Datatilsynet

Kunnskapsdepartementet
Postboks 8119 Dep
0032 OSLO

Deres referanse	Vår referanse	Dato
14/3274	14/00736-2/EOL	14. oktober 2014

Datatilsynets høringsuttalelse - NOU 2014:5 MOOC til Norge

Vi viser til deres brev av 24. juni 2014 hvor dere sender utredningen NOU 2014: 5 MOOC til Norge - Nye digitale læringsformer i høyere utdanning, ut på høring.

Våre kommentarer er knyttet til de sidene av utredningen som berører problemstillinger som gjelder personvern. Slik vi ser det gjelder dette særlig tema som verifisering av identitet, læringsanalyse, kvalitetsutvikling/forskning og finansiering.

Innledningsvis ønsker vi å påpeke at utvalget ser ut til å ha gjort et grundig utredningsarbeid på de temaene de har valgt å vektlegge. Det er for eksempel positivt at det er innhentet betenkninger fra to kompetente fagpersoner innen opphavsrett.

På den annen side ser vi at utvalget ikke har sett nødvendigheten av å foreta en konsekvensutredning av personvernkonsekvenser i forbindelse med bruk av MOOC (Massive Open Online Courses). Sider ved MOOC som utfordrer personvernet er nevnt enkelte steder i utredningen, men er konsekvent utelatt når utvalget skal oppsummere sine anbefalinger og råd etter hvert kapittel.

Vi mener det er en svakhet ved utredningen at den ikke går nærmere inn på personvernproblematikk, og heller ikke gir klare anbefalinger til ansvarlige myndigheter og/eller utdanningsinstitusjonene om å avklare hvilke plikter som påløper etter personvernregelverket ved å ta i bruk MOOC.

Vi vil i det følgende komme med kommentarer til de kapitlene vi mener særlig reiser problemstillinger knyttet til personvern.

Kapittel 8 Dokumentasjon av oppnådd kompetanse.
I dette kapittelet er det særlig pkt 8.4 Verifisering av identitet som reiser problemstillinger som vedrører personvern.

Som utvalget selv fastslår handler verifisering av identitet i MOOC om å kreditere riktig person for oppnådd kompetanse. Dette har betydning for forvaltningen av identitetsopplysninger ved bruk av MOOC.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Vi mener at de foreslåtte løsningene for bruk av biometri ikke er gode nok, og det vil ikke tilfredsstille noen trygg og sikker identifisering til dette formålet. Det vil være for enkelt å komme seg rundt slike løsninger. Vi foreslår heller at man avholder en fysisk eksamen på campus eller testsenter. Dersom man velger å la studenten avlegge eksamen over nett, bør identifisering gjøres ved at autorisert testpersonell foretar en manuell ID-kontroll i kombinasjon med bruk av e-ID ved levering. Det kan for eksempel være at man signerer elektronisk ved innlevering hvor man erklærer at det er riktig vedkommende som har utført eksamen.

Kapittel 10 Kvalitet og læringsutbytte
I dette kapittelet er det særlig pkt 10.3 Læringsanalyse og pkt 10.5.3 Virkemidler og premisser for kvalitetsutvikling som reiser problemstillinger som vedrører personvern.

Læringsanalyse
Utvalget trekker selv frem læringsanalyse som en av de mest sentrale endringene som heldigitale læringstilbud vil føre med seg. Sammenstilling av opplysningene lagret i digitale læringsressurser muliggjør analyser som tidligere ikke har vært mulig. Utvalget trekker frem at analyser kan gjøres på både makronivå (internasjonalt, regionalt, nasjonalt), mesonivå (institusjon) og mikronivå (deltakere og deltakergrupper).

Særlig analyse av data på mikronivå reiser problemstillinger som berører personvern. Viktige byggesteiner i personvernet er det enkelte menneskets rett og mulighet til selvbestemmelse, og medbestemmelse og kontroll med hvordan opplysninger om vedkommende blir brukt. I tillegg er formålsbestemthet, relevans, minimalitet, fullstendighet og kvalitet ved bruk av personopplysninger viktige prinsipper for ivaretakelse av personopplysningsvern[1].

Forskningsetikken er et eksempel på hvordan disse prinsippene er innbakt som spilleregler for all forskning som inkluderer behandling av personopplysninger. Prinsippet om selvbestemmelse gjenspeiles i hovedregelen om at bruk av personopplysninger i forskning forutsetter et frivillig, informert og uttrykkelig samtykke fra den opplysningene gjelder. Krav om formålsbestemthet er fremtredende i forskning og ivaretar personvernet ved at det for forskningsdeltaker er forutsigbart hva opplysningene skal brukes til.

I likhet med andre analysemetoder som baseres på stordataanalyse er det ved læringsanalyse utfordrende å ivareta enkeltpersoners rett til kontroll med personopplysningene sine. Dette fordi litt av poenget med å lagre store mengder personopplysninger er muligheten til bruk av disse personopplysningene til nye formål og bruksmuligheter som ikke nødvendigvis er forutsigbare på innsamlingstidspunktet.

Av de fem ulike formene for læringsanalyse som utvalget beskriver er det særlig prediktiv analyse og analyse av sosiale nettverk som er problematiske med hensyn til å ivareta studentenes personvern.

[1] Prinsippene er nærmere beskrevet i Datatilsynets rapport «Big data – personvernprinsipper under press»

Prediktiv analyse har som mål å forutsi hver enkelt students prestasjoner. Analysen gjøres ved hjelp av å kombinere demografiske data og tidligere studieresultater med opplysninger om for eksempel innloggingsmønstre på læringsplattformen, hvilke dokumenter studenten arbeider med og i hvilket omfang studenten deltar i nettdiskusjoner. 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. Det vil for eksempel kunne argumenteres med at god prediktiv analyse forutsetter at det meste av det studenten foretar seg i studietiden registreres og lagres, i tillegg til at studentens sosiale profil og forhistorie er tilgjengelig for studiestedet. En slik tilnærming utfordrer klart prinsippene om minimalitet og relevans fordi studiestedet med så bred datafangst vil sitte med mye overskuddsinformasjon. 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.

Den type læringsanalyse som går ut på å analysere sosiale nettverk har som mål å identifisere deltakere som ikke er sosialt og faglig integrert. Utvalget viser til forskning som viser at det er en klar sammenheng mellom samarbeid med andre og testresultater. De som samarbeider oppnår bedre resultater. Vi mener det er et betimelig spørsmål om en så omfattende overvåking av studentenes atferd er et forholdsmessig virkemiddel for å oppnå mer samarbeid mellom studenter.

Datatilsynet publiserte for et år tilbake en rapport som tar for seg personvernutfordringene knyttet til Big Data. Flere av synspunktene som fremkommer i denne rapporten har overføringsverdi til temaet læringsanalyse. For eksempel gjelder dette bekymringen omkring det vi kaller ***datadeterminisme***. I vår rapport «Big data – personvernprinsipper under press» er dette begrepet beskrevet slik:

«(...)utstrakt bruk av (...) prediksjonsanalyse kan befeste eksisterende fordommer og forsterke sosial ekskludering og lagdeling. En utvikling der stadig flere beslutninger blir tatt basert på algoritmer, kan lede til et "dataenes diktatur"; vi blir ikke vurdert ut fra hva vi faktisk foretar oss, men på basis av hva alle dataene om oss sier at vi sannsynligvis kan komme til å gjøre[2]*. «*

Vi vedlegger rapporten til inspirasjon i det videre arbeidet.

Vår anbefaling er at det må gjennomføres en utredning av personvernkonsekvenser av særskilt læringsanalyse før MOOC tas i bruk.

Virkemidler og premisser for kvalitetsutvikling
Utvalget drøfter under dette punktet hvilke strategiske grep som må tas for at utdanningsinstitusjonene skal kunne ta i bruk de pedagogiske mulighetene ved MOOC.

Datatilsynet er helt enig i at det bør tas noen strategiske grep, og vi er spesielt opptatt av de nasjonale rammebetingelsene. Med rammebetingelser i sammenheng med personvern og digitale læringsressurser mener vi avklaring av yttergrensen for hva et studiested kan

[2] Big data – personvernprinsipper under press, s. 6

«pålegge» en student å oppgi av personopplysninger – særlig når det er tale om å oppgi opplysningene til en tredjepart utenfor studiestedets kontrollsfære.

Personvern i skolen har vært et prioritert område for Datatilsynet i 2013-2014. Vi har i den sammenheng vært på kontroll hos en rekke grunn- og videregående skoler og sett særskilt på bruk av digitale læringsressurser. Funnene som vi gjorde her mener vi er relevante også for høyere utdanning.

Et fremtredende funn er at med mindre bruk av digitale læringsressurser har en økonomisk side (koster penger) har skoleeiere ikke kontroll eller oversikt over hvilke digitale læringsressurser som blir tatt i bruk i skolen. Mange digitale læringsressurser er gratis i den betydning at de ikke koster penger. «Gratis» applikasjoner har imidlertid en pris. Valutaen det betales i er studentenes personopplysninger. Identitet, kjønn, alder, interesser, tilstedeværelse, prestasjoner, kontakter, kalender etc. er opplysninger som er verdt milliarder i en industri i kraftig vekst.

For noen er denne prisen akseptabel – for andre ikke. Det problematiske med bruk av personopplysninger som betalingsmiddel i utdanningssektoren er at det ikke er studenten selv som tar avgjørelsen. Det er studiestedet som aksepterer betaling med personopplysninger på vegne av studenten.

I 2012 hadde Datatilsynet en sak til behandling som illustrerer hvorfor dette er problematisk. En gruppe studenter ved Høyskolen i Vestfold reagerte på at studiestedet hadde valgt en arbeidsplattform hvor studentene måtte legge ut sine individuelle skriftlige oppgaver åpent for hele studentkullet. Det var riktignok gitt en mulighet til å lukke siden for andre, men et slikt valg må begrunnes spesielt. Valg av publiseringsløsning var begrunnet med at studentene skulle tilegne seg digitale ferdigheter. Det kom imidlertid også frem at plattformen som var valgt var gratis, og at plattformer med bedre muligheter for ivaretagelse av personvern koster penger.

Datatilsynet anerkjenner selvsagt at studiestedene har en viss instruksjonsmyndighet over sine studenter som følger av avtalen mellom student og lærested, samt universitetsloven. Opplysninger om hva man presterer underveis i studietiden er imidlertid et eksempel på opplysninger som for mange er et anliggende mellom student og lærer/sensor. Datatilsynet mener at å legge opp til et system der alle studenter skal levere sine arbeider i åpne rom på digital plattform er å gå for langt i instruksjonsmyndigheten.

Datatilsynet ønsker ikke å være en bremsekloss for utprøving og satsing på digitale verktøy og innlæring av digitale ferdigheter hos studentene. Tvert imot mener Datatilsynet at rett bruk av digitale verktøy i undervisningssektoren kan medføre godt personvern for både studenter og ansatte. Det er imidlertid avgjørende for en god balansegang at det defineres noen yttergrenser for hva studiestedene kan pålegge studentene å oppgi av opplysninger og til hvem.

Vi merker oss at utvalget i sine vurderinger knyttet til kvalitet og læringsutbytte er innom spørsmålet om hvorvidt det kan tenkes at de store datamengdene som genereres og lagres for

bruk i særskilt læringsanalyse kan være problematisk med hensyn til personvern. Utvalgets konklusjon om at prinsipielle og uavklarte faktorer knyttet til personvern burde adresseres, gjenspeiles dessverre ikke i de anbefalingene de gir i slutten av kapittelet.

I sin drøfting og vurdering av digital kompetanse fremhever utvalget at bruk av teknologi i læring skaper behov for sammensatt kompetanse av pedagogisk, teknologisk og administrativ karakter. Datatilsynet mener at det til denne listen må tilføyes behov for kompetanse på personvern og informasjonssikkerhet.

Kapittel 18 Økonomiske og administrative konsekvenser av utvalgets anbefalinger
Utvalget har innhentet en uttalelse fra universitetslektor Gisle Hannemyr som blant annet tar for seg mulige finansieringsordninger for MOOC.

Hannemyr slår fast at MOOC ikke er gratis. Han trekker så frem aktuelle måter å finansiere MOOC på. Blant de aktuelle finansieringsordningene er det han kaller «persondata-graving». Dette innebærer at studentene for å delta må samtykke til at personopplysninger om dem blir samlet inn, og at disse kan selges til virksomheter som er villige til å betale for dem.

Hannemyr sier avslutningsvis at han av personverngrunner ikke ser for seg at persondata-graving skal bli en aktuell finansieringsform i Norge. Vi håper han har rett i dette, men med bakgrunn i kontrollene vi har gjennomført på grunn- og videregående skoler det siste året er vi imidlertid ikke overbevisst om at bevisstheten omkring personvern er høy nok til at dette er en reell terskel.

Vi anbefaler derfor at Kunnskapsdepartementet finner en finansieringsordning som hindrer at det utvikler seg en praksis hvor personopplysninger er betalingsmidlet for bruk av MOOC.

Innebygd personvern og PIA
Innebygd personvern (Privacy by Design) innebærer at det tas hensyn til personvern i alle utviklingsfaser av et system, i rutiner og i forretningspraksisen. Standardinnstillinger bør settes mest mulig personvernvennlige, og man bør bygge personvernet inn i designet. Det er viktig å ivareta informasjonssikkerheten fra start til slutt, og særlig viktig med tanke på læringsanalyse er det at det vises åpenhet. Mulige bruksområder for de dataene som samles inn bør kartlegges på forhånd, slik at et samtykke er presist og dekkende. Alt i alt handler det om å respektere brukerens rett til selvbestemmelse.

Utvalget anbefaler at norske MOOC-tilbud samles og profileres gjennom en egen nasjonal portal[3]. I den grad det blir aktuelt å bygge en norsk portal anbefaler Datatilsynet at Kunnskapsdepartementet gjør en vurdering av personvernkonsekvenser (Privacy Impact assessment (PIA)). En vurdering av personvernkonsekvenser bør blant annet inneholde en gjennomgang av mulige rettslige grunnlag for utlevering og gjenbruk av personopplysninger, prinsippene for formålsbegrensning, proporsjonalitet og dataminimalisering, samt teknisk

[3] NOU 2014:5, s. 67

tilgang og sikkerhet. Når man gjennomfører en slik vurdering bør også potensielle konsekvenser for de registrerte gjennomgås nøye[4].

I EU er det laget et PIA-rammeverk for RFID-applikasjoner for å hjelpe til med å avdekke personvernkonsekvenser som kan følge bruk av RFID. Rammeverket er laget av RFID-miljøet på oppdrag fra Artikkel 29-gruppen og kan ha overføringsverdi for forberedelse til bruk av MOOC[5].

En annen viktig del av innebygd personvern er å sørge for åpenhet. Virksomheter som benytter MOOC må være åpne om hvordan de behandler personopplysningene de samler inn. Dette innebærer blant annet å gi den enkelte innsyn i hvilke beslutningskriterier (algoritmer) som ligger til grunn for utvikling av profiler, og fra hvilke kilder opplysninger er hentet. En nasjonal portal bør tilrettelegge for slik åpenhet.

Videre kan det å sørge for dataportabilitet være innebygd personvern. En nasjonal portal bør tilrettelegge for at den enkelte kan få utlevert alle data som lagres i tjenestene i portalen i et brukervennlig format. Dataportabilitet kan hindre at kunder låses til enkelttjenester.

[4] Big Data – personvernprinsipper under press, s. 53
[5] Opinion 09/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

Oppsummering

- Det er nødvendig med en utredning av personvernkonsekvenser før Kunnskapsdepartementet legger til rette for bruk av MOOC.

- En utredning av personvernkonsekvenser bør særskilt ta for seg temaet læringsanalyse.

- Det er nødvendig med en avklaring av hvor langt den enkelte utdanningsinstitusjon kan gå i å gjøre utlevering av personopplysninger obligatorisk.

- Dersom man velger å la studenten avlegge eksamen over nett, bør identifisering gjøres ved at autorisert testpersonell foretar en manuell ID-kontroll i kombinasjon med bruk av e-ID ved levering.

- Kunnskapsdepartementet må finne en finansieringsordning som hindrer at det utvikler seg en praksis hvor personopplysninger blir betalingsmidlet for bruk av MOOC.

- En nasjonal satsing på MOOC må sørge for innebygd personvern i en MOOC-portal. Stikkord for innebygd personvern er: personvernvennlige standardinnstillinger, bygge personvern inn i designet, informasjonssikkerhet fra start til slutt, åpenhet, forhåndskartlegging av mulige bruksområder for de dataene som samles inn, dataportabilitet.

- Det bør utarbeides nasjonale rammebetingelser for bruk av MOOC og som inkluderer innebygd personvern.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO