registrerte informasjon om nevnte andre formål, og annen relevant informasjon som nevnt i GDPR artikkel 14 nr. 2.

4.6.2 Rett til retting

Et viktig personvernprinsipp er at personopplysninger som behandles er korrekte og, om nødvendig, oppdaterte. Feil og upresise opplysninger i et læringsanalyseverktøy vil kunne få direkte betydning for profileringen av en enkelt student, og vil også kunne påvirke lærerens vurdering av studenten, samt hvilke læringsressurser studenten får anbefalt.[27]

4.6.3 Rett til ikke å være gjenstand for helautomatiserte individuelle avgjørelser

En student har rett til å ikke være gjenstand for en avgjørelse som *utelukkende* er basert på automatisert behandling, herunder profilering, og som har rettsvirkning for eller på tilsvarende måte i betydelig grad kan påvirke vedkommende. Dersom et læringsanalyseverktøy er et fullt ut automatisk beslutningssystem – og ikke bare et beslutningsstøttesystem – kommer GDPR art. 22 til anvendelse, herunder krav til tiltak og garantier etter art. 22(3) og krav til hjemmel etter art. 22(2). Dessuten må det informeres om den underliggende logikken samt de forventede konsekvensene av en slik behandling for den registrerte, jf. art. 13(2)(f) og 14(2)(g). Se videre diskusjon i Ekspertgruppen for digital læringsanalyse (2022: kap. 10.8).

4.6.4 Rett til å protestere

Det bør her huskes at når behandlingsgrunnlag er hjemlet i enten GDPR artikkel 6 nr. 1 bokstav e eller f, både når personopplysninger er behandlet for det opprinnelige formålet og når de viderebehandles, har den registrerte til enhver tid, rett til å protestere mot behandlingen, jf. GDPR artikkel 21 nr. 1. Dersom den registrerte protesterer, skal den behandlingsansvarlige ikke lengre behandle personopplysningene, med mindre vedkommende kan påvise at det foreligger 'tvingende berettigede grunner for behandlingen' som går foran den registrertes

[27] Denne risikoen ble også fremhevet i sluttrapport fra sandkasseprosjektet med KS, SLATE ved UiB og Utdanningsetaten i Oslo kommune: se side 14, https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/avt-sluttrapport/.

interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav, jf. artikkel 21 nr. 1. Dette tilsier at den behandlingsansvarlige bør være forsiktig med tolkningen av hva som faller innenfor sine/tredjepartens 'berettigede interesser' (bokstav f) eller hva som er omfattet av 'allmennhetens interesse' (bokstav e).

4.7 Krav til innebygd personvern

Ved utvikling, anskaffelse eller annen form for valg av læringsanalysesystem og -løsning, skal det sørges at det eventuelle systemet og løsningen som utvikles/velges overholder krav til innebygd personvern og personvern som standardinnstilling (*data protection by design and by default*), jf. GDPR art. 25. Dette betyr at systemet/løsningen som utvikles skal ta hensyn til personvern i alle utviklingsfaser, og at ethvert system eller løsning som skal tas i bruk (f.eks. via lisenser) behandler personopplysninger i samsvar med personvernprinsippene, herunder dataminimering.

Ved offentlig anbud, bør det settes tydelig krav at tilbyderen gjør rede for hvordan systemet/verktøyet oppfyller krav til innebygd personvern og personvern som standardinnstilling, noe som det også oppmuntres til i GDPR fortalepunkt 78.[28]

4.8 Vurdering av personvernkonsekvenser (DPIA)

Etter GDPR art. 35 nr. 1, når det er sannsynlig at en type behandling «vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlig før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet», såkalt «DPIA» (*Data Protection Impact Assessment*). Siden 2019, ligger «[b]ehandling av personopplysninger for å evaluere læring, mestring og trivsel i […] alle utdanningsnivåer, fra barne- og ungdomsskole, videregående skoler og høyere utdanning» i Datatilsynets liste over behandlingsaktiviteter som alltid krever en vurdering av personvernkonsekvenser (DPIA) etter GDPR art. 35.[29] Listen ble godkjent av Det europeiske personvernrådet (EDPB) i 2019, jf. *Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment* (Article 35.4 GDPR).[30]

Dette betyr at alle former læringsanalyse med personopplysninger i dag krever at det gjennomføres en DPIA. Dessuten er en DPIA et viktig verktøy for ansvarlighet. Den hjelper UiO som behandlingsansvarlig med å sikre samsvar med kravene i GDPR, herunder punktene nevnt ovenfor i dette kapittelet. Dessuten hjelper DPIA med å dokumentere at det er gjort tilstrekkelige tiltak for å sikre at GDPR overholdes, ikke minst om hvordan krav om reell medbestemmelse, reel åpenhet, reell forutsigbarhet og tillit er innfridd. Blant de tiltak som bør vurderes er at den registrerte (herunder studenter og lærere) gis mulighet til å reservere seg fra å være gjenstand for analyse via et læringsanalyseverktøy (reservasjonsrett).

[28] GDPR fortalepunkt 78 siste setning lyder: 'Det bør også tas hensyn til prinsippene om innebygd personvern og personvern som standardinnstilling i forbindelse med offentlige anbud.'

[29] Se Datatilsynets liste https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/ (lest 20. mars 2022).

[30] Se https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-22019-draft-list-competent-supervisory_en (lest 20. mars 2022).

SURF har laget en veiledning for utdanningsinstitusjoner i Nederland som beskriver hvordan gå fram dersom det ønskes å utvikle eller ta i bruk et læringsanalyseverktøy. Denne veiledningen kan støtte arbeidet med UiOs endelige rutiner for gjennomføring av DPIA for læringsanalyse. Se videre diskusjon i del 6.

4.9 Behandling og lagring av personopplysninger i tredjeland

Mange relevante digitale verktøy for høyere utdanning er levert av selskaper og institusjoner i land utenfor EU/EØS, særlig USA. Hvis data sendes eller lagres utenfor EU/EØS-land vil behandlingen fortsatt være omfattet av personvernforordningen. Målet med personvernforordningen er å beskytte EU/EØS-innbyggeres personopplysninger, uansett hvor opplysningene behandles. Derfor må overføring bare skje hvis personopplysningsvernet innbyggere har innen EU/EØS opprettholdes (artikler 44-50). I tillegg kom EU-domstolen med «Schrems II-dommen» i 2020, som fastslo at det ikke er tilstrekkelig å basere en slik overføring av personopplysninger på EU-kommisjonens standardbestemmelser. Det er nødvendig å sørge for at det høye beskyttelsesnivået opprettholdes i praksis.

Siden land utenfor EU/EØS kan ha andre regler og praksiser kan disse kravene skape utfordringer. Det betyr at UiO må vurdere om overføringsgrunnlaget faktisk vil ivareta det høye beskyttelsesnivået som personvernforordningen tilsier, ellers kreves andre tiltak. Det kan bli en utfordring som ble nevnt i NIFUs rapport om digitalundervisning under pandemien:

> I fokusgruppeintervjuene var det stor enighet om at den mest sentrale utfordringen for bruk av digital teknologi i norsk UH-sektor i dag er de nye juridiske retningslinjene innført i kjølvannet av den såkalte «Schrems II-dommen» fra 2020. …. Flere av informantene pekte på at de ikke lenger får bruke verktøy de har benyttet seg av tidligere, og at det hindrer institusjonene å ta i bruk ny teknologi i undervisningen ... Dette ble beskrevet som «nesten virksomhetskritisk for det pedagogiske». (Korseberg m.fl. 2022: 105).

Implementering av en konkret vurdering av overføringsgrunnlaget og ekstra tiltak kan bli ressurskrevende. UiO må vurdere i hvilken grad institusjon alene og i samarbeid med andre (f.eks. Sikt, UHR) kan støtte vurderingsprosesser og forhandlinger med leverandører om løsninger som imøtekommer personvernkravene.

5. Medvirkning

5.1 Medvirkning av studenter

I utgangspunktet er studenter blandet i deres mening om at det samles inn data om dem (se kap. 3.3). Det vil være ulike hensyn som må tas for å opparbeide en tillitsfull behandling av dataene for studenter og for forelesere. En klar måte å danne tillit på, eller i det minste ikke svekke den fra start av, er å avklare at studentene ikke kan identifiseres i dataene, eller at bare svært få har tilgang til data (f.eks. lærere). Dette utelukker derimot enkelte og sannsynligvis viktige bruksområder for dataene. Dersom man får løsninger der studenter kan identifiseres eller at flere har tilgang, bør studentene få mulighet til å få innsyn i dataene som samles inn om dem og delta i avgjørelser om bruk av personopplysninger, både individuelt og kollektiv.

Som diskutert i kapittel 4.6 blir studentenes individuelle rett til kontroll over egne data regulert gjennom personopplysningsloven. Dessuten har studenter rett til medvirkning. I uhl. § 4-1 skal

studentorganene «høres i alle saker som angår studentene på det aktuelle nivå». Videre har studenter en eksplisitt rett til å delta i spørsmål som gjelder læringsmiljø, uhl. § 4-3 (1):

> Styret har ansvar for at læringsmiljøet på institusjonen er fullt forsvarlig ut fra en samlet vurdering av hensynet til studentenes helse, sikkerhet og velferd.... Styret skal, i samarbeid med studentsamskipnadene, legge forholdene til rette for et godt studiemiljø og arbeide for å bedre studentvelferden på lærestedet.

Læringsmiljøet er definert som «de forholdene som virker inn på studentenes muligheter til å tilegne seg kunnskap, og som er av betydning for studentenes fysiske og psykososiale helse», og inkluderes «digitale, organisatoriske, pedagogiske og psykososiale forhold», uhl. § 4-3 (2). Forhold som berører læringsmiljøet ved institusjoner blir behandlet i læringsmiljøutvalget, der studentene har like mange representanter som institusjonen. Utvalget har som oppgave å bidra til at kravene til et godt læringsmiljø blir fulgt og at studentene får sikret medvirkning i dette arbeidet, jf. uhl. § 4-3 (3).

Datainnsamling og læringsanalyse kan innebære omfattende og inngripende prosesser som berører studentene direkte. Det er data om studenter og deres bruksmønster som blir analysert, og det er i høy grad snakk om personopplysninger. Læringsanalyse kan brukes for å oppnå flere forskjellige mål på både faglig og sosialt nivå innenfor universitetet. Fellesnevneren er at prosessen og resultatene påvirker studentenes digitale, organisatoriske, pedagogiske og psykososiale forhold. Altså deres læringsmiljø og utdanning. I lys av læringsanalysens brede spekter vil det være nødvendig for studentene på institusjonelt nivå å kunne sikre at analysen foregår trygt og forsvarlig og at universitetet ikke benytter data fra analysen på andre måter enn foreskrevet i formålsbegrensningen eller lov. Dersom analysen(e) viser behov for oppfølging og universitetet er pliktet til dette, må studentene også kunne sikre at plikten overholdes.

Det må derfor spørres om hvilke systemer og vurderinger som ville øke studenters og læreres tillit til bruk av digital læringsanalyse. Etter vår vurdering burde det følgende være en del av UiOs policy:

- For at studenter skal ha tillit til at dataene som samles inn om dem brukes på en forsvarlig måte, er det viktig at de informeres om rettighetene de har i innsamlingen av data, på en tydelig måte som er offentlig kjent. Formålet med innsamlingen av dataene bør klargjøres.
- En reservasjonsrett med «opt-in» og «opt-out» løsninger for bruk av sensitive personopplysninger eller personalopplysninger på sensitive områder kan bidra tillit og en følelse av kontroll over dataene som samles inn.
- Universitetets læringsmiljøutvalg bør få et spesifisert ansvar for å sikre etterlevelsen av universitetets plikter i forbindelse med læringsanalyse. Siden utvalget er et rådgivende organ og dermed ikke kan iverksette tiltak på egenhånd, vil Universitetsstyret ha en spesiell oppfordring til å reagere dersom det fremgår at det forekommer avvik i analyse og håndtering av læringsanalysene pga. aktivitetens særlig sensitive natur.
- De lokale læringsmiljøutvalgene ved fakultetene bør også ha et ansvar for å sikre etterlevelse. På denne måten kan avvik lokalt fanges opp og meldes inn raskt. På lokalt nivå vil de ansatte også ha en bedre mulighet til å komme med innspill dersom de har bekymringer. Det er tross alt ikke bare studentenes data som analyseres, men også de ansattes.

- Behandlingen av dataene til læringsanalyse bør avgrenses til dem som har behov for tilgang ut fra formålene til bruk av personopplysninger. Utvalgte organer, for eksempel gjennom sentralt læringsmiljøutvalg (LMU) og lokale organer ved fakultetene som har ansvar for læringsmiljø (LAMU), bør ha mulighet til å påvirke hvem som får tilgang. Dette sikrer oppfølging og medvirkning for dataene med student- og ansattrepresentanter.
- Resultater, konklusjoner og beslutninger som fattes med bakgrunn i innsamlet datamateriale bør være offentlig tilgjengelige. Dersom det tas beslutninger for individer, må parten få fullt innsyn til beslutningsprosessen og denne må være etterprøvbar.
- De lokale læringsmiljøutvalgene kunne årlig fremstille en rapport om læringsanalyse ved deres fakultet. Det sentrale læringsmiljøutvalget bør lage en samlet oversikt og rapportere årlig til universitetsstyret og alle studentene. Dersom det fremkommer avvik må disse rapporteres så fort det lar seg gjøre, og kommuniseres til studentene.

Disse tiltakene vil både sikre studentenes rett til medvirkning etter uhl. § 4-3 og bidra til å øke studentmassens tillit til universitetets behandling av deres personopplysninger. Medlemmene i de lokale og det sentrale utvalget må ha taushetsplikt for informasjon som kan identifisere enkeltpersoner, når de får innsikt i læringsanalyseverktøy. Rapportene om bruk av læringsanalyse må anonymiseres tilstrekkelig for å sikre at offentliggjøring er mulig.

5.2 Underviseres autonomi og medvirkning

I teorien kan læringsanalyse begrense hvordan en underviser legger opp undervisning eller læringsmiljø. Hvis et verktøy krever tid til innhenting av data, oppleves som et inngrep i studenters personvern eller påvirker det materielle innholdet i faget kan det i enkelte situasjoner begrense underviseres frihet. Bestemmelsen om akademisk frihet i universitetsloven gir vitenskapelige ansatte og andre som gir undervisning «et selvstendig faglig ansvar for innhold og opplegg av denne innenfor de rammer som institusjonen fastsetter eller som følger av lov eller i medhold av lov.» (§1-5 andre ledd). Samtidig har universiteter og høyskoler et overordnet ansvar for kvaliteten av undervisning og systematisk arbeid for kvalitetssikring, som må påvirke rammer til undervisning (§1-6).

I 2020 oppsummerte Aune-utvalget gjeldende rett om spenningen mellom underviseres akademiske frihet og institusjoner ansvar for kvaliteten:

> Den som underviser ved en institusjon under loven, har et selvstendig faglig ansvar for innhold og opplegg i undervisningen innenfor rammene som institusjonen fastsetter. Dette utgjør kjernen i den individuelle akademiske friheten. Undervisningen må imidlertid være egnet til å lede frem til den aktuelle eksamenen eller graden. Studieplanen kan også sette begrensninger for valgfriheten rundt undervisningen. Underviserne har uansett frihet når det gjelder fremstilling av materiale og synspunkter. Fagets kjerneinnhold vil være satt av den faglige ledelsen, men undervisere har et spillerom når det gjelder både fremstilling, perspektiver som fremheves, og det rent kildemessige, så lenge temaene i studieplanen blir ivaretatt. Videre kan undervisningsfriheten begrenses av lov eller

> i medhold av lov, for eksempel av nasjonale rammeplaner gitt av departementet, jf. universitets- og høyskoleloven § 3-3 nr. 2.[31]

Kierulf-utvalget kommenterte nylig også denne spenningen::

> Undervisningsopplegg og utsagn gitt i undervisningssammenheng kan gripe inn i den akademiske ytringsfriheten. Friheten kan for eksempel oppleves redusert innenfor relativt rigide opplegg for rammeplanstyrte utdanninger. Ledere kan måtte gripe inn i situasjoner hvor en undervisers opplegg stadig får negative studentevalueringer, sviktende oppslutning og dårlige resultater målt gjennom eksamensvurderinger. Alle forholdene som knyttes til studentrelasjoner og undervisningopplegg vil også være tjent med forutsigbarhet skapt gjennom en diskusjon av hvordan man som miljø skal etablere endringer for å fremme kvalitet.[32]

Ser man disse to kommentarene sammen, viser de at læringsanalyse som særlig påvirker materielt innhold (f.eks. som er innebygd i adaptiv læring) kan reise spørsmål om akademisk frihet, men for annen bruk er det mye mer uklar om det et rent rettslig spørsmål om akademisk frihet.

Samtidig er det i Norge lang tradisjon for at fagmiljøene og den enkelte underviser selv for det meste avgjør hva slags informasjon en trenger å samle inn om studentene underveis i et semester og ved en sluttvurdering i et aktuelt emne. Utover bruk av læringsplattform og periodevise emneevalueringer, der forelesere fremdeles har stor definisjonsmakt, pålegger UiO sjelden enkeltforelesere bestemte måter å arbeide på. Dette innebærer at et sentralt ønske om økt bruk av læringsanalyse kan oppfattes som en innskrenkning av undervisers autonomi, et «rigide opplegg for rammeplanstyrte utdanninger» til å bruke uttrykket fra Kierulf-utvalget. Samtidig vil det være uheldig både dersom det samles inn en rekke data som aldri blir benyttet til læring, og dersom ulike emner i svært ulik grad følger opp dataene som hentes inn.

Kierulf-utvalgets anmodning om medvirkning, nemlig «forutsigbarhet skapt gjennom en diskusjon av hvordan man som miljø skal etablere endringer for å fremme kvalitet», kan derfor være et godt utgangspunkt for et prinsipp i UiOs policy om bruk av læringsanalyse. Dessuten burde det også være et klart prinsipp at undervisere skal få særlig medvirkning i læringsanalyse som kan påvirke "fremstilling av materiale og synspunkter".

For foreleseres tillit er det dessuten viktig at statistikken læringsanalyse gir ikke muliggjør uthenging eller skaper et rotterace mellom forelesere der man måler hverandre (og måles av andre) basert på klikk og engasjement fra studenter på Canvas eller andre plattformer. Dette kan for eksempel løses ved at det er begrenset hvem som har tilgang på statistikken fra forelesningsopptak og dataene tilknyttet disse, og at det settes noen kriterier eller avgrensninger til hva data tilknyttet foreleseres digitale engasjering av studenter kan brukes til og føre til av eventuelle endringer. Eventuelle endringer bør ikke føles som sanksjoner. Allikevel må universitetet effektivt kunne følge opp analysene og gjøre endringer, spesielt der det påvirker undervisningskvaliteten.

[31] NOU 2020: 3 Ny lov om universiteter og høyskoler, kap 15.2.

32 Akademisk ytringsfrihet 2022: 2, kap 7.4.2.

6. Institusjonalisering – veiledning, godkjenning og kompetanseheving

I hvilken grad burde UiO legge opp til et system for kvalitetssikring av digital læringsanalyse, særlig i forhold til juridiske krav, etiske hensyn og tilstrekkelig medvirkning av studenter og ansatte? I denne delen redegjør vi for praksis i andre land, eksisterende systemer på UiO og mulige modeller for institusjonalisering. Vi avrunder med en kort diskusjon om kompetanseheving av ansatte, som kan bli nødvendig for denne kvalitetssikringen i tillegg til god pedagogisk bruk av læringsanalyse.

6.1 Praksis på andre universiteter og land

6.1.1 JISC - Storbritannia

JISC har utviklet en *Code of practice for learning analytics* som beskriver utdanningsinstitusjonenes ansvar for å sikre at læringsanalyse gjennomføres på en ansvarlig, hensiktsmessig og effektiv måte (vedlegg 1 inneholder en oversettelse av disse retningslinjer av CELL). Retningslinjene tar opp noe viktige juridiske, etiske og logistiske problemstillingene som sannsynligvis oppstår ved bruk av læringsanalyse. Retningslinjene understreker at full transparens og klare retningslinjer hos utdanningsinstitusjonene er avgjørende med hensyn til formålet med læringsanalyse, dataene som samles inn, prosessene som inngår, og hvordan de brukes til å forbedre læringsutbyttet.

6.1.2 SURF - Nederland

SURF har utviklet en ganske detaljert veileder i fem trinn for utdanningsinstitusjoner som vurdere å bruke læringsanalyse: *Learning Analytics in 5 Steps: A Guide to the GDPR* (se oversettelse i vedlegg 2, oversatt av CELL). Dokumentet understreker at veilederen er ment som støttedokument til utdanningsinstitusjoner, og at hver enkelt institusjon må foreta sine egne konkrete vurderinger før de setter i gang et prosjekt eller en aktivitet som innebærer bruk av læringsanalyse.

De fem trinnene som er beskrevet i detalj i veilederen inneholder de følgende punktene:

Trinn 1: Forberedelse

- Definere de spesifikke målene dere ønsker å nå med læringsanalysen
- Etablere en tverrfaglig prosjektgruppe
- Beskrive interessenter

Trinn 2: Utforming

- Inkludere personvern i utformingen
- Definere omfanget av behandlingen
- Beskrive hvordan personopplysninger vil bli behandlet
- Beskrive (sikkerhets-)tiltakene
- Definere interessenters personvernroller

Trinn 3: Vurdering

- Lovligheten av læringsanalyseprosessen
- Vurdering av personvernkonsekvenser (DPIA) for læringsanalyse

- Hvordan gjennomføres en DPIA?
- Definere konsekvensene av læringsanalyse (risikovurdering)
- Definere tiltak som reduserer risiko
- Resultater av DPIA

Trinn 4: Implementering

- Fullføre de nødvendige kontraktene
- Utarbeid de nødvendige dokumentene med retningslinjer og prosedyrer
- Informere enkeltpersoner om behandling av personopplysninger ved læringsanalyse
- Sikkerhet og risikoreduserende tiltak
- Andre tiltak
- Pilot

Trinn 5: Evaluering

- Evaluer med jevne mellomrom
- Publiser erfaringer

6.2 Eksisterende praksis på UiO

6.2.1 Rutiner og malverk

UiO har flere etablerte rutiner og malverk for å påse at personvern og informasjonssikkerhet ivaretas ved datahåndtering. Under trekker vi frem de som kan være mest relevante ved aktiviteter knyttet til læringsanalyse:

- Lagringsguiden angir i hvilke tjenester man kan behandle ulik informasjon ved UiO.
- Lagringsguiden må ses i sammenheng med Klassifiseringsguiden som angir de forskjellige klassifiseringene av informasjon ved UiO. Informasjon deles inn i grønn, gul, rød eller svart avhengig av hvor beskyttelsesverdige dataene er.
- Mal for DPIA
- Sjekkliste for systemeiere
- Rutine ved avvik ved behandling av personopplysninger

6.2.2 Skytjenester

IT-tjenester som brukes ved UiO skal ivareta nødvendige krav til personvern og informasjonssikkerhet. Dersom et miljø ved universitetet ønsker å ta i bruk en skytjeneste som ikke fremgår av UiOs tjenestekatalog eller enhetenes IT-tjenester i forbindelse med læringsanalyse, skal tjenesten vurderes og godkjennes i henhold til gjeldende regelverk. Det må i mange tilfeller være inngått databehandleravtale (GDPR art. 28), informasjonssikkerheten i tjenesten må vurderes (jf. særlig GDPR art. 32) og eventuelle overføringer av personopplysninger ut av EØS må vurderes i lys av kravene i Schrems II-dommen omtalt ovenfor i kap. 4.9. Hvis aktuelt må også betalingsordning og forholdet til anskaffelsesregelverket vurderes.

UiO har en veileder for hvordan man går frem ved ønske om en ny skytjeneste, samt en sjekkliste for prosessen.

6.2.3 Meldeappen

Som behandlingsansvarlig har UiO plikt til å føre protokoll over de behandlingsaktivitetene som utføres ved universitetet, jf. GDPR art. 30. Meldeappen er UiOs oversikt over administrative behandlinger av personopplysninger. Her skal administrative behandlinger som har en vedvarende karakter, er gjentagende eller gjøres som en rutine eller etter en retningslinje, registreres. Hvis UiO igangsetter en ny behandling av personopplysninger i forbindelse med læringsanalyse, må denne registreres her for å oppfylle protokollkravet.

6.2.4 Personvernvurdering i forskningsprosjekter

Sikt (tidligere NSD) er UiOs tjenesteleverandør av personvernvurderinger innen forskning. Ved UiO er rutinen at alle student- og forskningsprosjekter som behandler personopplysninger skal meldes til Sikt for å få en vurdering av personvernet.[33] I tilfeller det er påkrevd å gjøre en DPIA, vil Sikt bistå prosjektet med dette før den godkjennes ved UiO. Sikt fører også protokollen i henhold til art. 30 på vegne av UiO i forskningsprosjekter. Dette innebærer at forskning ved UiO som knytter seg til læringsanalyse skal meldes til Sikt såfremt prosjektet behandler personopplysninger.

6.3 Mulige modeller for institusjonalisering

Dagens overnevnte rutiner dekker mange elementer av bruk av læringsanalyse på UiO, særlig når det gjelder hvilke tjenester man kan bruke til å behandle, lagre, og bearbeide informasjon og innkjøp av nye digitale skytjenester, samt forskning med læringsanalyse. Ut fra analyse i resten av rapporten og diskusjoner i arbeidsgruppen er det noen utfordringer i dagens system:

- Manglende veiledning til systemeiere og USIT om når læringsanalyse kan begrunnes i artikkel 6 personvernsordningen, som ofte leder til at læringsanalyse ikke tas i bruk.
- Sterk desentralisering av søknadsprosessen til systemeiere for tilgang til data for bruk i læringsanalyse som faller utenfor prosesser for innkjøp av skytjenester. Det gjør systemeiere usikker på om kravene i personvernordningen er oppfylt.
- Manglende system for direkte involvering av studenter og ansatte for avgjørelser om bruk av personopplysninger i læringsanalyse, særlig kommunisering om bruk av data og involveringen av læringsmiljøutvalgene.
- Manglende oversikt av i hvilken grad studenters og læreres data er brukt i eksisterende læringsanalyse på UiO.
- Manglende støtte til ansatte som vil bruke verktøy som krever overføringer av personopplysninger ut av EØS, særlig gitt kravene i Shrems II-dommen

Arbeidsgruppen har vurdert tre forskjellige modeller:

1. *Hybrid*. UiO fortsetter med dagens modell med blanding av sentraliserte og desentraliserte prosesser, men med ekstra veiledning og støtte.
    - Læringsanalyser som er innebygd i *nye* digitale tjenester som skal kjøpes inn, vurderes sentralt av USIT etter eksisterende rutiner.
    - Læringsanalyser som involverer behandling av personopplysninger i verktøy utviklet av UiO-ansatte eller i samarbeid med tredje partner (inkludert leverandører av eksisterende skytjenester) er vurdert fortsatt av individuelle systemeiere.

[33] https://www.uio.no/for-ansatte/arbeidsstotte/personvern/rutine-for-forskning-med-personopplysninger.html.

- Ekstra veiledning gis til alle relevante aktører (f.eks. systemeiere, USIT, læringsmiljøutvalg) om både vurderingsgrunn og medvirkningsbehov.
- Bedre støtte er gitt til ansatte som vil bruke verktøy som krever overføringer av personopplysninger ut av EØS.

2. *Sentralisert*. UiO skaper en ny intern rutine for bruk av personopplysninger til kvalitetsarbeid.
    - Rutinen kunne ta utgangspunkt i systemet for nye digitale skytjenester, men legge opp til en adskilt veilednings- og søknadsprosess, og bedre medvirkning av studenter og ansatte
    - Det kunne også legges opp til at den nye rutinen brukes aktiv når nye digitale skytjenester inneholder muligheten for bruk av læringsanalyse (som tidligere med Canvas, og nylig med Watermark for UiOs nye evalueringssystem).
    - Bedre støtte til ansatte som vil bruke verktøy som kreves overføringer av personopplysninger ut av EØS.

3. *Delegert*. UiO delegerer vurdering av personopplysninger til kvalitetsarbeid til en ekstern aktør som Sikt.
    - Rutinen kunne ta utgangspunkt i NSDs system for forskning, men legge opp til en adskilt søknadsprosess. Det vil bety at den eksterne aktøren har ansvar for ev. DPIA.
    - Den eksterne aktøren kan bli bedt om å gi bedre støtte til ansatte som vil bruke verktøy som kreves overføringer av personopplysninger ut av EØS. F.eks. forhandlet Sikt (tidligere gjennom UNINETT) med Zoom i 2019 om en løsning.

6.4 Kompetanseheving på UiO om læringsanalyse

Dersom vi mener at læringsanalyse er et viktig element for å kvalitetssikre og videreutvikle kvalitet i utdanningen ved UiO, er det viktig at det finnes tilstrekkelig kompetanse om hva læringsanalyse er og hvordan det kan brukes på ulike nivåer i organisasjonen. Dersom en virkelig skal utnytte læringsanalyse vil dette innebære at dataene brukes a) på systemnivå for eksempel for å videreutvikle ulike studieporteføljer og se sammenheng mellom ulike fag og fagkombinasjoner, b) på emnenivå, for eksempel for å kunne vurdere endringer i emnet over tid og se hvordan ulike endringer i emnet påvirker studentdeltagelse eller studentresultater, og ikke minst c) på individnivå, for eksempel for at en foreleser skal kunne få mer informasjon underveis i emnet om studentenes deltagelse og resultater. Det vil være behov for såkalt "data literacy", forstått som evnen til å lese, tolke, analysere og bruke data i relevante kontekster, på både faglig og administrativt nivå (Wolff m.fl., 2016; Hachmeister, m.fl. 2021).

Per i dag er det ingen krav om at alle ansatte ved UiO skal ha kompetanse om læringsanalyse, eller være villige til å benytte digitale spor fra studentens aktiviteter i digitale læringsomgivelser til å forbedre undervisningen sin eller følge opp studenter som trenger det. Det obligatoriske kurset i universitetspedagogikk, etter hva vi kan se i hvert fall, inneholder per i dag heller ingen systematisk gjennomgang av potensiale for læringsanalyse i høyere utdanning generelt eller ved UiO spesifikt. Vi kan anta at svært få av UiOs undervisere har et aktivt forhold til læringsanalyse.

Dersom UiO ønsker økt bruk av læringsanalyse, forutsetter dette en målrettet kompetanseheving både på fakultet og instituttnivå, slik at dataene kan brukes til å forbedre emner over tid og evaluere på emnenivå. Det forutsetter også kompetanseheving på individnivå, slik at enkeltforelesere er i stand til å for eksempel lese et såkalt "dashboard" eller tolke ulike studentdata som kan gi verdifull innsikt i studentenes læring. All bruk av læringsanalyse forutsetter at dataene som samles inn brukes godt i en pedagogisk sammenheng. Dataene tolker ikke seg selv, og forutsetter tilstrekkelig analytisk kompetanse eller "data literacy" for å være nyttige. Dersom konkrete kompetansetiltak ikke kommer på plass, er det grunn til å tro at bruken av læringsanalyse vil bli begrenset til miljøene der en allerede har en sterk interesse for dette feltet, noe som vil kunne gi ulik kvalitet i undervisningstilbudet til UiO og ujevnt kvalitetsarbeid.

7. Konklusjoner og anbefalinger

Læringsanalyse har stort potensielle på UiO til å forstå og forbedre læringsprosessen og det sosiale miljøet der læring foregår. Samtidig har lite skjedd på UiO og i Norge sammenlignet med andre land. UiO har en lovlig plikt og uttalt ambisjon om å systematisk utvikle arbeidet med kvalitet i utdanningene, men det må være kunnskapsbasert, forankret i empiri, data og analyser, og i tråd med etikk og rettslige krav. Denne rapporten viser hvordan man kan balansere disse forskjellige behovene, særlig når det gjelder pedagogisk nytte og personvern, samtidig viser vi behov for en bedre institusjonalisering av godkjenningsprosesser, støtte til ansatte når personopplysninger skal overføres til land utenfor EU/EØS og kompetansebygging av ansatte om god og etisk bruk av læringsanalyse. Vi håper prinsippene vi har skissert og foreslått skaper grunnlaget for en overordnet og gjennomførbar policy knyttet til læringsanalyse.

Referanser

Ahern, S.J. (2020). Making a #Stepchange? Investigating the Alignment of Learning Analytics and Student Wellbeing in United Kingdom Higher Education Institutions. *Front. Educ.* 5:531424. doi: 10.3389/feduc.2020.531424

Aljohani, N. R., and H. C. Davis (2013). *Learning Analytics and Formative Assessment to Provide Immediate Detailed Feedback Using a Student Centered Mobile Dashboard*. Paper presented at the Seventh International Conference on Next Generation Mobile Apps, Services and Technologies.

Arnold, K. E., & Pistilli, M. D. (2012, April). Course signals at Purdue: Using learning analytics to increase student success. In *Proceedings of the 2nd international conference on learning analytics and knowledge*, 267-270.

Blikstad-Balas, Marte & Klette, Kirsti (2020). Still a long way to go Narrow and transmissive use of technology in the classroom. *Nordic Journal of Digital Literacy.* 15(1): 55–68. doi: 10.18261/issn.1891-943x-2020-01-05.

Botnevik, S. (2021). *Student Perceptions of Privacy in Learning Analytics: A Quantitative Study of Norwegian Students.* Master's thesis, Information Science, Department of Information Science and Media Studies, University of Bergen.

Dahl, M. (red., 2015). *Læringsanalyse.* Senter for IKT i utdanningen. URL: https://www.udir.no/globalassets/filer/laeringsanalyse.pdf

Samson Yoseph Esayas (2015). The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the "all or nothing" Approach. *European Journal of Law and Technology,* 6(2): 1-28.

Ferguson, R. and Clow, D. (2017). Where is the evidence? A call to action for learning analytics. In: LAK '17 Proceedings of the Seventh International Learning Analytics & Knowledge Conference, ACM International Conference Proceeding Series, ACM, New York, USA, pp. 56–65. DOI: https://doi.org/10.1145/3027385.3027396

Fernandez-Nieto, G., Martinez-Maldonado, R., Echeverria, V., Kitto, K., An, P., & Buckingham Shum, S. (2021). What Can Analytics for Teamwork Proxemics Reveal About Positioning Dynamics In Clinical Simulations? *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1): 1-24.

Foster, F. & Francis, P. (2020). A systematic review on the deployment and effectiveness of data analytics in higher education to improve student outcomes. *Assessment & Evaluation in Higher Education*, 45:6, 822-841, doi: 10.1080/02602938.2019.1696945

Dolonen, J. & Ludvigsen, S. (2021). *Notat om læringsanalyse ved UiO: Et mulig program?* Internt notat, UiO.

Echeverria, V., Martinez-Maldonado, R., & Buckingham Shum, S. (2019). *Towards Collaboration Translucence: Giving Meaning to Multimodal Group Data. In Proceedings of ACM CHI conference* (CHI'19) | https://doi.org/10.1145/3290605.3300269

Gašević, D., Joksimović, S., Eagan, B.R., & Shaffer, D.W. (2019). SENS: Network analytics to combine social and cognitive perspectives of collaborative learning. *Computers in Human Behavior*, 92 (PG-562–577): 562-577, 10.1016/j.chb.2018.07.003

Hachmeister, N., K. Weiß, J. Theiß & R. Decker (2021). Balancing Plurality and Educational Essence: Higher Education Between Data-Competent Professionals and Data Self-Empowered Citizens. *Data* 2021: 6, 10. https://doi.org/10.3390/data6020010

Ifenthaler, D., DK. Mah, J. Yau & J. Yau (2019). Utilising Learning Analytics for Study Success: Reflections on Current Empirical Findings. In: D. Ifenthaler, DK. Mah, J. Yau, (red.) *Utilizing Learning Analytics to Support Study Success*. Springer, Cham. https://doi.org/10.1007/978-3-319-64792-0_2

Jivet, I., Wong, J., Scheffel, M., Valle Torre, M., Specht, M., & Drachsler, H. (2021). *Quantum of Choice: How learners' feedback monitoring decisions, goals and self-regulated learning skills are related*. In Proceedings of LAK21: 11th International Learning Analytics and Knowledge Conference, Irvine, CA, USA. *Best Full Paper Award*

Kaliisa, R., & Dolonen, J.A. (2020). *CADA: a teacher-facing learning analytics dashboard to foster teachers' awareness of students' participation and discourse patterns in online discussions.* Tech Know Learn. https://doi.org/10.1007/s10758-022-09598-7

Langford, M, C. Damsa, J. Larsen, K. Slåttå, H. Westbye og S. Wulff. (2020). *Første uken med digital undervisning I koronatiden: Jusstudenters erfaring*. Centre for Experiential Legal Learning (CELL), Universitet i Oslo, Report No. 1/2020.

Lauría, E. J., Moody, E. W., Jayaprakash, S. M., Jonnalagadda, N., & Baron, J. D. (2013, April). Open academic analytics initiative: initial research findings. In *Proceedings of the Third International Conference on Learning Analytics and Knowledge*: 150-154.

Lu, O. H., J. C. Huang, A. Y. Huang, and S. J. Yang. 2017. "Applying Learning Analytics for Improving Students Engagement and Learning Outcomes in an Moocs Enabled Collaborative Programming Course." Interactive Learning Environments 25 (2): 220–234. doi:10.1080/10494820.2016.1278391

Muñoz-Merino, P.J., Moreno-Marcos, P.M., Rubio-Fernández, A., Tsai, Y., Gašević, D. & Delgado Kloos, C. (2022). A systematic analysis of learning analytics using multi-source data in the context of Spain, *Behaviour & Information Technology*, doi: 10.1080/0144929X.2022.2039767

Nouri, J., Ebner, M., Ifenthaler, D., Saqr, M., Malmberg, J., Khalil, M., Bruun, J., Viberg, O., Conde González, M. Ángel, Papamitsiou, Z., & Berthelsen, U. D. (2019). Efforts in Europe for Data-Driven Improvement of Education – A Review of Learning Analytics Research in Seven Countries. *International Journal of Learning Analytics and Artificial Intelligence for Education (iJAI)*, 1(1): 8–27. https://doi.org/10.3991/ijai.v1i1.11053

Oshima, J., Oshima, R. and Saruwatari, S. (2020). Analysis of students' ideas and conceptual artifacts in knowledge-building discourse. *Br J Educ Technol*, 51: 1308-1321. https://doi.org/10.1111/bjet.12961

Rahal, A., and M. Zainuba (2016). Improving Students' Performance in Quantitative Courses: The Case of Academic Motivation and Predictive Analysis. *The International Journal of Management Education* 14(1): 8–17 https://doi.org/10.1016/j.ijme.2015.11.003

Schlater, N. (2016). Developing a code of practice for learning analytics. *Journal of Learning Analytics*, 3(1), 16–42.

Tsai, Y.-S., Rates, D., Moreno-Marcos, P.M., Muñoz-Merino, P.J., Jivet, I., Scheffel, M., Gašević, D. (2020). Learning analytics in European higher education—Trends and barriers. *Computers & Education*, 155 , s.103933, 10.1016/j.compedu.2020.103933

Velander, J., Otero, N., Pargman, T. C., & Milrad, M. (2021). We Know What You Were Doing. In *Visualizations and Dashboards for Learning Analytics*. Springer, Cham: 323-347.

Viberg, O., Hatakka, M., Bälter, O., & Mavroudi, A. (2018). The current landscape of learning analytics in higher education. *Computers in Human Behavior*, 89: 98–110. https://doi.org/10.1016/j.chb.2018.07.027

Weitzenboeck, Emily, Pierre Lison, Malgorzata Cyndecka and Malcolm Langford (2022), ''The GDPR and unstructured data: is anonymization possible?', *International Data Privacy Law,* ipac008: https://doi.org/10.1093/idpl/ipac008

Wolff, A., Gooch, D., Montaner, J.J., Rashid, U., & Kortuem, G. (2016). Creating an Understanding of Data Literacy for a Data-driven Society. J. Community Informatics, 12.

Vedlegg 1: JISCs Retningslinjer for læringsanalyse

Oversettelse av CELL.

Beskrivelse av utdanningsinstitusjonenes ansvar for å sikre at læringsanalyse gjennomføres på en ansvarlig, hensiktsmessig og effektiv måte.

Innledning

Læringsanalyse bruker data om studenter og deres aktiviteter til å hjelpe institusjonene med å forstå og forbedre læringsprosessene og gi elever og studenter bedre støtte.

Læringsanalyse bør brukes til studentenes beste. Dette kan skje ved å bistå dem enkeltvis, eller ved å bruke aggregerte og anonymiserte data til å hjelpe andre studenter. Læringsanalyse kan også brukes til å forbedre læringsutbyttet mer generelt. Den skiller seg fra vurdering, og bør brukes til formative snarere enn summative formål.

Effektiv bruk av læringsanalyse vil i utgangspunktet innebære innføring av nye systemer sammen med endringer i institusjonens retningslinjer og prosesser. Det kan samles inn nye data om enkeltpersoner og deres læringsaktiviteter. Dataene vil bli analysert, og det kan iverksettes tiltak som følge av dette. Dette gir muligheter for positiv involvering og innvirkning på læring, men også for misforståelser, misbruk av data og negative konsekvenser for studentene.

Full transparens og klare retningslinjer hos institusjonen er derfor avgjørende med hensyn til formålet med læringsanalyse, dataene som samles inn, prosessene som inngår, og hvordan de brukes til å forbedre læringsutbyttet.

Disse retningslinjene tar sikte på å beskrive utdanningsinstitusjonenes ansvar for å sikre at læringsanalyse gjennomføres på en ansvarlig, hensiktsmessig og effektiv måte, og tar opp de viktigste juridiske, etiske og logistiske problemene som sannsynligvis vil oppstå.

Utdanningsinstitusjoner i Storbritannia har allerede innført retningslinjer og prosedyrer for informasjonsstyring og har lang erfaring i å håndtere sensitive opplysninger og personopplysninger i samsvar med den britiske personvernloven, Data Protection Act 1998. Nå må de også overholde EUs personvernforordning (GDPR).

Når institusjonene overfører og tilpasser denne kompetansen for å regulere behandlingen av data for læringsanalyse, bør de fastsette de retningslinjene og prosedyrene som er nødvendige for å kunne behandle dataene til enkeltpersoner på lovlig og rettferdig måte.

Ansvar

Institusjonene må bestemme hvem som har det overordnede ansvaret for effektiv bruk av læringsanalyse i samsvar med rettslige og etiske krav. De bør tildele spesifikke ansvarsområder i institusjonen for

- innsamling av data som skal brukes til læringsanalyse,
- anonymisering av dataene der det er hensiktsmessig,
- analyseprosessene som skal utføres på dataene, og hvilke formål de har,
- tiltakene som skal gjennomføres,

- oppbevaring og forvaltning av data som brukes til og genereres ved læringsanalyse.

Studentrepresentanter og sentrale ansattgrupper ved institusjonene bør tas med på råd når det gjelder målsetninger for og utforming, utvikling, utrulling og overvåking av læringsanalyse.

Transparens og samtykke

Institusjonene vil definere målene for bruk av læringsanalyse, hvilke data som er nødvendige for å nå disse målene, og hva som ligger utenfor rammene. Datakildene, analysens formål, hvilke parametrer som brukes, hvem som har tilgang til analysen, grensene for bruk av dataene og hvordan de skal tolkes, må formidles tydelig til ansatte og studenter.

Institusjonene bør også gi studenter og ansatte en tydelig beskrivelse av prosessene som brukes til å utarbeide analysen, eller gjøre algoritmene transparente for dem.
Det kreves samtykke fra studentene for å kunne samle inn og bruke "særlige kategorier av opplysninger", for eksempel om etnisk opprinnelse, som definert i GDPR.

Studentene vil normalt også bli bedt om å samtykke til at det iverksettes personlige tiltak basert på læringsanalysen. Dette vil vanligvis bli gjort på det tidspunktet det foreslås et bestemt tiltak. Det kan imidlertid foreligge juridiske eller vernemessige hensyn eller andre forhold der studentene ikke har mulighet til å velge bort slike tiltak. I så fall må disse angis tydelig og være berettiget.

Nye læringsanalyseprosjekter vil muligens ikke være omfattet av institusjonens eksisterende ordninger. Innsamling og bruk av data til slike prosjekter kan kreve ytterligere tiltak, for eksempel konsekvensutredninger av personvern og innhenting av ytterligere samtykke.

Alternativer til samtykke må være tydelige og forståelige og forklare forventede konsekvenser av å gi eller nekte samtykke. Studentene bør enkelt kunne endre sine beslutninger senere.

Personvern

Tilgangen til studentdata og analyser bør begrenses til de personene som institusjonen har identifisert som å ha et berettiget behov for å se dem.
Når data skal brukes anonymt, må institusjonene være særlig nøye med å unngå

- identifisering av enkeltpersoner på grunnlag av metadata,
- reidentifisering av enkeltpersoner ved aggregering av flere datakilder.

Bruk av "særlige kategorier av opplysninger" med sikte på læringsanalyse krever ytterligere garantier. Omstendighetene der data og analyser kan deles eksternt - f.eks. ved forespørsler fra utdanningsmyndigheter, sikkerhetstjenester eller arbeidsgivere - vil gjøres uttrykkelig klart overfor ansatte og studenter, og kan kreve ytterligere samtykke.

Institusjonene bør sikre at studentdata er beskyttet når tredjeparter gis i oppdrag å lagre data eller utføre læringsanalyse på dem.
Institusjonene kan ha en rettslig forpliktelse til å gripe inn og dermed overstyre noen begrensninger i personvernet, dersom data eller analyser avdekker at en student er i fare. Slike omstendigheter bør være tydelig spesifisert.

Gyldighet

Det er viktig at institusjonene overvåker kvaliteten, robustheten og gyldigheten av sine data- og analyseprosesser for å kunne utvikle og opprettholde tilliten til læringsanalyse og sikre at den brukes til studentenes beste. Institusjonene bør sikre at

- unøyaktigheter i dataene forstås og minimeres,
- konsekvensene av ufullstendige datasett forstås,
- et optimalt utvalg av datakilder velges,
- falske korrelasjoner unngås.

Alle algoritmer og parametrer som brukes til prediktiv analyse eller tiltak, bør forstås, valideres, gjennomgås og forbedres etter behov av kvalifisert personell.

Data og analyser kan være gyldige, men bør også være nyttige og hensiktsmessige. Læringsanalyse bør ses i et bredere perspektiv og kombineres med andre data og tilnærminger etter behov.

Tilgang

Studentene bør i et forståelig og tilgjengelig format ha tilgang til all læringsanalyse som utføres på deres data, og bør få kopier av disse dataene i et bærbart, digitalt format. Studenter har en juridisk rett i henhold til GDPR til å kunne få rettet uriktige personopplysninger om seg selv.

De skal normalt også kunne få se hvilke parametrer og hvilken merking som er knyttet til dem. Hvis en institusjon anser at analysen kan ha skadelig innvirkning på studentens faglige progresjon eller velferd, kan den holde analysen tilbake fra studenten, med forbehold for at det foreligger klart definerte og beskrevne retningslinjer. Den enkelte student skal imidlertid få se dataene om seg selv hvis vedkommende ber om det.

Mulighet for å iverksette positive tiltak

Institusjonene bør spesifisere under hvilke omstendigheter de mener de bør gripe inn når analysen antyder at en student kan dra nytte av ytterligere støtte. Dette kan omfatte å gi studentene råd om ikke å fortsette i en bestemt retning. Studentene kan også være forpliktet til å handle ut fra analysen de får framlagt for seg – i så fall bør slike forpliktelser være tydelig beskrevet og kommunisert overfor studentene.

Typen og arten av tiltak og hvem som er ansvarlig for å gjennomføre dem, bør være tydelig spesifisert. Noen kan kreve menneskelig heller enn digital formidling. Prediksjoner og tiltak vil vanligvis være registrert og kunne revideres, og deres hensiktsmessighet og effektivitet gjennomgås.

Effekten av tiltak på ansattes roller, opplæringskrav og arbeidsbelastning bør vurderes. Ivaretakelse av dette krever støtte fra den øverste ledelsen. Institusjonene bør også være tydelige på hvordan de prioriterer læringsanalyse i forhold til andre krav.

Institusjonene bør bestemme hvordan de skal fordele ressurser til læringsanalyse hensiktsmessig med hensyn til elever og studenter med forskjellige behov, og sikre at ulike grupper og enkeltpersoner ikke forskjellsbehandles.

Minimering av negative konsekvenser

Institusjonene må anerkjenne at analyse aldri kan gi et fullstendig bilde av en persons læring, og at det noen ganger kanskje ikke tas hensyn til personlige forhold.
Institusjonene bør treffe tiltak for å sikre at trender, normer, kategorisering eller enhver karakterisering av studenter ikke påvirker ansattes, studentenes eller institusjonenes oppfatning av og atferd overfor dem, forsterker diskriminerende holdninger eller øker sosiale maktforskjeller.

Analysesystemer og tiltak bør utformes nøye og gjennomgås regelmessig for å sikre at

- studentene beholder en passende grad av selvbestemmelse i beslutningsprosesser knyttet til egen læring og bruker læringsanalyse der det er hensiktsmessig for å bidra til å begrunne sine beslutninger,
- mulighetene til å "manipulere systemet", eller fordelene for studenten ved å gjøre det, minimeres,
- kunnskapen om at aktiviteten overvåkes, ikke fører til at studentene ikke deltar eller andre negative konsekvenser for deres faglige progresjon eller velferd,
- negative konsekvenser som følge av å gi studenter og ansatte informasjon om studentenes resultater eller sannsynlighet for suksess minimeres,
- ansatte har en praktisk forståelse av juridisk, etisk og uetisk praksis.

Forvaltning av data

Data som brukes til læringsanalyse, skal være i samsvar med institusjonens eksisterende retningslinjer for databehandling og GDPR, og skal særlig

- holdes på det minimum som er nødvendig for å kunne oppnå formålene med analysen på en pålitelig måte,
- behandles i EØS-området, eller dersom de behandles andre steder, kun i samsvar med GDPR,
- oppbevares bare i et tidsrom som er hensiktsmessig, og som er klart definert.

På forespørsel fra studenter bør alle personopplysninger som er brukt til eller generert av læringsanalyse, destrueres eller anonymiseres, med unntak av visse klart spesifiserte datafelt som kreves for utdanningsmessige eller lovbestemte formål, for eksempel karakterer.

LÆRINGSANALYSE I FEM TRINN

EN VEILEDNING TIL GDPR

INNLEDNING

Læringsanalyseer å «måle, samle inn, analysere og rapportere data fra studenter og deres miljø for å forstå og optimalisere læringen og læringsmiljøet» (Siemens, 2011). Analysene av dataene kan gi forskjellige målgrupper (studenter, lærere, institusjoner) verdifull innsikt i flere aspekter ved utdanningsprosessen. Innsamling og analyse av data innebærer ofte behandling av personopplysninger – data som direkte eller indirekte inneholder informasjon om enkeltpersoner som studenter og lærere. Når en utdanningsinstitusjon behandler personopplysninger, er det EUs personvernforordning (GDPR) som gjelder.

GDPR fastsetter strenge kriterier for grunnlaget for bruken av læringsanalyse. Bruken av læringsanalyse krever omhyggelig vurdering av risikoen for enkeltpersoner, og at det iverksettes egnede tiltak. Det holder ikke bare å innhente samtykke én gang og legge ut en personvernerklæring på nettstedet.

I dette veikartet tar SURF sikte på å bistå utdanningsinstitusjoner i utformingen av deres læringsanalyse i samsvar med GDPR. Veikartet er bare ment som en veiledning, og hver enkelt utdanningsinstitusjon må foreta sine egne vurderinger for å ivareta personvernet. Det støtter institusjoner i å sikre de juridiske aspektene ved deres læringsanalyseprosjekter. Dette bidrar til å skape et trygt læringsmiljø som respekterer personvernet til enkeltpersoner.

Viktig

Denne planen tilbyr institusjoner et rammeverk for innføring av læringsanalyse ved institusjonen. Den gir imidlertid ikke uttømmende råd om hvordan hver enkelt institusjon skal overholde lover og forskrifter.

Komme i gang

Ønsker institusjonen å begynne med læringsanalyse og sette i gang et prosjekt til dette formålet? Gjennomgå planens trinnvise anvisninger med læringsanalysegruppen for umiddelbart å kartlegge læringsanalysens konsekvenser for personvernet. Ikke hopp over noen av trinnene. Det beste er å fokusere på trinnene som er mest relevante for deres prosjekt. På hvert trinn kan dere lese om de relevante juridiske termene og hva dere må gjøre. Sørg også for at institusjonens personvernombud blir involvert i innføringen av denne planen.

Tips

Hvis dere vil ha mer kontekst rundt de juridiske termene, kan dere konsultere:

- **the GDPR guide from the Government (in Dutch)**
- **the SURFwiki explaining the GDPR and how to interpret it (in Dutch)**
- **SURF's 'Privacy in research' online module (in Dutch)**

TRINN 1: FORBEREDELSE

Under forberedelsene til læringsanalysen er det viktig å begynne med å sette sammen en prosjektgruppe som i fellesskap skal definere formålet med prosessen. Det er også viktig å identifisere alle prosjektets interessenter. På dette trinnet beskrives hvilke forberedelser som kreves.

1.1 Definere de spesifikke målene dere ønsker å nå med læringsanalysen

Det er viktig at de spesifikke målene for prosjektet defineres så tidlig som mulig. Bruk det første trinnet til å vurdere og beskrive hva institusjonen egentlig vil oppnå med læringsanalysen. Begynn med å definere prosjektets formål, etterfulgt av en beskrivelse av hvordan læringsanalyse kan hjelpe dere å oppfylle det. Dere kommer også til å bruke målene dere formulerer i denne fasen, i utformingsfasen (trinn 2) og i vurderingen av legitimitet ved hjelp av en vurdering av personvernkonsekvenser (Data Protection Impact Assessment, DPIA) i trinn 3.

Å beskrive de spesifikke målene er uhyre viktig ettersom det gjør behandlingen av personopplysninger rettferdig, gjennomsiktig og forståelig. Viktige prinsipper er:

- **Formålsbegrensning:** Personopplysninger kan kun behandles for spesifikke, uttrykkelige og legitime formål. Læringsanalyse er et middel til å nå målene deres. Under bestemte forhold kan innsamlede opplysninger også brukes på et senere tidspunkt og til et annet formål enn det de opprinnelig ble innhentet for. Dette må imidlertid være kompatibelt med formålet opplysningene ble innsamlet for.
- **Dataminimering:** Opplysningene må være adekvate, relevante og begrenset til bare det som er nødvendig for formålet de behandles for.
- **Lagringsbegrensning:** Fastsett tidsfrister for sletting av personopplysninger når de ikke lenger er nødvendige for formålet de ble innhentet for.
- **Ansvarlighet:** Dere må registrere bruken av personopplysninger og forklare bruken av opplysningene for enkeltpersoner på en gjennomsiktig, forståelig måte og i et lett tilgjengelig format. Dere finner mer informasjon under «Informere», avsnitt 4.3.

Eksempler

Definer og beskriv formålene så spesifikt som mulig. Generelle beskrivelser som «forbedre læringsprosessen» eller «lagre svar for å utarbeide en pilottest» er ikke tilstrekkelig. Konteksten og enkeltpersoners forventninger avgjør hvilket detaljnivå som kreves. Dere bør derfor utdype det generelle formålet nærmere nedenfor, og beskrive hvordan opplysningene blir behandlet for det formålet:

- **Formål:** «Fokusere nærmere på emner der det gjøres mest feil i undervisningstimer». Den fullstendige beskrivelsen av formålet, herunder hvordan læringsanalysen skal gjennomføres, blir da for eksempel: «Utdanningskoordinatoren for modulen 'Grunnlag for personvernloven' analyserer svarene i det digitale læringsmiljøet på gruppenivå gjennom studieåret for å forutsi i hvilke fag det gjøres flest feil, slik at disse fagene kan vies større oppmerksomhet i undervisningen.»
- **Formål:** «Å kunne tilby fremragende studenter honours-programmer som er relevante for dem». Den fullstendige formålsbeskrivelsen, inkludert hvordan læringsanalysen utføres, blir i dette tilfellet: «Koordinatorene for honours-programmene ønsker å gi fremragende studenter anerkjennelse ut fra gjennomføringshastighet og resultater på praksisprøver i det nettbaserte læringsmiljøet i relevante fag ved utgangen av et studieår slik at disse studentene kan tilbys relevante studieprogrammer.»

En god, fullstendig formålsbeskrivelse har følgende struktur: «Hvem» ønsker å gjøre «hva» ved hjelp av «hvilke» personopplysninger, og «når» skal et «resultat» foreligge. Husk SMART-prinsippet: Spesifikt, målbart, ambisiøst, realistisk og tidsavgrenset. Godt beskrevne formål vil gjøre det lettere å gjennomføre den trinnvise planen.

1.2 Etablere en tverrfaglig prosjektgruppe

Det neste trinnet i gjennomføringen av en læringsanalyseprosess er å etablere en prosjektgruppe. Tenk etter hvem i organisasjonen(e) som kan ha interesse av å delta i prosjektet. Har en lignende prosjektgruppe vært etablert tidligere? Finn i så fall ut hvem som var med i den gruppen.

Engasjer personer med spisskompetanse i gruppen. For eksempel med følgende bakgrunn: klient, prosjektleder, prosjektdesigner, funksjonsleder, jurist og lærere.

I tillegg til prosjektgruppen bør dere også vurdere hvilke interessenter som må involveres i prosjektet nå og i fremtiden. En spesielt viktig rolle er personvernombudet. Dere må rådføre dere med personvernombudet under behandling og gjennomføring av en vurdering av personvernkonsekvenser (DPIA). Dette blir nærmere diskutert i trinn 3.

Definer hvordan dere vil opprette støtte på institusjons- og individnivå. Hvordan kan dere overbevise studenter om at læringsanalyse er viktig? Diskuter prosjektet med dem. Det er også en viktig del av gjennomføringen av en DPIA.

1.3 Beskrive interessenter

Beskriv hvilke spesifikke grupper av interessenter som kommer til å spille en rolle i distribusjonen av læringsanalyse, angi hvilke stillinger de har og hvilke forventninger eller ønsker (interessentanalyse). Det omfatter grupper innen institusjonen, de som kommer til å arbeide med og administrere læringsanalysesystemet, og i tillegg grupper som hjelper til med å vedlikeholde systemet, underleverandører og grupper det innhentes opplysninger fra. Eksempler omfatter studenter, lærere, mellomledere, prosjektledere og ledelsen. Institusjonen kan allerede ha innført prosedyrer for fremsetting av et prosjekt for medvirkningsrådet eller studentrådet, eller for å få det vurdert av en testkommisjon eller et etikkråd. Hvis det finnes erfarne sakkyndige som allerede har brukt læringsanalyse i eller utenfor institusjonen, bør de involveres.

En interessentanalyse vil hjelpe dere å lære av andres erfaringer, fange opp fokusområder og risikoer dere ikke hadde tenkt på tidligere, og skape støtte blant interessentene.

TRINN 2: UTFORMING

Når rammeverket for læringsanalyseprosessen er definert og beskrevet i førsteutkastet til handlingsplan, må dere finne ut hvordan prosessen skal implementeres. Dette trinnet skal resultere i en beskrivelse av systemene som trengs for å gjennomføre læringsanalyse. Denne utformingen skal gjøre det klart både teknisk og juridisk hvordan institusjonen skal utføre læringsanalyse.

De følgende trinnene i utformingen har allerede tatt hensyn til de relevante juridiske prinsippene. I denne fasen er det imidlertid for tidlig å tenke på hvorvidt læringsanalysesystemet som helhet er legitimt og hvilket vurderingsgrunnlag som kan benyttes. Utformingen må være ferdig før dette kan tas stilling til. Legitimiteten skal derfor ikke vurderes før senere. Den blir nærmere diskutert på trinn 3.

2.1 Inkludere personvern i utformingen

Læringsanalyse fungerer bare dersom dere er i stand til å behandle de innsamlede opplysningene på riktig måte. I de følgende trinnene må dere vurdere hvilke opplysninger som må samles inn for å nå de fastsatte målene, og inkludere resultatet av denne vurderingen i utformingen.

Definer hvilke opplysninger dere trenger som et minimum for å oppfylle formålene

Kan målsettingen også oppfylles hvis dere samler inn opplysninger fra færre personer? Eller ved å samle inn færre opplysninger fra hver enkelt person? I utformingen av læringsanalysesystemet er dere rettslig forpliktet til å inkludere personvern i utformingen fra starten av.

Konseptet innebygd personvern betyr at de personvernsensitive egenskapene til et produkt eller en tjeneste skal tas hensyn til fra utformingsfasen og videre, og at tilstrekkelige personvernhensyn skal integreres for å beskytte og sikre personopplysninger.

Jo færre opplysninger dere innhenter fra enkeltpersoner, jo lettere er det å beskytte de aktuelle opplysningene og desto mindre er risikoen for brudd på personvernet. Dere kan også beskytte opplysninger ved å dele dem opp slik at personopplysningene behandles separat og opplysningene bare settes sammen med et klart formål. Noen ganger kan personopplysninger også sikres ved å bruke dem på en abstrakt måte: kollektivt i stedet for enkeltvis. Statistikk er den best kjente måten å presentere forskningsdata på uten å avdekke personopplysninger.

Tips

Les mer om innebygd personvern og de aktuelle strategiene her:

- **Privacy Designer (in Dutch)**
- **the Blauwe Boekje (pdf) privacy design strategies (in Dutch)**

2.2 Definere omfanget av behandlingen

Det er viktig at omfanget av prosjektet fra et personvernperspektiv er kjent i utgangspunktet. Det er viktig å avgjøre følgende på forhånd:

1. hvilken type personopplysninger dere bruker
2. hvor sensitive opplysningene er
3. mengden av opplysninger som skal behandles
4. hvorvidt det er andre relevante faktorer som påvirker omfanget av behandlingen, for eksempel geografisk område

1. Definere hvilke deler av datasettet som inneholder personopplysninger

Ifølge GDPR er personopplysninger «enhver opplysning om en identifisert eller identifiserbar fysisk person». Dette henviser til opplysninger som enten er direkte tilknyttet en person eller kan spores tilbake til vedkommende. Personopplysninger omfatter derfor for eksempel navn og adresser, men også eksamensresultater eller informasjon om atferd. Ved å sette disse opplysningene ytterligere i sammenheng (eventuelt med andre opplysninger) er det dermed mulig å spore opplysningene tilbake til enkeltpersoner. Dette gjelder indirekte identifiserbare opplysninger.

Beskriv hvilke personopplysninger som skal samles inn som en del av dette prosjektet. For more information see the GDPR guide from the Government (in Dutch) and the SURFwiki explaining the GDPR and how to interpret it (in Dutch).

2. Fastslå hvorvidt dere behandler sensitive personopplysninger

Sensitive personopplysninger er opplysninger som angår en persons helse, etnisitet, seksualitet, politisk oppfatning eller religion. Behandling av slike opplysninger er forbudt med mindre institusjonen har den registrertes samtykke eller behandlingen av dem er lovregulert. Samtykke innebærer å spørre særskilt etter de relevante opplysningene og forklare hvorfor, og det er frivillig å gi sitt samtykke.

Innhenting av uttrykkelig samtykke er det mest åpenbare unntaket for behandling av sensitive opplysninger ved bruk av læringsanalyse. De grunnleggende elementene er beskrevet under Samtykke i avsnitt 3.1. Hvis det er umulig å be om samtykke, finnes et mulig unntak for vitenskapelig forskning (se artikkel 24 GDPR Den behandlingsansvarliges ansvar).

Tips

For more information about the difference between explicit consent to process sensitive personal data and consent as a basis of assessment, see the directives on consent from the European Data Protection Board (pdf in Dutch).

Vær oppmerksom på følgende

Fødselsnummeret – det ellevesifrede identifikasjonsnummeret fra Folkeregisteret – er også en egen type personopplysning. Fødselsnumre kan bare behandles når et er saklig behov for det, og formålet med behandlingen må oppgis. For eksempel må fødselsnummeret sladdes hvis et identitetsbevis skal kopieres.

Som institusjon kan dere også behandle sensitive personopplysninger når det ikke er den primære hensikten, for eksempel hvis institusjonen foretar en detaljert analyse av studieatferd i nettbaserte læringsmiljøer, og funnene er spesifikt knyttet til medisinske (søvnmønstre og livsstil) eller religiøse (atferd på helligdager) opplysninger. På dette trinnet bør dere derfor prøve å merke dere eventuelle konsekvenser læringsanalyse kan medføre.

3. Definere mengden av opplysninger som skal behandles

Når dere har fastslått hvilken type (sensitive) personopplysninger som er nødvendige for å oppfylle formålet, er det også viktig å definere hvor mange forskjellige typer opplysninger dere kommer til å behandle i læringsanalyseprosessen. I den sammenheng er det viktig som et minimum å svare på følgende spørsmål:

- Hvor mange typer opplysninger planlegger vi å behandle?
- Hvor ofte kommer vi til å behandle disse opplysningene?
- Hvor lenge varer behandlingen av opplysningene (fra innsamling til sletting/anonymisering)?
- Hvor mange registrerte (deltakere i læringsanalyseprosessen) blir det behandlet opplysninger fra?

4. Definer hvorvidt andre elementer er relevante for omfanget av behandlingen.

I noen tilfeller er det tilleggsfaktorer som påvirker definisjonen av behandlingens omfang. Ett eksempel kan være det geografiske området som opplysningene behandles innenfor. Det kan hende at enkelte regler er annerledes dersom personopplysninger om enkeltpersoner blir behandlet i andre (europeiske) land. Hvis dere konkluderer med at dette faktisk er tilfellet, anbefaler vi dere å konferere med personvernombudet for å fastslå om spesifikke tiltak er påkrevd.

2.3 Beskrive hvordan personopplysninger vil bli behandlet

1. Definer hvilke tiltak dere vil iverksette: behandling av personopplysninger

Beskriv de forskjellige handlingene som vil utført med personopplysningene. Behandling betyr alle handlinger en utdanningsinstitusjon kan utføre med personopplysninger, fra innsamling og lagring til sletting av opplysningene. Dere må derfor beskrive hver enkelt fase av behandlingen for læringsanalyse, som innsamling, påfølgende analyse og endelig bruk av resultatene. For eksempel er det å spore hva en person gjør i et læringsmiljø, en form for behandling av personopplysninger. Bruk av synonymer og anonymisering av data er gode tiltak dere kan iverksette for å ivareta enkeltpersoners personvern, men disse handlingene anses også som behandling.

2. Beskrive datakildene dere vil bruke

Beskriv datakildene (inndataene) dere vil bruke, og opprinnelsen til de aktuelle kildene. Definer hvilke opplysninger dere trenger og som institusjonen allerede sporer, og hvor opplysningene er å finne.

Utdanningsinstitusjoner har en rekke systemer som kan inneholde relevante opplysninger. Disse omfatter læringsstyringssystemer, studentinformasjonssystemer, testsystemer, systemer for registrering av fravær og til og med mobilapper med sensorer som GPS-sporing. Den store fordelen ved læringsanalyse er at du kan kombinere disse dataene ved hjelp av tekniske standarder.

Viktig

Ta ikke umiddelbart i bruk alle de foreliggende opplysningene i læringsanalyseprosjektet. Arbeid dere i stedet først gjennom veikartet, og følg alltid prinsippet om dataminimering.

3. Beskrive systemene som brukes

Skisser systemene og tjenestene i og utenfor institusjonen som er relevante for å gjennomføre prosessen. Hvordan vil dere sette opp læringsanalysesystemet? Kommer dere til å bruke et separat nettsted, eller kanskje en app? Eller kommer et eksisterende system til å bli brukt til læringsanalyse? Omfatter systemet nye teknologier hvis risiko ennå ikke er fastslått?

Vær oppmerksom på at lov om elektronisk kommunikasjon (ekomloven) gjelder når dere samler inn data ved hjelp av informasjonskapsler (og sammenlignbare teknologier som skript). Se reglene under Samtykke i avsnitt 3.1.

4. Beskrive de aktuelle tjenesteleverandørene

Utdanningsinstitusjoner benytter seg ofte av tjenesteleverandører som leverandører ved læringsanalyse. Definer hvem som kommer til å ha tilgang til personopplysningene og hvem institusjonen kommer til å dele opplysningene med. Det kan hende at tjenesteleverandørene får tilgang til opplysninger gjennom programvare for læringsanalyse. Dette kan for eksempel skje med skytjenester for studenter eller eksterne systemer som registrerer testprestasjoner og genererer rapporter ut fra disse opplysningene.

Hvis dere bruker tredjeparts programvare eller tjenester, er det to ting dere bør være oppmerksomme på:

1. Juridisk sett har institusjonen alltid ansvaret for kvaliteten på og eventuelle problemer med tjenester som ytes. Det er også tilfellet dersom programvareleverandøren ikke ønsker på påta seg noe ansvar. Institusjonen kan ikke unngå dette ansvaret ved for eksempel å legge inn en ansvarsbegrensning i læringsanalysesystemets samtykkeerklæring på startsiden i programvaren.
2. Hvis den eksterne tjenesteleverandøren også mottar personopplysninger, slik tilfellet er med skytjenester, må institusjonen inngå separate avtaler om hva tjenesteleverandøren kan gjøre med de aktuelle opplysningene. Her er det viktig å avklare tjenesteleverandørens rolle. For å definere hvilken rolle en tjenesteleverandør skal ha med hensyn til personvernet, bør dere lese forklaringen i avsnitt 2.5.

Velge tjenesteleverandører

Når dere velger tjenesteleverandører, bør dere i utvelgelsesprosessen inkludere GDPR-krav som sikkerhets- og informasjonsforpliktelser og -tiltak ved behandling av opplysninger utenfor EØS-området. Hvis dere overlater behandlingsaktiviteter til tjenesteleverandører, må dere benytte dere av tjenesteleverandører som stiller tilstrekkelige garantier, spesielt hva angår kompetanse, pålitelighet og ressurser. Da kan dere være sikre på at de tekniske og organisatoriske tiltakene overholder personvernreglene, også med hensyn til sikker behandling.

2.4 Beskrive (sikkerhets-)tiltakene

Institusjoner som bruker personopplysninger, må beskytte opplysningene i samsvar med personverndirektivet, GDPR. Det reduserer faren for datainnbrudd og andre potensielle brudd på personvernet. Ifølge GDPR må dere iverksette egnede tekniske tiltak til dette formålet, for eksempel å bruke moderne teknologi til å sikre personopplysninger. Dere må ikke bare se på teknologien, men også på hvordan dere som organisasjon behandler personopplysninger. Hvem har for eksempel tilgang til opplysningene?

Iverksett tekniske og organisatoriske tiltak for å garantere personopplysningenes konfidensialitet, integritet og tilgjengelighet

Hvis dere lagrer personopplysninger, må de beskyttes forsvarlig. Det betyr at dere som institusjon innen rimelighetens grenser må beskytte personopplysningene dere innhenter, mot uautorisert eller ulovlig tilgang eller bruk. Dette gjelder ikke bare opplysninger dere har bedt om, men også personopplysninger dere uforvarende har mottatt. Vi anbefaler dere derfor å opprette retningslinjer for sikkerhet og mot eventuelle datainnbrudd.

Den finnes fremdeles ingen generelt gyldig norm eller standard som fokuserer spesifikt på beskyttelse av personopplysninger. I enkelte bransjer gjelder spesifikke normer som NEN 7510. SURF har opprettet en norm og et testrammeverk for informasjonssikkerhet basert på NEN 27001.

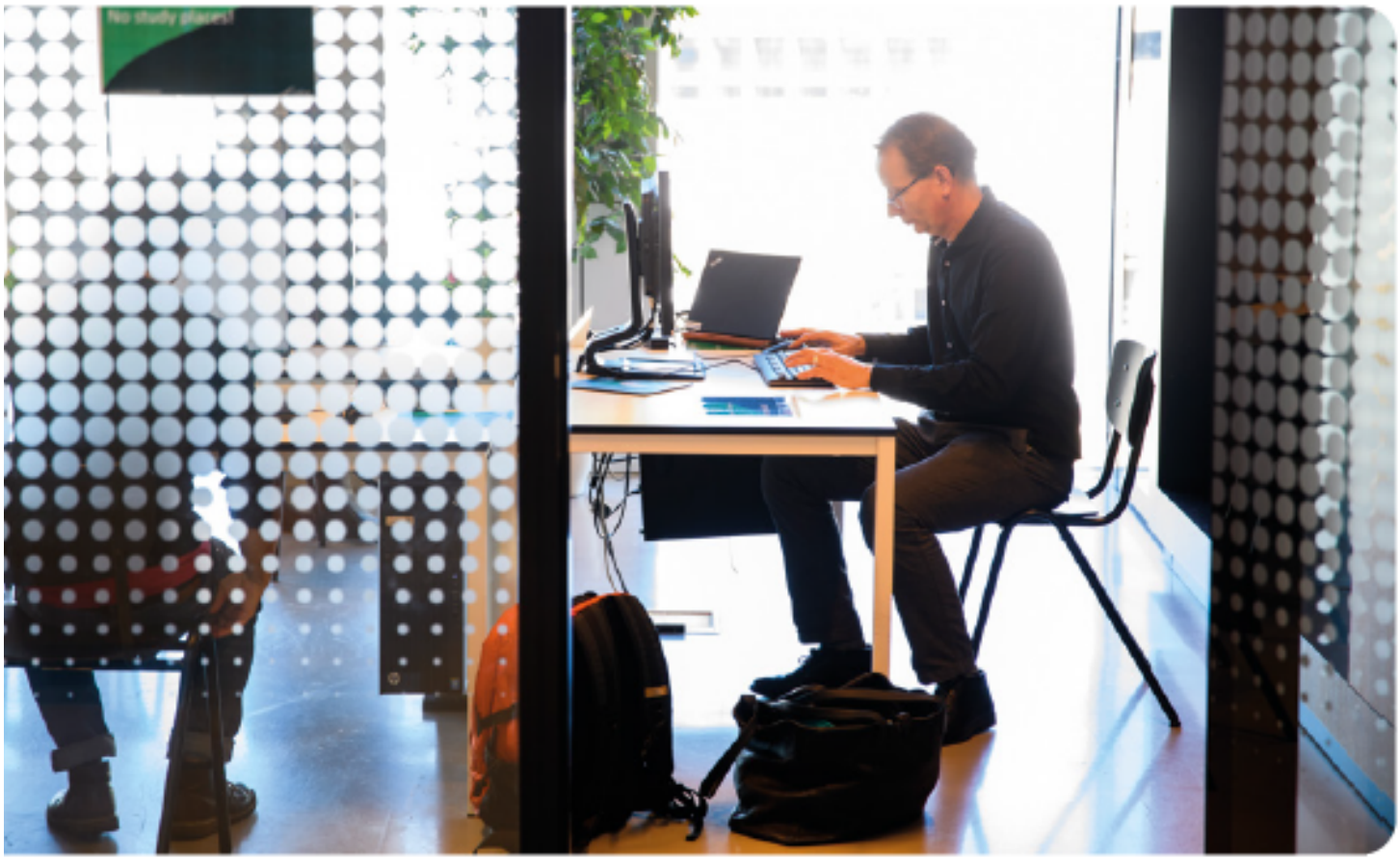
Datatilsynet har publisert retningslinjer for hvordan institusjoner kan oppfylle sikkerhetskravene. Ifølge disse retningslinjene må sikkerheten være en integrert del av utviklingen og forbedringen av tjenester, og institusjonene må jevnlig kontrollere at sikkerheten er tilstrekkelig (PlanDoCheckAct).

I tillegg skal personopplysninger holdes nøyaktige og tilgjengelige. Iverksett derfor tiltak for å forebygge bearbeiding av data og redusere og fjerne trusler som kan gjøre at dataene ikke lenger er tilgjengelige. Iverksett for eksempel tiltak mot løsepengevirus og DDoS-angrep.

Tips

Se ekstra ressurser om sikkerhet:

- **Datatilsynets nettsted**
- **De nyttige rapportene fra franske personvernmyndigheter og ENISA/Teletrust**



Bruk aggregater og pseudonymer

I noen tilfeller iverksettes tiltak for å beskytte eller sikre opplysningene bedre. Hashing – en praksis som behandler data kryptert – er et eksempel på dette. Datatilsynet mener at til og med slike praksiser utgjør behandling av personopplysninger. Bare hashing av navn eller identifiserende opplysninger uten ytterligere tiltak betyr ikke at personopplysninger ikke blir behandlet. I disse tilfellene er det derfor fremdeles mulig å spore opplysningene tilbake til enkeltpersoner. Dette kalles også pseudonymisering. Opplysningene er fremdeles dekket av GDPR.

Opplysninger anses bare som anonymisert hvis det ikke lenger finnes noen rimelig måte å spore dem tilbake til en person på. For eksempel ved å tilordne unike vilkårlige numre til data og deretter slette listen som kobler navnene til de aktuelle numrene. Selv da kan imidlertid en person ofte bli identifisert ved hjelp av andre data, selv om de ikke er koblet til et navn eller sporbart unikt nummer. For eksempel er en samling av en students prøveresultater og moduler unik. To studenter i samme årskull får aldri nøyaktig samme karakterer på det samme pensumet. Denne samlingen utgjør derfor et sett med personopplysninger, selv om studentens navn eller unike nummer ikke er oppgitt.

Data kan miste sin status som personopplysninger hvis de blir tilstrekkelig aggregert, det vil si, hvis de slås sammen med utsagn som gjeldere flere personer. «Åtti prosent av studentene strøk på denne eksamenen» er for eksempel ikke en personopplysning. Det stilles ingen lovbestemte krav til denne typen statistikk.

Viktig

Tilstrekkelig aggregerte data gir flere alternativer, men datagrunnlaget er fortsatt personopplysninger som styres av GDPR. Kun behandling som starter med aggregerte data, gir dere flere alternativer. For eksempel kreves et grunnlag dersom en lærer måler hvor raskt enkelte studenter jobber seg gjennom kursmateriellet på en nettbasert læringsplattform. Det er tilfellet også selv om læreren bare bruker funnene til statistiske formål. Mer informasjon er tilgjengelig i retningslinjene for forskning og anonymisering av data, publisert av forløperen for European Data Protection Board (EDPB).

Definere organisasjonens tidsrom for lagring av datasett

Personopplysninger kan ikke oppbevares lenger enn det som er nødvendig ut fra formålet de ble innhentet for. Opplysninger som ikke lenger er nødvendige, skal tilintetgjøres eller slettes. Dere må derfor angi på forhånd et tidsrom for oppbevaring av de forskjellige datasettene. Tidsrommets varighet avhenger helt og fullt av formålet med oppbevaringen av de forskjellige datasettene og hvordan systemet behandler dem.

- Anslå hvor lenge dere har bruk for datasettene for å nå de fastsatte målene.
- Vær oppmerksom på, i den grad det er mulig, ytterligere behandlingsformål som å underbygge undersøkelser i rapporter, arkivering, akademisk ansvar og personopplysningsmyndighetens direktiver.

Tips

Se også håndboken til National Coordination Point Research Data Management (LCRDM).

2.5 Definere interessenters personvernroller

Definer hvilke roller de involverte partene spiller for personvernet i hvert enkelt tilfelle av opplysninger som behandles. Rollene som defineres av GDPR, er:

- Behandlingsansvarlig: den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes
- Flere behandlingsansvarlige: de som i fellesskap bestemmer formålet med og hvilke midler som skal brukes til uløselig sammenknyttede behandlingsaktiviteter
- Databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige
- Tredjepart: andre parter.

For eksempel: En høyskole beslutter å analysere studentdata for å finne ut hvilke moduler studenter oftest ikke består. For å analysere dette bruker høyskolen et skybasert verktøy der de registrerer alle studentenes karakterer i ett år. I dette tilfellet definerer høyskolen hvilke data de analyserer og til hvilket formål. Leverandøren av skyløsningen utfører bare analyse på vegne av høyskolen. I dette tilfellet er høyskolen den behandlingsansvarlige, mens leverandøren av verktøyet er en databehandleren.

Tips

Dere finner mer kontekst om de juridiske begrepene i Datatilsynets GDPR-veiledning.

TRINN 3: VURDERING

3.1 Lovligheten av læringsanalyseprosessen

Det er viktig å undersøke om formålet med læringsanalysen står i forhold til inngrepet overfor personene hvis opplysninger dere behandler (proporsjonalitetsprinsippet), og om det er mulig å oppnå samme formål på en måte som er mindre ufordelaktig for de berørte personene (prinsippet om subsidiaritet). Hvis alt er forsvarlig utført, har dere allerede vurdert disse punktene i prosjektets utformingsfase (se trinn 2).

Fastslå om bruken er forholdsmessig
Proporsjonalitet avhenger av om bruk av læringsanalyse er forholdsmessig. Dere skal derfor vurdere hva institusjonen søker å oppnå med læringsanalysen, og definere hvordan dette formålet står i forhold til potensielle konsekvenser for enkeltpersoner. Selv om målet ikke helliger middelet, tillates generelt sett mer for et mer krevende formål. Dataene må være nødvendige for å oppfylle formålet. Dette er strengere enn «ønskelige» eller «nyttige».

Definer om mindre inngripende midler kan oppfylle det samme formålet.
Læringsanalyse må vurderes ikke bare med henblikk på proporsjonaliteten, men også for subsidiaritet. Det betyr at det ikke må finnes en mindre inngripende måte å oppfylle det samme formålet på. I en læringsanalysekontekst betyr dette blant annet at dere må granske det overordnede formålet og vurdere om det kan oppfylles uten bruk av læringsanalyse. Ta i betraktning behovet for å behandle personopplysninger, kompleksiteten og konsekvensene ved å bruke læringsanalyse.

Når læringsanalyseprosjektet er utformet (resultatet av trinn 2) og dere har definert proporsjonaliteten og subsidiariteten, kan dere definere de/de relevante grunnlaget/-ene for å behandle personopplysninger. Hver enkelt behandling av personopplysninger krever et støttende grunnlag eller en rettferdiggjøring. Grunnlaget rettferdiggjør institusjonens behandling av personopplysninger til læringsanalyseformål. I prinsippet kreves ett av følgende seks grunnlag for hver enkelt fase (innsamling, analyse, bruk):

- samtykke
- nødvendig for å oppfylle en avtale
- rettslig plikt
- beskyttelse av vitale interesser
- utførelse av offentlig tjeneste
- legitim interesse

Bruke personopplysninger til annet formål enn det opprinnelige formålet med innsamlingen
En institusjon kan bare samle inn og behandle personopplysninger på et av grunnlagene som er beskrevet ovenfor. Som institusjon kan dere bruke disse opplysningene til faglig forskning, statistiske formål eller andre kompatible formål såfremt institusjonen har iverksatt de nødvendige tiltakene for å sikre at videre behandling bare blir utført for disse formålene. Hvis dere har en persons e-postadresse fordi vedkommende har stilt et spørsmål, kan dere svare denne personen, men dere kan ikke føre vedkommende opp som abonnent på nyhetsbrevet deres, for det er et annet formål. Et annet formål er tillatt hvis det er i samsvar med det opprinnelige.

Et eksempel på dette kan være å sende ut en spørreundersøkelse om kvaliteten på brukerstøtten til en som har benyttet seg av tjenesten. Ettersom videre behandling (i dette tilfellet læringsanalyse) må samsvare med de spesifikke formålene, er formålsbegrensning et vanskelig krav. Tanken er å skaffe til veie nye kunnskaper, bli i stand til å stille nye spørsmål og se på data fra nye innfallsvinkler.

Dette er per definisjon ikke et «spesifikt formål». Vi anbefaler derfor å føre opp så mange konkrete formål som mulig i informasjonen som gis, og revidere dem med jevne mellomrom. Når dere reviderer formålene institusjonen har fått samtykke til, må dere innhente nytt samtykke til de reviderte formålene.

For eksempel: *En lærer bruker et overvåkingsverktøy under en eksamen for å måle hvorvidt personer som tar eksamenen på nytt, oppnår andre resultater enn dem som tar den for første gang. Det gjeldende grunnlaget her er «legitim interesse». Resultatene må deretter behandles ved statistisk forskning på suksessfaktorer for den aktuelle eksamenen. Dette anses som videre behandling til forskningsformål.*

Tips

Rammebetingelsene for vitenskapelig forskning er også å finne i håndboken til National Coordination Point Research Data Management (LCRDM).

Bruker institusjonen læringsanalyse på opplysninger som er blitt innsamlet på lovlig vis tidligere, og er formålet med læringsanalysen kompatibelt med formålet som personopplysningene opprinnelig ble innsamlet for? I så fall er det ikke behov for et separat rettslig grunnlag utover det som behandlingen opprinnelig var basert på.

Følgende faktorer er viktige for å bestemme om formålene er kompatible:

- spesielt **enkeltpersoners rimelige forventning** basert på forholdet de har til institusjonen med henblikk på videre bruk
- eventuelle koblinger mellom de opprinnelige formålene og formålene med ytterligere behandling
- konteksten opplysningene ble innsamlet i: hva er forholdet mellom institusjonen og den enkelte?
- opplysningenes type og karakter: er de sensitive?
- de mulige konsekvensene av ytterligere behandling: hva er konsekvensene for den enkelte?
- om det er tilstrekkelige sikringstiltak som kryptering, aggregering, bruk av pseudonymer

Dette unntaket basert på «kompatibilitet» er relevant hvis enkeltpersonene kan forvente at bare opplysninger som er innhentet tidligere, vil bli brukt i den spesifikke læringsanalyseprosessen, at dens formål ligner de opprinnelige formålene, og at opplysningene som brukes, er ikke-sensitive opplysninger som dermed ikke vil ha store konsekvenser for enkeltpersonene i læringsanalyseprosessen.

Hvis læringsanalysen avhenger helt eller delvis av nye kilder, eller hvis formålene ikke er kompatible med de opprinnelige, må institusjonen undersøke om et av de seks grunnlagene kan benyttes, som oppgitt i begynnelsen av dette avsnittet.

Grunnlag: Avgjøre om «samtykke» er påkrevd for (deler av) behandlingen

I noen tilfeller må enkeltpersoner gi sitt samtykke til institusjonen som sporer dem med læringsanalyse. På grunn av vilkårene som samtykket må oppfylle, er dette en utfordring sett fra et juridisk og faglig ståsted. Å gi samtykke er ikke bare formaliteten ved å krysse av i en boks eller klikke på en popup for å få den til å forsvinne. Samtykket må være en frivillig godkjenning fra enkeltpersoner og gi dem kontroll over (deler av) læringsanalysebehandlingen.

Som en tommelfingerregel kan man i hvert fall gå ut fra at enkeltpersoners samtykke er påkrevd hvis læringsanalysen:

- behandler sensitive personopplysninger (se avsnitt 2.2)
- behandler sensitive personopplysninger som posisjonsdata. I noen tilfeller kan dette utgjøre en alvorlig risiko for personvernet og innebærer at en høy grad av individuell kontroll er nødvendig
- plasserer eller leser informasjonskapsler eller andre data, som læringsanalyseskript på datamaskinene, nettbrettene eller telefonene som enkeltpersoner bruker
- tar beslutninger utelukkende basert på automatisert behandling av personopplysninger hvis disse beslutningene har juridiske konsekvenser eller på annen måte påvirker enkeltpersonene i betydelig grad
- hvis, etter avveining av interessene og tiltakene som er iverksatt på grunnlag av «legitim interesse», enkeltpersoners interesser ikke er respektert i tilstrekkelig grad. Dette grunnlaget beskrives på slutten av dette avsnittet.

Loven gir ingen presis beskrivelse av hvordan samtykke skal etterspørres. Men måten institusjonen ber om samtykke på, må oppfylle følgende spesifikke krav:

1. **Frivillig:** Samtykket må være frivillig. Enkeltpersoner må ha anledning til å si «nei». Dette kan for eksempel ikke medføre at de nektes adgang til en obligatorisk modul eller hindres i å avlegge eksamen.
2. **Utvetydig:** Samtykket må gis i form av en aktiv og tydelig handling. Det betyr at bokser ikke kan være avkrysset på forhånd.
3. **Informert:** Som institusjon må dere informere enkeltpersoner om de viktigste elementene (som formålet med hver av behandlingene som dere ber om samtykke til, hvilke opplysninger som vil bli behandlet, og hvordan samtykket kan trekkes tilbake) umiddelbart og på forhånd. Det må være like enkelt å trekke tilbake samtykket som det er å gi det.
4. **Spesifikt:** Samtykket må alltid være til en spesifikk behandling og et spesifikt formål. «Jeg samtykker til læringsanalyse» er ikke spesifikt. Gjør det klart hvem som skal ha tilgang, hvilke opplysninger som samles inn, og hva opplysningene skal brukes til. Et eksempel: «Jeg samtykker til at mine faglige prestasjoner blir sporet og registrert i denne modulens nettbaserte læringsmiljø. Det skal brukes til å tilby meg personlig tilpasset studieveiledning. Veilederen skal få disse opplysningene for sammen med meg å kunne kartlegge risiko for forsinkelser.»

Hvis dere ber om samtykke til flere formål i løpet av behandlingen, må dere som institusjon informere de berørte og be om deres samtykke til hvert enkelt formål separat. Formålet kan heller ikke endres over tid.

Kort sagt må det fremgå tydelig hvilke moduler samtykket gjelder, hvor langt overvåkingen i hver modul strekker seg, og hvilke konsekvenser det har for den enkelte modul. Dere kan også skrive en kort forklaring med lenke til en tydeligere og mer informativ personvernerklæring med mer spesifikk informasjon. Innhenting av samtykke gjennom brukervilkår, generelle vilkår eller en personvernerklæring er ikke tillatt. Dere kan imidlertid henvise til en personvernerklæring for å gi mer informasjon om samtykket. Dere finner mer informasjon på trinnet «Informere», avsnitt 4.3.

Samtykket er ikke gyldig med mindre kravene ovenfor er oppfylt. Dere kan derfor ikke behandle personopplysninger (for denne delen). Under behandlingen og i opptil fem år etter må dere som institusjon dessuten kunne dokumentere at gyldig samtykke ble innhentet. Dette gjør grunnlaget for samtykke svakt og vanskelig å bruke.

1 *Dette gjelder ikke informasjonskapsler som er nødvendige for den tekniske funksjonen til (utdannings)tjenesten eller for analytiske informasjonskapsler som bare i ubetydelig grad krenker enkeltpersoners personvern (see also Article 11.7a of the Telecommunications act and the future ePrivacy Regulation and the step-by-step plan of the Personal Data Authority. (pdf in Dutch)*

Tips

For more information please see the Dutch translation of the GDPR guidelines on consent from the European Data Protection Board (EDPB).

Grunnlag: Nødvendig for å oppfylle en avtale

Personopplysninger kan behandles dersom det er nødvendig for å oppfylle en avtale. Hvis en institusjon har inngått en avtale med en person, kan institusjonen behandle vedkommendes personopplysninger i den grad det er nødvendig for å oppfylle avtalen. Det må dreie seg om en avtale der den aktuelle personen er en aktør. Behandlingen må være et nødvendig resultat av avtalen.

Bare det faktum at læringsanalyse inngår i en avtale med en person, betyr ikke at kravet er oppfylt med mindre behandlingen er nødvendig for å oppfylle avtalen. Når man vurderer om behandling av personopplysninger er nødvendig for inndataene om utdanningsresultatene, er det innholdet og det underliggende formålet med avtalen som bestemmer om behandlingen virkelig er nødvendig for (utdannings)resultatene. Hvis dette er tilfelle, kan institusjonen bruke det som grunnlag. Avtalen i seg selv kan imidlertid ikke fokusere utelukkende på behandling av personopplysninger, men må ha et annet (utdanningsmessig) formål. Utdanningsinstitusjoner inngår vanligvis ikke avtaler med studenter. Enkelte anser registreringen hos institusjonen som en avtale, men fra et strengt juridisk ståsted er ikke dette tilfelle.

Som utdanningsinstitusjon må dere for dette grunnlaget dokumentere at bruken av læringsanalyse er nødvendig. Ettersom læringsanalyse er relativt nytt, kan det lett bli sett på som unødvendig for utdanningen. Den gjengse oppfatningen er at utdanningen kan være like god uten læringsanalyse. Det kan bare presenteres som nødvendig hvis det er tydelig at utdanning uten læringsanalyse er mindreverdig. Dette kan imidlertid bare gjøres dersom læringsanalysen beviser sin verdi over flere år. Dette grunnlaget kan derfor brukes, selv om den sannsynlige koblingen til spesifikke utdanningsformål er mindre sterk.

Grunnlag: Nødvendig for å oppfylle en rettslig plikt

Det tredje behandlingsgrunnlaget som nevnes i GDPR, er rettslig plikt. Personopplysninger må behandles hvis det er pålagt ved lov. For å kunne behandle personopplysninger på dette grunnlaget må det være umulig å oppfylle denne forpliktelsen uten å behandle opplysningene.

Som institusjon må dere anse det som at det er nødvendig for å oppfylle formålet med lovgivningen. Dette krever en god forståelse av utdanningsresultater. Læringsanalyse er en måte å skaffe til veie denne forståelsen på. Det argumentet kan rettferdiggjøre bruken av dette verktøyet. De samme merknadene om nødvendighet gjelder her som for grunnlaget «Nødvendig for å oppfylle en avtale».

Grunnlag: Nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet

Dette grunnlaget er relevant hvis institusjonen utfører et offentlig oppdrag i allmennhetens interesse, for eksempel i henhold til lov om universiteter og høyskoler. Det omfatter oppgaver som er basert på denne loven og er relevante for institusjonen. Som for de andre grunnlagene er «nødvendighet» kriteriet som må kunne bekreftes. Det holder ikke at opplysningene er «relevante» eller «nyttige».

En utdanningsinstitusjon som skal bekrefte nødvendighet, kan hevde at de utfører en oppgave i allmennhetens interesse. Dette krever en god forståelse av utdanningsresultater. Læringsanalyse er en måte å skaffe til veie denne forståelsen på. Det resonnementet kan rettferdiggjøre bruken av dette verktøyet. Institusjonen må selv kunne dokumentere at læringsanalyse virkelig er i allmennhetens interesse eller å utøve offentlig myndighet, og at det ikke finnes noe annet alternativ.

Tips

For behandling av personopplysninger for læringsanalyseformål som ikke faller inn under institusjonens utøvelse av offentlig myndighet, kan dere vurdere vilkårene for «å ivareta legitime interesser» nedenfor. Som mer eller mindre offentlige organisasjoner er det ikke sikkert utdanningsinstitusjonene kan basere utøvelsen av offentlig myndighet på «legitime interesser».

Grunnlag: Nødvendig for å ivareta legitime interesser

Dette grunnlaget betyr at behandlingen av personopplysninger er nødvendig for institusjonens (utdanningsmessige) interesser, eller for en ekstern part eller enkeltpersoner, og at enkeltpersoners personvern dermed blir ivaretatt i størst mulig grad.
Kameraovervåkning er et godt eksempel. Det er vanskelig å be om samtykke fra alle som går inn i en bygning, men behovet for den spesifikke interessen «overvåking og sikkerhet» er åpenbart. I dette eksemplet er det tilstrekkelig med et oppslag og en forskrift som informerer om hvordan de innhentede bildene blir behandlet. I tillegg er filming ikke tillatt på steder der personvernet veier tyngre, for eksempel i garderober eller toalettrom.

Institusjonen kan bruke «legitime interesser» som behandlingsgrunnlag hvis:

- institusjonen, en ekstern part eller enkeltpersoner har en klart definert legitim interesse eller fordel
- behandling av læringsanalysen er nødvendig for å ivareta denne interessen Som beskrevet tidligere betyr altså dette at dere som institusjon må undersøke hvorvidt interessen av behandlingen er proporsjonal med konsekvensene for enkeltpersoners personvern, og hvorvidt det ville være mulig for institusjonen å oppnå formålene på en annen måte som er mindre ugunstig for de berørte personene.
- institusjonen har avveid interessene og de utdanningsmessige interessene mot interessene til enkeltpersoner, og dette er dokumentert. Institusjonen kan også bli nødt til å iverksette tiltak for å sikre at enkeltpersoners rettigheter og frihet tillegges større betydning enn den legitime interessen. Enkeltpersoners rimelige forventning basert på forholdet de har til institusjonen, må i dette tilfellet tas hensyn til. Bruken av dette behandlingsgrunnlaget er underlagt strenge krav: Institusjoner må for eksempel publisere sine vurderinger (f.eks. på nettstedene sine) og i prinsippet tilby enkeltpersoner rett til å klage (trekke seg) når som helst.

Tips

Bruk en «legitim interesseavveiing» eller Datatilsynets forklaringer til å veie interessene for grunnlaget «legitim interesse».

3.2 Vurdering av personvernkonsekvenser (DPIA) for læringsanalyse

Ifølge GDPR må organisasjoner, i tillegg til å bruke et behandlingsgrunnlag, i enkelte situasjoner gjennomføre en vurdering av personvernkonsekvenser (*Data Protection Impact Assessment,* DPIA). Dette er et verktøy for å skissere og vurdere på forhånd personvernrisikoene ved databehandling på en strukturert, standardisert måte, slik at tiltak kan iverksettes senere for å redusere disse risikoene til et minimum. Dokumentasjonen viser også at dere som institusjon har oppfylt de lovbestemte kravene for behandling.

Selv om gjennomføringen av en DPIA ikke alltid er obligatorisk, anbefales det for læringsanalyseprosjekter. En DPIA bidrar ikke bare til å økt bevissthet om konsekvensene ved å bruke personopplysninger; ofte er det også en *profilerings*- eller høy personvernrisiko for enkeltpersoner som gjør det
obligatorisk å gjennomføre en slik vurdering. SURF anbefaler alle institusjoner som bruker læringsanalyse, å gjennomføre en DPIA. Se også Datatilsynets forklaring av DPIA.

Vær oppmerksom på følgende

Bruk av læringsanalyse vil i mange tilfeller bli kategorisert som profilering. Profilering er blant det som krever en obligatorisk vurdering av personvernkonsekvenser, og beskrives som følger: «*systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering. Eksempler omfatter vurdering av arbeidsprestasjoner, studieprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd.*»

- Les mer om vurdering av personvernkonsekvenser på nettstedet til Datatilsynet
- Se også den norske oversettelsen av retningslinjene for vurdering av personvernkonsekvenser

3.3 Hvordan gjennomføres en DPIA?

Det finnes flere måter å gjennomføre en DPIA på. Dere kan velge en av dem så lenge den oppfyller de grunnleggende kravene i GDPR. De grunnleggende kravene er en systematisk beskrivelse av databehandlingen dere skal gjennomføre, en vurdering av nødvendigheten av og proporsjonaliteten til læringsanalysen vis-à-vis det uttalte formålet, en vurdering av personvernrisikoen for enkeltpersoner og tiltak for å redusere denne risikoen. Deretter er det opp til institusjonen å implementere disse tiltakene. Dere er også pålagt å rådføre dere med personvernombudet. Det gir en ekstra sikkerhet på at DPIA-en i tilstrekkelig grad tar hensyn til risikoen, og at tilstrekkelige tiltak blir iverksatt for å håndtere denne risikoen.

Hvis DPIA-en avdekker at læringsanalyse utgjør en høy grad av risiko, og dere som institusjon ikke er i stand til å finne (tilstrekkelige) tiltak for å redusere denne risikoen, må dere konferere med det nasjonale personvernombudet før dere kan ta i bruk læringsanalyse.

Tips

- **(Data) Protection Impact Assessment templates and risk forms have been drawn up by SURF (in Dutch)**
- **Det finnes også eksempler på DPIA-maler fra veiledende myndigheter som kan brukes eller tilpasses:**
  - **Commission Nationale de l'Informatique et des Libertés (CNIL)**
  - **Information Commisioner's Office (ICO)**

3.4 Definere konsekvensene av læringsanalyse (risikovurdering)

Bruk av læringsanalyse må være i tråd med institusjonens egne formål og samfunnsmessige retningslinjer. Verdiene som institusjonen forfekter, forholdet til studentene, bærekraft, mangfold og lignende må gjenspeiles i læringsanalysesystemet. Risikovurdering er en viktig del av DPIA.

Når læringsanalyse brukes for å oppfylle et gitt formål, er det med sikte på å realisere fordeler for både institusjonen og enkeltpersoner. Fordelene kan blant annet være frihet, velvære, bærekraft, inkludering og mangfold, likestilling, et passende tjenestetilbud, rettferdighet, effektivitet og kostnadsreduksjon.

Beskriv fordelene for institusjonen og for enkeltpersoner

Fordelene ved læringsanalyse kan ligge på forskjellige nivåer og berøre forskjellige parter. En institusjon kan bruke læringsanalyse med reduserte kostnader som formål og samtidig ta sikte på å oppfylle politiske, utdanningsmessige eller forskningsmessige formål.

Beskriv risikoen for institusjonen og for enkeltpersoner

Dere må som institusjon iverksette egnede tiltak for å redusere risikoen ved læringsanalyse. I praksis innebærer dette en fortløpende vurdering av risikoen læringsanalysen medfører, for å kunne oppdage når personvernrisiko for enkeltpersoner oppstår. En «risiko» er et scenario som beskriver en hendelse og dens konsekvenser, anslått ut fra alvorlighetsgrad og sannsynlighet for at den skal inntreffe. Som institusjon må dere håndtere slik risiko ved å koordinere aktiviteter for å veilede organisasjonen og ved å iverksette tiltak.

Som en del av DPIA må dere som institusjon undersøke om planlagte tiltak, sikringstiltak og mekanismer for å beskytte enkeltpersoners interesser er tilstrekkelige, eller om det kan gjøres mer for å redusere risikoen for involverte parter ytterligere. Dere må derfor være oppmerksom på de mulige konsekvensene for enkeltpersoner og hvilke skadevirkninger behandling av personopplysninger kan ha, enten det dreier seg om fysiske, emosjonelle eller materielle skader. Vær spesielt årvåkne når det gjelder læringsanalysens potensielle risiko for:

- at det blir umulig å håndheve rettigheter (f.eks. personvernrettigheter)
- avslag på søknad om tjenester eller utdanningsmuligheter
- tap av kontroll over bruken av personopplysninger
- diskriminering
- identitetstyveri eller bedrageri
- økonomisk tap
- svekkelse av omdømme
- fysisk skade
- brudd på taushetsplikt
- gjenidentifisering av pseudonymiserte opplysninger
- andre betydelige økonomiske eller sosiale ulemper

3.5 Definere tiltak som reduserer risiko

Når all risiko er kartlagt, må institusjonen beskrive tiltakene den har til hensikt å innføre for å bøte på risikoen, herunder sikringstiltak, sikkerhetsforanstaltninger og mekanismer for å garantere vern av personopplysninger og dokumentere overensstemmelse med GDPR.

Registrer kilden til hver risiko eller potensiell ulempe som identifiseres. Vurder hvilke alternativer som er tilgjengelige for å redusere risikoen. For eksempel:

- beslutte ikke å samle inn visse typer opplysninger
- begrense omfanget av behandlingen
- forkorte lagringstiden
- iverksette ytterligere teknologiske sikkerhetsforanstaltninger
- gi medarbeidere opplæring i å forutse og håndtere risiko
- om mulig anonymisere eller pseudonymisere opplysninger
- utarbeide interne retningslinjer eller prosedyrer for å unngå risiko
- bruke annen teknologi
- inngå klare avtaler angående deling av data (se «Behandleravtale»)
- endre personvernerklæringer (se «Informere»)
- gi enkeltpersoner en rimelig grad av kontroll over opplysningene som behandles av institusjonen. Kanskje dere vil kunne oppnå de fastsatte formålene bare ved å gi enkeltpersoner tilgang til funnene i læringsanalysen
- gi enkeltpersoner mulighet til å trekke seg fra deltakelse i prosjektet dersom det er nødvendig, eller
- innføre nye systemer for å hjelpe folk med å ivareta sine rettigheter

Denne listen er ikke uttømmende. Dere finner mer informasjon i Datatilsynets veiledning «Vurdering av personvernkonsekvenser (DPIA)» . Rådfør dere også med personvernombudet. Avgjør om tiltakene reduserer eller fjerner risikoen. Vurder fordeler og ulemper ved hvert enkelt tiltak for å avgjøre om det er egnet.

3.6 Resultater av DPIA

Når all informasjon er inkludert i DPIA-en, er det viktig å spørre institusjonens personvernombud til råds. Det gir en ekstra sikkerhet på at DPIA-en i tilstrekkelig grad tar hensyn til risikoen, og at tilstrekkelige tiltak blir iverksatt for å håndtere denne risikoen. Rådene må dokumenteres sammen med institusjonens beslutning om å gå videre med læringsanalyseprosessen eller ikke. Det anbefales også å spørre enkeltpersoner (f.eks. studenttillitsvalgte) hva de mener om prosjektet.

Tips

Send resultatene av DPIA-en til personvernombudet og/eller institusjonens interne juridiske avdeling for en siste gjennomgang.

Hvis DPIA-en viser at behandling av personopplysninger medfører en høy risiko for enkeltpersoner, og den risikoen ikke fjernes ved hjelp av avbøtende tiltak, må institusjonen drøfte saken med Datatilsynet før behandlingen begynner. Dette kalles en «innledende drøfting». Dere finner mer informasjon på Datatilsynets nettsted.

TRINN 4: IMPLEMENTERING

Hvis vurderingen gir et positivt resultat, læringsanalyseprosessen anses som forholdsmessig og ingen restrisiko er identifisert, er tiden inne for å iverksette de nødvendige juridiske, tekniske og organisatoriske tiltakene.

4.1 Fullføre de nødvendige kontraktene

I utformingsfasen (trinn 2) skisserte dere hvilke leverandører og andre tredjeparter som er involvert i læringsanalysesystemet. Umiddelbart etter definerte dere hvilke parter som skal ha hvilke roller (behandlingsansvarlig/behandlet) ifølge personvernlovgivningen. Institusjonen må bruke denne informasjonen til å forberede og fullføre avtaler.

Utarbeid en avtale om ansvarsfordeling

Hvis institusjonen definerer formålet med og midlene til læringsanalyseprosessen sammen med andre, resulterer det i et delt ansvarsforhold. De som deler ansvaret, må opprette gjensidige ordninger for gjennomsiktig innretting av ansvarsområdene etter GDPR. Dette berører særlig hvordan enkeltpersoners rettigheter ivaretas, og hvem som skal gi informasjon om læringsanalyse. Hovedtrekkene i denne avtalen må også være tilgjengelige for enkeltpersoner.

Tips

- **SURF har en mal til avtale om ansvarsfordeling**
- **Se også SURFs portal for konsekvenser og risikovurdering**

Utarbeid en databehandleravtale

I en databehandleravtale beskrives forholdet mellom en tjenesteleverandør (databehandleren) som behandler personopplysninger på vegne av en annen part (den behandlingsansvarlige). Denne avtalen er obligatorisk. Store leverandører har ofte sine egne modellavtaler. En databehandler kan bare behandle personopplysninger på oppdrag fra den behandlingsansvarlige i henhold til databehandleravtalen. Kontroller omhyggelig om behandlingen under læringsanalysen og formålet med den er tydelig beskrevet i databehandleravtalen.

Tips

Institusjoner og SURF har i fellesskap utarbeidet en modellavtale for databehandler som en del av SURF Legal Standards Framework for (Cloud) Services. Dette dokumentet setter standarder for konfidensialitet, personvern og tilgjengelighet for (sky-)leverandører.

Tilgang til personopplysninger utenfor Det europeiske økonomiske samarbeidsområdet (EØS)

Institusjoner har ingen plikt til å lagre personopplysninger sammen med parter innen Europa, men det gjør det noe enklere fra et juridisk ståsted. Det er fordi GDPR gir enkeltpersoner de samme personvernstandardene i alle EU-land, mens andre regler gjelder for overføring av personopplysninger til parter utenfor EU, til organer i såkalte tredjeland. Tredjeland er alle land som ikke er medlem av EU, pluss Norge, Liechtenstein og Island (EØS-landene). Som følge av Brexit er det sannsynlig at også Storbritannia kommer til å bli et tredjeland.

Hovedregelen for tredjeland er at organisasjoner bare kan overføre personopplysninger til dem hvis de har et tilstrekkelig beskyttelsesnivå. Europakommisjonen har utarbeidet en liste over tredjeland som anses å ha et tilstrekkelig beskyttelsesnivå. I tillegg til tilfellene som er beskrevet ovenfor, er internasjonal overføring av personopplysninger bare tillatt på grunnlag av bestemmelsene i GDPR, som å garantere et beskyttelsesnivå med kontraktsbestemmelser (modellkontrakter eller *Standard Contractual Clauses*) eller som angitt av Europakommisjonen (f.eks. *Privacy Shield*, et sertifikat for parter i USA som mottar europeiske personopplysninger). Det er derfor dere må kontrollere om avtalene dere inngår med de relevante partene, krever avklaring eller gjennomgang.

Dere må kontrollere løsningene som brukes av parter i tredjeland for å tilrettelegge for overføring av personopplysninger. Se mer informasjon fra Datatilsynet angående internasjonal overføring.

4.2 Utarbeid de nødvendige dokumentene med retningslinjer og prosedyrer

Lag en oversikt over hvilke retningslinjer som er aktuelle for læringsanalyse. Definer de riktige oppfølgingstrinnene hvis institusjonen ennå ikke har relevante prosedyrer.

- Retningslinjer for sikkerhet, herunder håndtering av brukeridentitet (se SURF-publikasjoner om sikkerhet).
- Prosedyrer for håndtering av datainnbrudd for å overholde rapporteringsplikten ved datainnbrudd. Hvis et datainnbrudd skjer, er institusjonen i visse tilfeller pålagt å rapportere det. Dere må avgjøre om et datainnbrudd er av en slik art at det må rapporteres til Datatilsynet og eventuelt de involverte partene.
- Prosedyrer for behandling av forespørsler fra enkeltpersoner om tilgang til eller sletting av opplysninger.

4.3 Informere enkeltpersoner om behandling av personopplysninger ved læringsanalyse

Alle som behandler personopplysninger, må tydelig informere berørte personer om hva som skjer med personopplysningene deres, og hvorfor. Hver enkelt person må motta denne informasjonen før eller på tidspunktet da institusjonen behandler opplysningene deres.

Institusjoner kan bruke personvernerklæringer til å forklare enkeltpersoner, for eksempel studenter, hva som skjer med personopplysningene deres. Måtene institusjoner bruker data på, kan deles inn i kategorier. Vurder i hvilken grad institusjonen deres kan være åpen med hensyn til læringsanalyse. Formålet med åpenhet er å tilrettelegge for forklaring av bruken og virkningene av læringsanalyse. I tillegg til eksistensen og virkningene av læringsanalysen er det også viktig å forklare konsekvensene av den på en tydelig måte. I personvernerklæringen forklarer dere enkeltpersoner nøyaktig hva læringsanalyse er, hvilke opplysninger institusjonen bruker til formålet, og hvordan og med hvilke konsekvenser læringsanalyse trekker konklusjoner. For eksempel: «Vi fører tilsyn med hvor lang tid du bruker på de nettbaserte oppgavene. Hvis du bruker betydelig lengre tid enn gjennomsnittet, får du tilleggsforklaringer og oppgaver å gjennomgå før du kan fullføre denne modulen.»

Det er viktig at enkeltpersoner enkelt kan be om tilgang til personvernerklæringen og erklæringen om bruk av informasjonskapsler (om nødvendig) for personopplysningene deres behandles. Bekreftelse er ikke obligatorisk, og dere er heller ikke pålagt å tvinge enkeltpersoner til å lese personvernerklæringen. Det er ikke nødvendig å få den enkelte til å erklære (f.eks. ved avkryssing) at de godtar personvernerklæringen.

Hvis institusjonen påberoper seg samtykke som behandlingsgrunnlag, kan enkeltpersoner gi sitt samtykke ved å krysse av i en rubrikk på en samtykkeerklæring. Denne erklæringen må være tydelig på hva studenten gir sitt samtykke til. Se også grunnlag for «Samtykke» i avsnitt 3.1.

4.4 Sikkerhet og risikoreduserende tiltak

Bruk de beskrevne sikkerhetstiltakene til å garantere at personopplysningenes konfidensialitet, integritet og tilgjengelighet. Iverksett også de ekstra risikoreduserende tiltakene i avsnitt 3.5. Kontroller hvorvidt tiltakene har den ønskede virkning.

4.5 Andre tiltak

Implementer en rett til å protestere mot profilering

En person kan alltid protestere mot å ha vært gjenstand for profilering eller blitt berørt av et tiltak basert på vedkommendes personlighetsprofil. Den enkelte må eksplisitt informeres om muligheten til å protestere. Personen som mottar protesten, må deretter ha mulighet til å oppheve tiltaket. Hvis samarbeid med en programvareleverandør er nødvendig for å oppheve en handling som er utført av læringsanalysesystemet, må dere ha lagt til rette for denne prosessen i samarbeid med leverandøren (i databehandleravtalen).

Kommunikasjon

Definer hvorvidt institusjonen må iverksette flere tiltak basert på læringsanalysen, og implementer disse. For eksempel:

- etablere en kommunikasjonsprosedyre eller brukerstøtte for spørsmål fra enkeltpersoner og andre interessenter
- opprette en informasjonsside med vanlige spørsmål og svar
- lære opp brukerne av læringsanalysesystemet

4.6 Pilot

Vurder å gjennomføre et pilotprosjekt for å finne ut om alle funksjoner fungerer forsvarlig. Etter pilotprosjektet kan dere godkjenne eller avvise driften. Hvis det godtas, kan dere innføre læringsanalyse i større omfang som konklusjon på implementeringsfasen.

TRINN 5: EVALUERING

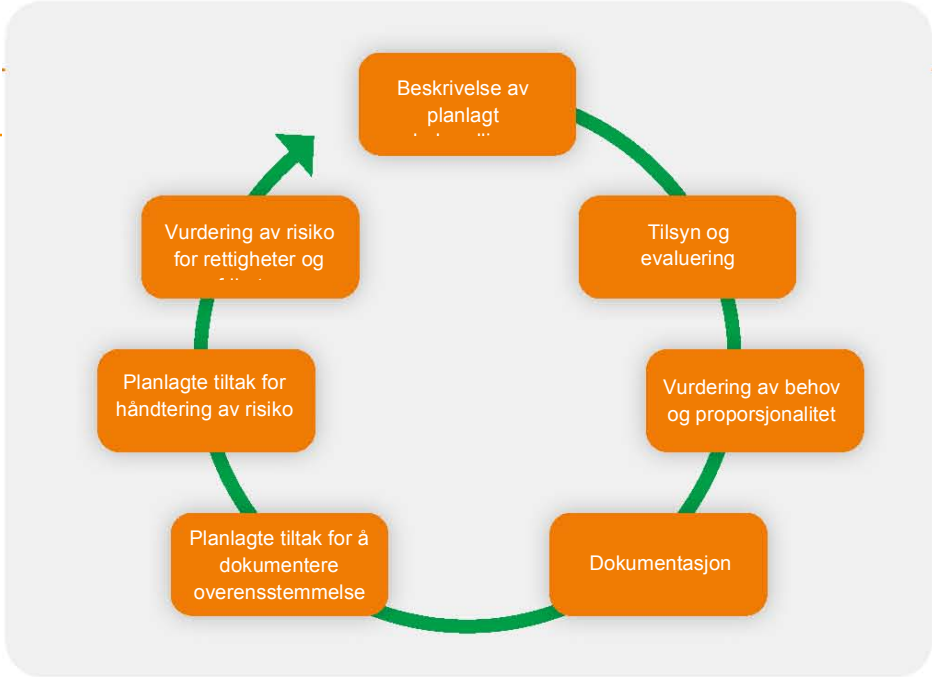
5.1 Evaluer med jevne mellomrom

Å vurdere hvorvidt et læringsanalysesystem er forsvarlig ut fra et personvernrettslig perspektiv er ingen engangsforeteelse. Både organisasjonen og de ytre faktorene endrer seg. Det kan påvirke de samfunnsmessige og juridiske rammene for systemet og derfor også dets legitimitet. Derfor er det viktig å evaluere jevnlig om systemet fremdeles er forsvarlig. Ved å gjennomføre periodisk evaluering oppdager dere ny risiko i tide og oppretter en tilbakemeldingssløyfe som forbedrer bruken av læringsanalyse og gjør den mer formålstjenlig.

Evaluering kan gjennomføres med jevne mellomrom (f.eks. årlig), men det er også lurt å kunne kjenne igjen situasjoner som innebærer ny evaluering. For eksempel:

- Læringsanalysesystemet brukes til et annet formål enn det opprinnelig var ment for
- Nye datakilder eller ny teknologi er tatt i bruk
- Eksisterende datakilder er endret eller ikke lenger i bruk

I slike situasjoner bør dere forbedre prosessen og om nødvendig gjennomgå denne trinnvise planen på nytt. Realiseringen av denne trinnvise planen er ingen engangsoppgave, men en løpende prosess.



Kilde: Skisse fra DPIA-synspunkt på EPDB, s. 20.

5.2 Publiser erfaringer

Vurder å lagre og dele arbeidsmetodene deres. Hvordan kan dere sikre at lærere vet hvor de finner beskrivelsen av læringsanalyseprosessen og hvilke personvernhensyn som er tatt? For eksempel bruker spesialister ofte en felles plattform der dere kan publisere arbeidsmetodene deres, som SURFs personvern-wiki. Dere kan også bruke institusjonens interne portal.

TAKK

Komposisjon og redigering
Niels Westerlaken, *Project Moore*
Jocelyn Manderveld, *SURF*
Floortje Jorna, *SURF*

Takk til
Arnoud Engelfriet, *ICT Recht*
Evelijn Jeunink, *SURF*
Sebas Veeke, *SURF*

Prosjektledelse
Jocelyn Manderveld, *SURF*
Marieke de Wit, *SURF*

Layout
Vrije Stijl, Utrecht

Trykk
Drukkerij Libertas Pascal

Forsidebilde
Annemiek van der Kuil, PhotoA.nl

Foto
s. 10, 21: Sicco van Grieken, Erasmus Universiteit Rotterdam
s. 18: Sicco van Grieken, Wageningen University & Research

Mai 2019

SURF
088 – 787 30 00
www.surf.nl/onderwijs
onderwijsinnovatie@surf.nl